



**CAMBRIDGESHIRE
& PETERBOROUGH**
COMBINED AUTHORITY

AUDIT AND GOVERNANCE COMMITTEE

Date: Friday, 24 September 2021

Democratic Services

Robert Parkin Dip. LG.
Chief Legal Officer and Monitoring Officer

10:30 AM

72 Market Street
Ely
Cambridgeshire
CB7 4LS

Fenland Hall County Road, March PE15 8NQ
[Venue Address]

AGENDA

Open to Public and Press

1 Apologies and Declarations of Interest

At this point Members must declare whether they have a disclosable pecuniary interest, or other interest, in any of the items on the agenda, unless it is already entered in the register of members' interests.

2 Chair Announcements

3 Minutes of the Previous Meeting

To approve the minutes of the meeting held on 30th July 2021 and note the Action Log.

AG Draft Minutes 300721 V2

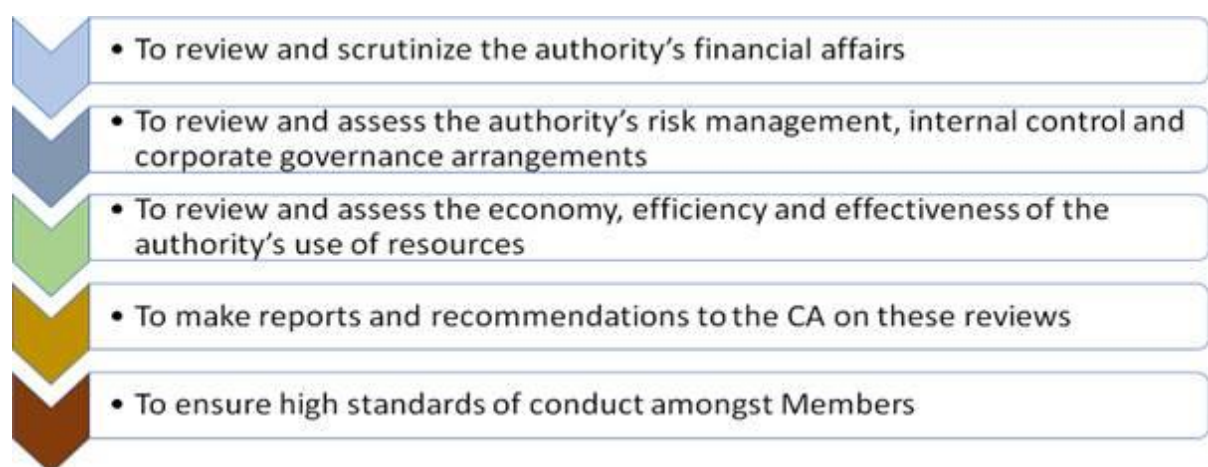
5 - 16

4	Combined Authority Update	
	To receive a verbal update from the Chief Executive of the Combined Authority	
5	Internal Audit	
	a) Progress Report	
	b) Annual Report	
	Internal Audit Progress Report Sept 2021	17 - 44
6	Trading Companies	
	Item 6 AG Trading Companies	45 - 50
7	One CAM Referral	
	Item 7 AG One CAM Referral	51 - 54
8	Format of Business Board Meetings	
	Item 8 AG - Format of Business Board Meetings - 240921	55 - 58
9	Work Programme and Updated Terms of Reference	
	Item 10 Work Programming Report	59 - 80
10	Corporate Risk Register	
	Item 9 Corporate Risk report	81 - 90
11	Information Governance Update	
	Item 11 Information Governance Update report	91 - 160
12	Date of next meeting:	
	26th November 10:00am at New Shire Hall, Alconbury Weald.	
	AG Draft Minutes 240921 Final	161 - 168

The Audit and Governance Committee comprises the following members:

For more information about this meeting, including access arrangements and facilities for people with disabilities, please contact

The Audit and Governance Committee Role.



The Combined Authority is committed to open government and members of the public are welcome to attend Committee meetings. It supports the principle of transparency and encourages filming, recording and taking photographs at meetings that are open to the public. It also welcomes the use of social networking and micro-blogging websites (such as Twitter and Facebook) to communicate with people about what is happening, as it happens.

Councillor David Brown

John Pye

Councillor Ian Benney

Councillor Graham Bull

Councillor Tony Mason

Councillor Shaz Nawaz

Councillor Mike Sargeant

Councillor Graham Wilson

Clerk Name:	Anne Gardiner
Clerk Telephone:	

Clerk Email:	anne.gardiner@cambridgeshirepeterborough-ca.gov.uk
--------------	--



CAMBRIDGESHIRE & PETERBOROUGH COMBINED
AUTHORITY –
DRAFT MINUTES

AUDIT AND GOVERNANCE COMMITTEE: MINUTES

Date: 30th July 2021

Time: 10:00am

Location: Dance Studio Burgess Events and Conference Centre, One Leisure,
Westwood Road, St Ives PE27 6WU

Present:

Mr John Pye
Cllr Ian Benney
Cllr Tony Mason
Cllr Graham Bull
Cllr Mike Sargeant
Cllr Graham Wilson

Chairman
Fenland District Council
South Cambridgeshire District Council
Huntingdonshire District Council
Cambridge City Council
Cambridgeshire County Council

Officers:

Kim Sawyer
Robert Parkin
Anne Gardiner
Jon Alsop
Daniel Harris
Robert Emery
Suresh Patel

Interim Chief Executive Officer
Monitoring Officer
Scrutiny Officer
Chief Finance Officer (S73 Officer)
Internal Auditors (RSM)
Chief Accountant and Deputy S73 Officer
External Auditors (Ernst & Young)

1. Apologies for Absence and Declarations of Interest

- 1.1 Apologies were received from Cllr Brown.
- 1.2 No declarations of interest were made.

2. Chair's Announcements

- 2.1 The attendance of the Business Board Chair scheduled for this meeting had been deferred due to the outcome at the CA Board when the proposal had been discussed and had failed at the vote due to the Mayor not supporting the proposal. The Chair

advised that a meeting between himself and the Business Board Chair was being arranged to discuss how to take this forward.

- 2.2 The Chair requested that all members of the committee submit their Register of Interest forms to officers as soon as possible as some were still outstanding.
- 2.3 The Chair requested that members of the Committee complete and send to the Scrutiny Officer the Members Skill Set form to help inform future development sessions.
- 2.4 The Chair informed the Committee that the Combined Authority had been approached by members of the CA Board to consider the processes used in the closure of the Combined Authority trading company One CAM. Officers were going to look into this and report back.

The scope would need to be provided to the Committee for them to consider.

This issue had highlighted that there was currently no route for how members could refer matters to the Audit and Governance Committee, and this would be discussed in the work programming paper later in the meeting.

3. Minutes of the last Meeting

- 3.1 The minutes from the meeting held on the 25th June 2021 were agreed as a correct record subject to the following amendment:

Under item 5 – Cllr Sargeant raised a point that the review of the CA governance arrangements and that the Housing Programme in regards to the MHCLG should be looked into.

- 3.2 The Actions from the previous meeting were noted.

4. Combined Authority Board Update

- 4.1 The Committee received the update from the Interim Chief Executive Officer which provided an update on the activities of the CA Board.
- 4.2 The Combined Authority had passed its first Gateway Review; the organisation had received £20m in gainshare funding and to ensure they continued to receive funding the Combined Authority had to demonstrate that they were safe custodians of public money. The government review based the future performance on the past performance and as a result of passing the process the Combined Authority had secured £20m per annum over the next five years. This also meant that any further funding from other government departments would be forthcoming.

In response to a question about the Gateway process the Chief Executive advised that reports were drafted by the Combined Authority and submitted to government, there were also meetings between the ministry and officers. An initial response was provided by government which the Combined Authority had the opportunity to respond to before MHCLG made their final decision.

- 4.3 The Board had agreed to support two new Lead Member Responsibilities, Public Health and Climate Change.
- 4.4 The Board had agreed to the appointment process for two independent persons to handle any code of conduct issues that may arise at the Combined Authority.
- 4.5 The CA Board had considered a report regarding the progress made on the Devolution Deal and had agreed to hold an away day for members to discuss the future vision for the Combined Authority; build relationships with the new Chief Executive and those from the constituent councils.
- 4.6 The CA Board had received a report on the budget and also on the closing down of the One CAM; there had been questions raised around decision making processes

and the use of consultants and the Board had requested that a review into the use of consultants was carried out; in particular reference to the Local Transport Plan.

- 4.7 The Local Transport Plan would be an important issue going forward considering the possible removal of the One CAM as there would need to be a new way to help solve the issues across the region; to unite the north and south of the region, consider ways to relieve congestion, work with external partners such as the GCP, zero emissions buses and possible processes around active travel.
- 4.8 The CA Board received recommendations from the Business Board regarding a performance review and funding for its own assessments.
- 4.9 In regards to the LEP review being done by government; the Chief Executive advised that they had received word from BEIS that the review would now be part of the levelling up white paper due out in Autumn.
- 4.10 In regard to the Affordable Housing Programme there had been a meeting with Cllr Sargeant and the Chair of the Housing Committee, and the Combined Authority were waiting to hear from MHCLG on proposals that had been put forward.
- 4.11 The Chief executive gave an update on the Governance Review and advised that the scope of the review had been increased to also consider ways of working at the Combined Authority, looking at partnerships with constituent councils, how the Board operated and how policies were developed. The full scope would be brought to the Audit and Governance Committee to ensure they were fully engaged.

5. Work Programming Report

- 5.1 The Committee received the report which requested that the committee discuss the suggested ways of developing their work programme.
- 5.2 The following points were raised during the discussion:-

Members requested that referrals could also be received from members of constituent councils.
- 5.3 In response to a question about the list of standing items the Committee would consider throughout the year the Monitoring Officer advised that the list reflected the content within the Terms of Reference for the Committee.
- 5.4 The Horizon Scanning report would be a mechanism for members to review items that could be added to the work programme; it would be important to ensure they fell within the remit of the Committee.
- 5.5 The decision to add an item to the work programme should be a decision for the whole committee.
- 5.6 In response to a question about how the trading companies and the Business Board would be factored in the Monitoring Officer advised that the Committee would receive a report on the Trading Companies at the next meeting and that the governance around the Business Board was covered by the Assurance Framework which was brought to this committee annually to approve.
- 5.7 The Committee discussed the definition of what the Audit and Governance Committee should look at when considering referrals and it was advised that each referral would need to be considered by the Committee to decide whether a review fell within the providence of the committee.
- 5.8 The Committee RESOLVED:

a) that officers should take forward the proposals in the report and provide an up-dated work programme and terms of reference for the committee to agree at their next meeting.

b) to invite the Chief Legal Officer/Monitoring Officer to develop proposals for a formal process of referral to the Audit and Governance Committee by other committees or the Combined Authority Board.

c) that Members from constituent councils should be able to submit referrals to the committee

d) to note the current work programme for the Audit and Governance Committee for the 2021/22 municipal year attached at Appendix 3

Items 6 and 7 contained exempt appendices under Part 1 of Schedule 12A of the Local Government Act 1972, as amended, and it would not be in the public interest for this information to be disclosed - Not for publication by virtue of Paragraphs 3 and 7 of Part 1 of Schedule 12A of the Local Government Act 1972

The Committee AGREED that they would want to go into closed session to discuss the exempt items within the appendix.

The Chair advised that as this was the case he would move items 6 and 7 on the agenda to the end of the meeting to allow the live stream to continue uninterrupted until the Committee went into closed session on these items.

8. External Audit - Results

8.1 The Committee received the report from the External Auditors which requested that they approve the Management Representation Letter 2021 and note the External Auditors report.

8.2 The Chair informed the Committee that the External Auditor was not in a position to sign off the accounts as the auditor of the pension fund providers had not provided the assurances that the External Auditor had requested.

The External Auditor advised that the information had been promised from the pension fund auditor in the next week and there was no reason to suspect it would present any material changes.

8.3 The External Auditor was leaving his role at EY next week and therefore the Committee were advised if they chose to wait until the September meeting to approve the accounts then there would need to be additional work undertaken by the new EY external auditor at an additional cost.

8.4 The External Auditor informed the committee that the audit had gone smoothly; the main focus had been on revenue funded from capital and these had been tested quite significantly.

8.5 The Committee RESOLVED to approve the Management Representation Letter 2020/21 and note the External Auditors report 2020/21.

9. Statement of Accounts and Annual Governance Statement

9.1 The Committee received the report which requested that they approve the Statement of Accounts for 2020/21 and approve the Annual Governance Statement 2020/2021.

9.2 The Chief Finance Officer advised that due to the delay with the information from the pension provider mentioned in the previous item that the committee could approve the accounts and annual governance statement in principle and delegate to the Chair to sign them off once the External Auditor had completed their audit.

9.3 Changes suggested by the Committee at their previous meeting had been implemented and were reflected in the track changed copy of the report.

In response to a question about the withdrawal of the government funding for the Housing Programme the Chief Finance Officer agreed that this could be added to the narrative but that it would have no impact on the accounts.

9.4 The Committee discussed the Annual Governance Statement

9.5 A member raised a query around the level of detail in the report and was advised that much of the detail was included within the exempt information which would be discussed later in the meeting.

9.6 The Committee Agreed in principle to approve the accounts and delegated to Sec 73 Officer and Chair to approve unless any substantial changes were made.

The Committee agreed to approve the Annual Governance Statement subject to the discussions due to be held under item 6 and 7 from the Internal Auditors.

9.7 The Committee thanked Suresh Patel for his work over the past four years and wished him success in his new role.

10. Corporate Risk Register

10.1 The report asked that the Committee note and review the Combined Authority's Corporate Risk Register and recommend any proposed changes for reporting to the next Combined Authority Board meeting for approval.

10.2 An error in the risk register dashboard was noted by members which officers agreed to amend before the next meeting.

10.3 The Committee Agreed that the residual risk for Climate Change should be considered by the CA Board at their next meeting to determine whether the significance of the risk had been properly calibrated.

10.4 The Committee noted the Corporate Risk Register.

11. Appointment of Independent Persons for Member Conduct

11.1 The Committee received the report from the Monitoring Officer which asked members to note the appointment process and role description to recruit two Independent Persons and request that the Chief Legal Officer/Monitoring Officer undertake the work necessary to recruit the Independent Persons.

11.2 The Committee were advised that the CA Board had requested an amendment to the description of the Independent Persons – that they should not be a member of any political party not just an active member.

11.3 The Committee queried the role description as it read more as a Person Specification and requested that a Role Description be brought back to the next meeting for members to consider.

11.4 The Committee questioned whether it was necessary to have the amendment from the CA Board as there could be other memberships which would rule out a potential candidate; the Monitoring Officer advised that the role referred to independence and impartiality which would be tested through the recruitment process.

11.5 The Chair queried whether this could be put on hold until the next meeting and if necessary use Independent Persons from Constituent Councils if a complaint came up; the Monitoring Officer advised that it would be appropriate to get the process started but that the Constituent Councils could be contacted to encourage their Independent Persons to consider applying for the roles.

11.6 The Committee RESOLVED to:

a) note the appointment process and requested that the role description to recruit two Independent Persons be brought back to the next meeting for the committee to review.

b) Ask the Chief Legal Officer/Monitoring Officer to undertake the work necessary to recruit the Independent Persons

6. Items 6 and 7 – Internal Audit – Progress and Annual Report

6.1 At this point in the meeting the internet connection went down and the Internal Auditor was unable to attend via Zoom to present his report and therefore the Committee Agreed to defer items 6 & 7 until the September meeting.

6.2 As there were items of relevance within these reports for the Annual Governance Statement the Committee were unable to review these points.

The Chair called for a vote to delegate to the Section 73 Officer and the Chair to approve the Annual Governance Statement as it stood noting that the officers had responded to changes requested at their previous meeting.

The Vote fell with 2 votes in favour and 3 against.

The Committee RESOLVED not to approve the Annual Governance Statement but defer this until the September meeting. As a result, the Statement of Accounts were not signed off and would need to be reviewed by an alternative auditor before the September meeting.

12. Date of next meeting

12.1 The next meeting would be held on the 24th September 2021, Venue TBC

Meeting Closed: 12:10pm



**CAMBRIDGESHIRE
& PETERBOROUGH**
COMBINED AUTHORITY

Audit and Governance Committee Action Log

Purpose: The action log records actions recorded in the minutes of Audit and Governance Committee meetings and provides an update on officer responses.

Minutes of the meeting 30th July 2021

Minute	Report title	Lead officer	Action	Response	Status
2.4	Chair's Announcements	Robert Parkin	Scope for the referral to consider the closure of the trading company One CAM would be brought to the Committee to consider	Report coming to September meeting	Closed
4.11	Combined Authority Update	Robert Parkin	The full scope of the governance review would be brought to the Audit and Governance Committee to ensure they were fully engaged.	Report coming to September meeting	Closed
5.2	Work Programming	Anne Gardiner	For future work programming items members requested that referrals could also be received from members of constituent councils.	Included in the updated Terms of Reference being brought to September meeting for Committee review.	Closed
5.8	Work Programming	Anne Gardiner	Updated work programme and terms of reference for the committee to be brought to the next meeting including the process for referrals.	Report coming to September meeting	Closed
10.2	Corporate Risk Register	Robert Parkin/Robert Fox	Error on Risk Register Dashboard to be rectified before being presented to the committee at next meeting.	Dashboard rectified	Closed
10.3	Corporate Risk Register	Robert Parkin/Anne Gardiner/Robert Fox	The residual risk for Climate Change should be considered by the CA Board at their next meeting to determine whether the significance of the risk had been properly calibrated.	Report due to go to CA Board in September – will include this recommendation from A&G	Closed
11.6	Appointment of Independent Persons	Robert Parkin/Anne Gardiner	The role description to recruit two Independent Persons be brought back to the next meeting for the committee to review.	Role description to be circulated to members prior to the September meeting	Closed

6.2	Annual Accounts and AGS	Jon Alsop/Robert Emery	Annual Accounts and AGS to be brought back to September meeting for sign off.	Report coming to September meeting	Closed
-----	-------------------------	------------------------	---	------------------------------------	--------

Minutes of the meeting 25th June 2021

Minute	Report title	Lead officer	Action	Response	Status
6.2	Internal Audit Progress Report	Daniel Harris (RSM)	Internal Auditors to include the current work programme in all reports.	Included in July 2021 papers and will be going forward.	Closed
7.4	Draft Statement of Accounts and AGS 2021	Jon Alsop	Officers agreed to check what the increase in governance costs from £17k to £49k were.	Will update the Board at the meeting.	Closed
8.7	Treasury Outturn Report	Rob Emery	Breakdown summary of slippage requests to be provided to the committee.	Apologies to the committee, this will be provided ahead of the meeting.	Open
10.5	Climate Change Commission	Adrian Cannard	Terms of reference for the Climate Change Working group to be brought to the committee for consideration and to request that the working group advise how flooding considerations will be included within the recommendations of the group.	Report to come to November or January meeting	Open
13.2	Work Programme	Anne Gardiner/Rob Parkin	Briefing note on the background of the Trading Companies to be provided to members before the training session in September	Briefing Note provided to members before September meeting.	Closed

Minutes of the meeting on 6th April 2021

Minute	Report title	Lead officer	Action	Response	Status
4.3	Combined Authority Update	Rochelle Tapping	Business Board Chair to be invited to meet with committee once the Business Board had discussed the recommendation on amending the presumption of holding meetings in public.	The Business Board considered the recommendation from the Audit and Governance Committee at its meeting on 19 May 2021. Meeting to be arranged between Chair's to discuss outcome of CA Board discussion to report back to committee in September.	Closed

Minutes of the meeting on 5th March 2021

Minute	Report title	Lead officer	Action	Response	Status
4.4	Assurance Framework	Robert Parkin	A proposal outlining how the Combined Authority would address the oversight arrangements for Trading Companies going forward and demonstrate how these would be effective; drawing on real examples from Nottingham and Croydon Councils would be brought to the committee.	Report and Training Session on Trading Companies scheduled for September 2021	Closed
5.4	Revision to Constitution – Housing Committee	Robert Parkin	Revision to Housing Committee remit to be included in annual review of constitution	Review of constitution is in progress.	Open
8.2	Information Governance Update	Rochelle Tapping	Officers to implement a process to enable experiences with ICT issues to be shared across the constituent councils of the Combined Authority	The CA have a new ICT provider SOCITM which has resolved the issues that had been experienced. Therefore the sharing of experience with other constituent councils was no longer required.	Closed

Minutes of the Meeting on 2nd October 2020

Minute	Report title	Lead officer	Action	Response	Status
7.3	Combined Authority Update	Kim Sawyer	The Chief Executive to provide the Committee with regular updates on the working relationship between the Combined Authority and Greater Cambridge Partnership as part of the CAB updates	Ongoing	Open



**CAMBRIDGESHIRE
& PETERBOROUGH**
COMBINED AUTHORITY

Agenda Item No: 5

Internal Audit Report

To: Audit and Governance Committee

Meeting Date: 24th September 2021

From: Jon Alsop, Head of Finance and S73 Officer

Key decision: Not a key decision

Forward Plan ref: n/a

Recommendations: The Audit and Governance Committee is recommended to:

- a) Receive and note the annual internal audit report for 2020/21 as provided by the Combined Authority's internal auditors, RSM Risk Assurance Services LLP (RSM).
- b) Receive and note the internal audit progress report for 2021/22 as provided by RSM

Voting arrangements: Note only item, no vote required.

1. Purpose

- 1.1. The purpose of the report is for the Audit and Governance Committee to:
- (a) Receive and note the annual internal audit report for 2020/21
 - (b) Receive and note progress being made against the internal audit plan for 2021/22.

2. Background

- 2.1. The Chief Internal Auditor of a Local Authority is required annually to provide their opinion on the overall systems of internal control and their effectiveness.

The Annual Internal Audit Opinion

- 2.2. The Internal Audit Plan for 2020/21 presented by RSM to the Committee in November 2020 stated that “As the provider of the internal audit service we are required to provide an annual opinion on the adequacy and effectiveness of the organisation’s governance, risk management and control arrangements. The annual opinion will be provided to the organisation by RSM Risk Assurance Services LLP at the financial year end.”
- 2.3. The annual opinion should be used to inform the organisation’s annual governance statement.
- 2.4. The internal audit opinion for Cambridgeshire and Peterborough Combined Authority for 2020/21 is as follows:
- 2.5. “The organisation has an adequate and effective framework for risk management, governance and internal control. However, our work has identified further enhancements to the framework of risk management, governance and internal control to ensure that it remains adequate and effective.”
- 2.6. The full report is attached at appendix 1.

Internal Audit Plan 2021/22

- 2.7. RSM presented the internal audit plan for 2021/22 to the Audit and Governance Committee in April 2021.
- 2.8. The attached report provides an update to the Audit and Governance Committee against the internal audit plan for the year.

3. Financial Implications

- 3.1. Internal audit fees are within those agreed as part of the internal audit service contract.

4. Legal Implications

- 4.1. No legal implications have been identified.

5. Other Significant Implications

- 5.1. No other significant implications have been identified.

6. Appendices

- 6.1. Appendix 1 – Internal Audit Annual Report 2020/21 (RSM)
Appendix 2 – Internal Audit update report 2021/22 (RSM)

7. Background Papers

- 7.1. Outline Audit Plan – A&G Committee November 2020

[A&GC Nov 2020 Internal Audit Plan](#)

Internal Audit Plan – A&G Committee April 2021

[Internal Audit Plan A&GC April 2021](#)



CAMBRIDGESHIRE AND PETERBOROUGH COMBINED AUTHORITY

Annual internal audit report 2020/21

16 July 2021

This report is solely for the use of the persons to whom it is addressed.

To the fullest extent permitted by law, RSM Risk Assurance Services LLP will accept no responsibility or liability in respect of this report to any other party.

THE ANNUAL INTERNAL AUDIT OPINION

This report provides an annual internal audit opinion, based upon and limited to the work performed, on the overall adequacy and effectiveness of the organisation's risk management, control and governance processes. The opinion should contribute to the organisation's annual governance reporting.

The opinion

For the 12 months ended 31 March 2021, the head of internal audit opinion for Cambridgeshire and Peterborough Combined Authority is as follows:



Please see appendix A for the full range of annual opinions available to us in preparing this report and opinion.

It remains management's responsibility to develop and maintain a sound system of risk management, internal control and governance, and for the prevention and detection of material errors, loss or fraud. The work of internal audit should not be a substitute for management responsibility around the design and effective operation of these systems.

Scope and limitations of our work

The formation of our opinion is achieved through a risk-based plan of work, agreed with management and approved by the audit and governance committee, our opinion is subject to inherent limitations, as detailed below:

- internal audit has not reviewed all risks and assurances relating to the organisation;
- the opinion is substantially derived from the conduct of risk-based plans generated from a robust and organisation-led assurance framework. The assurance framework is one component that the board takes into account in making its annual governance statement (AGS);
- the opinion is based on the findings and conclusions from the work undertaken, the scope of which has been agreed with management / lead individual;
- where strong levels of control have been identified, there are still instances where these may not always be effective. This may be due to human error, incorrect management judgement, management override, controls being by-passed or a reduction in compliance;
- due to the limited scope of our audits, there may be weaknesses in the control system which we are not aware of, or which were not brought to our attention; and
- our internal audit work for 2020/21 has been undertaken through the substantial operational disruptions caused by the COVID-19 pandemic. In undertaking our audit work, we recognise that there has been a significant impact on both the operations of the organisation and its risk profile, and our annual opinion should be read in this context.

FACTORS AND FINDINGS WHICH HAVE INFORMED OUR OPINION

Our opinion has been informed by seven assurance reviews undertaken during 2020/21. One review concluded with minimal assurance (IT Control Framework Review) and resulted in six high and four medium priority management actions being agreed. We also issued one partial assurance opinion for the Risk Management review.

Five further reviews were undertaken, four of these resulting in reasonable assurance being taken by the Authority for the following reviews:

- Impact of COVID-19 on Project Delivery
- Accounts Payable
- Appointments to Boards and Committees;
- COVID-19 Capital Grants

In addition, our Follow Up review, conducted on a sample of the recommendations from the previous internal auditors concluded that the Authority had made **good progress** in implementing recommendations. We confirmed that seven recommendations had been fully implemented and two had been superseded. We did agree a management action in relation to the monitoring and reporting of management actions agreed, given that this was not formally in place at the time of our review.

We issued one audit where the Authority could take only partial assurance.

For this area, the Authority could take partial assurance that the controls to manage these risks are suitably designed and consistently applied. However, action was needed to strengthen the control framework to manage the identified risks:

Risk Management (1.20.21)

We noted that the Authority was yet to undertake detailed risk management training, specifically in ensuring risks are clear and mitigation plans and actions are specific, measurable, achievable, realistic and time relevant (SMART). In addition, we noted the Authority does not capture evidence of the review and scrutiny of the Corporate Risk Register at an Executive level and had not at the time of the review implemented a reporting framework for risk registers below the Corporate level. We further noted that risk escalation was at the discretion of risk owners and therefore could be subjective and inconsistent.

We also found that minimum frequencies for the review of risks have not been formally documented and noted that as the organisation takes positive steps towards its compliance with the new risk management strategy and processes, it would be equally important to link assurances to individual risks and controls.

Since issuing the final report we have held various meetings with Officers to discuss how CPCA could further develop the risk management control framework and strategy whilst satisfying the issues identified through our review.

We issued one audit where the Authority could take only minimal assurance.

IT Control Framework Review (5.20.21)

Overall, the Combined Authority is at the early stages with respect to the development and operation of an overarching IT control framework. We were advised by the Authorities IT provider that some controls surrounding IT are in place. Further work was however required to address some significant control weaknesses where we concluded improvements were required, in particular regarding IT management experience (including IT contract management) within the Combined Authority, network access and security, patch management, incident response and backups. Furthermore, we noted that policies and procedures were not in place for any IT area, for example IT security, data protection and remote working specifically for the Combined Authority.

We also noted issues with engagement between the Combined Authority and the ICT provider, including the fact that a contract/Service Level Agreement is not in place and periodic meetings were not being held between the Combined Authority and the ICT provider to discuss service performance.

It should be noted that since our fieldwork, we understand the Combined Authority are being supported by an external consultancy provider in respect of the Combined Authority IT control framework.

Since the issue of the draft report, the Combined Authority has changed IT provider. The new providers have been informed of key priorities which include addressing cyber security and business continuity risks.

Topics judged relevant for consideration as part of the annual governance statement (AGS)

The Combined Authority should consider including the 'partial' and 'minimal' assurance opinions in the AGS for the areas identified above together with the actions planned and undertaken to date to improve the weaknesses identified.

The Combined Authority may also wish to consider whether any other significant issues have arisen, including the results of any external reviews, which it might want to consider for inclusion in the AGS. In addition, the current COVID19 pandemic and its impact on the operations of the Combined Authority will obviously need reflecting in the AGS.

THE BASIS OF OUR INTERNAL AUDIT OPINION

As well as those headlines previously discussed, the following areas have helped to inform our opinion. A summary of internal audit work undertaken, and the resulting conclusions, is provided at appendix B.

Acceptance of internal audit management actions

Management have agreed actions to address all of the findings reported by the internal audit service during 2020/21.

Implementation of internal audit management actions

Our follow up of the actions agreed to address previous years' internal audit findings shows that the organisation had made **good progress** in implementing the agreed actions.

We undertook one Follow Up reviews in June 2021 and confirmed that from the nine management actions sampled, seven of these (78 per cent), had been fully implemented with the remaining two actions superseded based on changes to working arrangements. However, we agreed a management action in relation to the monitoring and reporting of action progress/implementation, given that this was not formally in place at the time of our review.

Working with other assurance providers

In forming our opinion, we have not placed any direct reliance on other assurance providers.

OUR PERFORMANCE

Wider value adding delivery

Area of work	How has this added value?
Sector Briefings	Issued briefings relating to the sector within our progress reports presented to the AGC to assist officers and committee members in being informed on the latest developments within the sector.
RSM Business Continuity Planning – COVID-19	We provided details of our response to the COVID-19 pandemic, including the focus of the health and welfare of our clients and staff, our ability to support you in all scenarios and delivery of our planned audit reviews.
Coronavirus: Various briefings and webinars	RSM have delivered a number of webinars and client briefings in relation to Coronavirus (ranging from Government financial support for employers, fraud briefings, HR and Legal Support etc).
Audit and Governance Committee attendance	We have attended all AGC's and where appropriate contributed to the wider agenda.
Webinar invitations	Various invitations have been sent to management to attend webinars to inform of any sector and wider sector updates. Examples include VAT, Employment Tax and COVID-19.

Conflicts of interest

RSM has not undertaken any work or activity during 2020/2021 that would lead us to declare any conflict of interest.

Conformance with internal auditing standards

RSM affirms that our internal audit services are designed to conform to the Public Sector Internal Audit Standards (PSIAS).

Under PSIAS, internal audit services are required to have an external quality assessment every five years. Our risk assurance service line commissioned an external independent review of our internal audit services in 2016 to provide assurance whether our approach meets the requirements of the International Professional Practices Framework (IPPF) published by the Global Institute of Internal Auditors (IIA) on which PSIAS is based.

The external review concluded that 'there is a robust approach to the annual and assignment planning processes and the documentation reviewed was thorough in both terms of reports provided to audit committee and the supporting working papers.' RSM was found to have an excellent level of conformance with the IIA's professional standards.

The risk assurance service line has in place a quality assurance and improvement programme to ensure continuous improvement of our internal audit services. Resulting from the programme, there are no areas which we believe warrant flagging to your attention as impacting on the quality of the service we provide to you.

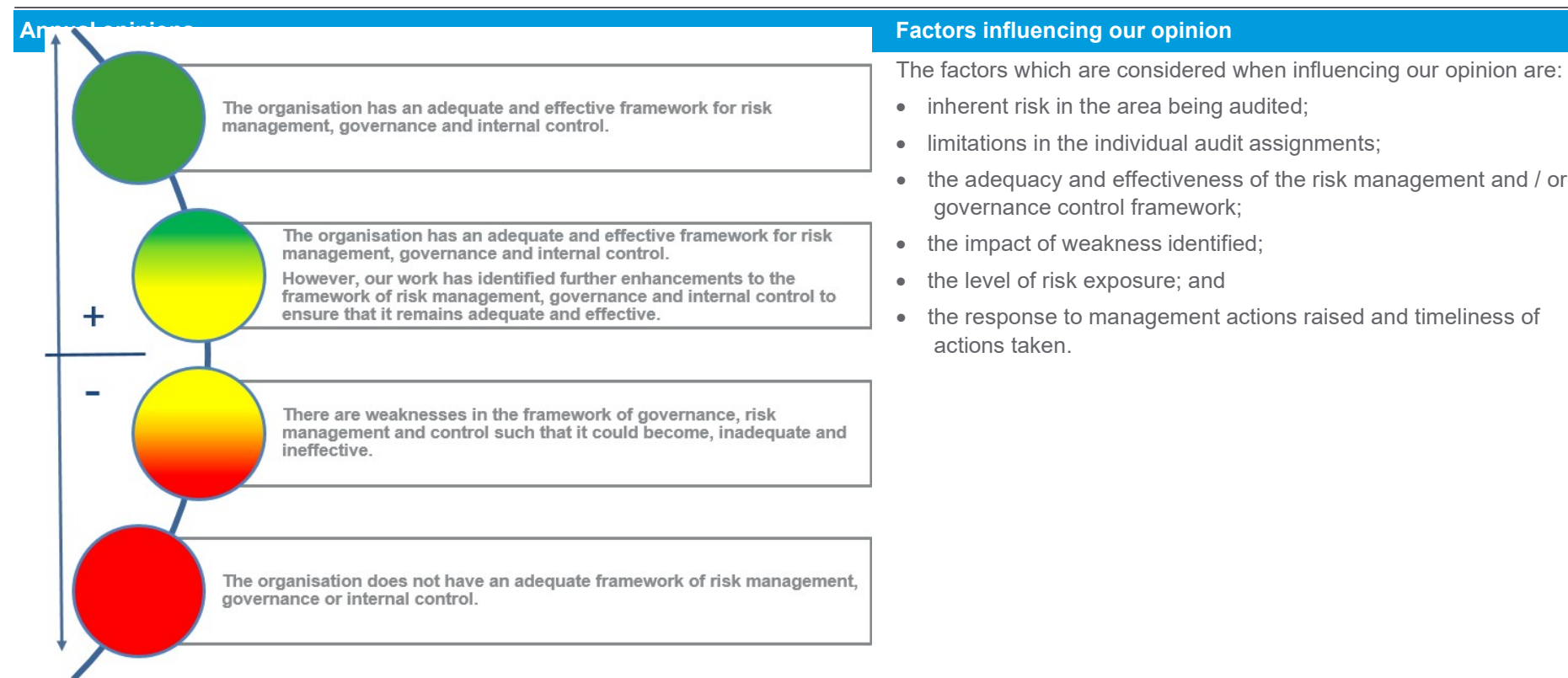
Quality assurance and continual improvement

To ensure that RSM remains compliant with the PSIAS framework we have a dedicated internal Quality Assurance Team who undertake a programme of reviews to ensure the quality of our audit assignments. This is applicable to all Heads of Internal Audit, where a sample of their clients will be reviewed. Any findings from these reviews are used to inform the training needs of our audit teams.

This is in addition to any feedback we receive from our post assignment surveys, client feedback, appraisal processes and training needs assessments.

APPENDIX A: ANNUAL OPINIONS

The following shows the full range of opinions available to us within our internal audit methodology to provide you with context regarding your annual internal audit opinion.



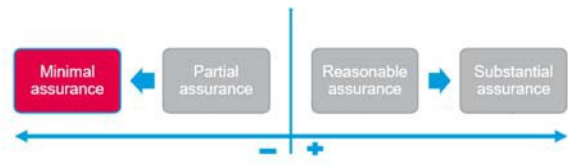
APPENDIX B: SUMMARY OF INTERNAL AUDIT WORK COMPLETED 2020/21

All of the assurance levels and outcomes provided above should be considered in the context of the scope, and the limitation of scope, set out in the individual assignment report.

Assignment	Executive lead	Assurance level	Actions agreed		
			L	M	H
Risk Management 1.20.21 FINAL	Robert Parkin, Chief Legal Officer (Monitoring Officer)	Partial Assurance [●]	1	7	0
Impact of COVID-19 on Project Delivery 2.20.21	Jon Alsop – Head of Finance / Chief Finance Officer	Reasonable Assurance [●]	3	2	0
Appointments to Boards and Committees 3.20.21 FINAL	Robert Parkin, Chief Legal Officer (Monitoring Officer)	Reasonable Assurance [●]	2	2	0
Accounts Payable 4.20.21	Jon Alsop, Chief Finance Officer Robert Emery, Deputy Chief Finance Officer	Reasonable Assurance [●]	5	3	0
IT Control Framework Review 5.20.21	Jon Alsop, Chief Finance Officer Robert Parkin, Chief Legal Officer and Monitoring Officer	Minimal Assurance [●]	0	4	6
Follow Up 6.20.21	Robert Emery – Deputy Chief Finance Officer	Good progress	0	1	0
COVID-19 Capital Grants 7.20.21	Jon Alsop – Chief Finance Officer	Reasonable Assurance [●]	1	2	0

APPENDIX C: OPINION CLASSIFICATION

We use the following levels of opinion classification within our internal audit reports, reflecting the level of assurance the board can take:



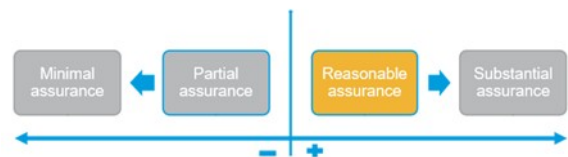
Taking account of the issues identified, the board can take minimal assurance that the controls upon which the organisation relies to manage this risk are suitably designed, consistently applied or effective.

Urgent action is needed to strengthen the control framework to manage the identified risk(s).



Taking account of the issues identified, the board can take partial assurance that the controls upon which the organisation relies to manage this risk are suitably designed, consistently applied or effective.

Action is needed to strengthen the control framework to manage the identified risk(s).



Taking account of the issues identified, the board can take reasonable assurance that the controls upon which the organisation relies to manage this risk are suitably designed, consistently applied and effective.

However, we have identified issues that need to be addressed in order to ensure that the control framework is effective in managing the identified risk(s).



Taking account of the issues identified, the board can take substantial assurance that the controls upon which the organisation relies to manage this risk are suitably designed, consistently applied and effective.

YOUR INTERNAL AUDIT TEAM

Daniel Harris, Head of Internal Audit

Daniel.Harris@rsmuk.com

(+44) 07792 948767

Jay Desai, Client Manager

Jay.Desai@rsmuk.com

(+44) 07436 268278

rsmuk.com

The matters raised in this report are only those which came to our attention during the course of our review and are not necessarily a comprehensive statement of all the weaknesses that exist or all improvements that might be made. Actions for improvements should be assessed by you for their full impact. This report, or our work, should not be taken as a substitute for management's responsibilities for the application of sound commercial practices. We emphasise that the responsibility for a sound system of internal controls rests with management and our work should not be relied upon to identify all strengths and weaknesses that may exist. Neither should our work be relied upon to identify all circumstances of fraud and irregularity should there be any.

Our report is prepared solely for the confidential use of Cambridgeshire and Peterborough Combined Authority, and solely for the purposes set out herein. This report should not therefore be regarded as suitable to be used or relied on by any other party wishing to acquire any rights from RSM Risk Assurance Services LLP for any purpose or in any context. Any third party which obtains access to this report or a copy and chooses to rely on it (or any part of it) will do so at its own risk. To the fullest extent permitted by law, RSM Risk Assurance Services LLP will accept no responsibility or liability in respect of this report to any other party and shall not be liable for any loss, damage or expense of whatsoever nature which is caused by any person's reliance on representations in this report.

This report is released to you on the basis that it shall not be copied, referred to or disclosed, in whole or in part (save as otherwise permitted by agreed written terms), without our prior written consent.

We have no responsibility to update this report for events and circumstances occurring after the date of this report.

RSM Risk Assurance Services LLP is a limited liability partnership registered in England and Wales no. OC389499 at 6th floor, 25 Farringdon Street, London EC4A 4AB.



CAMBRIDGESHIRE AND PETERBOROUGH COMBINED AUTHORITY

Internal Audit Progress Report

24 September 2021

This report is solely for the use of the persons to whom it is addressed.
To the fullest extent permitted by law, RSM Risk Assurance Services LLP
will accept no responsibility or liability in respect of this report to any other party.



CONTENTS

Contents2

1 Key messages3

Appendix A – Progress against the internal audit plan 2020/216

Appendix B – Progress against the internal audit plan 2021/227

Appendix C – Other matters8

Appendix C - Key performance indicators (KPIs) for 2020/21 delivery10

For more information contact11

1 Key messages

The internal audit plan for 2020/21 was approved by the Audit and Governance Committee at the November 2020 meeting, with the internal audit plan for 2021/22 approved at the April 2021 meeting. This report provides an update on progress against that plan and summarises the results of our work to date.

As the developments around Covid-19 will continue to impact on all areas of the organisation's risk profile, we will continue to work closely with management to deliver an internal audit programme which remains flexible and 'agile' to ensure it meets your needs in the current circumstances.

2020/21 Internal Audit Delivery

Three reports have been finalised in relation to:



- Impact of COVID-19 on CPCA delivery of projects;
- IT Control Framework Review; and
- COVID-19 Emergency Active Travel Fund (Capital).

[\[To discuss and note\]](#)

2021/22 Internal Audit Plan



The 2021/22 Internal Audit plan was presented and agreed at a previous Audit and Governance Committee, and we are in the process of undertaking the planning meetings for the audits identified within the programme for 2021/22. The table of audits, and their planned dates have been included in Appendix B, below. [\[To note\]](#)

Other Matters





Annual Governance Statement (AGS) – Please note that we have reviewed the AGS presented to the last Committee meeting we are content that it reflects our opinion and the two negative opinion reports finalised for the 2020/21 internal audit plan. We have suggested a further addition in relation to explaining that management actions have been agreed to address the minimal assurance opinion.

Sector News - We have also included some sector news in Appendix B which highlights some of the current issues being faced in the sector and the areas that the Combined Authority may wish to consider. [\[To note\]](#)

2 Reports

Summary of final reports being presented to this committee

This section summarises the reports that have been finalised since the last meeting.

Assignment	Opinion issued	Actions agreed		
		L	M	H
2020/21 Internal Audit Plan				
Impact of COVID-19 on Project Delivery (2.20/21)	Reasonable Assurance 	3	2	0
IT Control Framework Review (5.20/21)	Minimal Assurance 	0	4	6

Further work is however required to address some significant control weaknesses where improvements are required, in particular regarding IT management experience (including IT contract management) within the Combined Authority, network access and security, patch management, incident response and backups. Furthermore, we noted that policies and procedures were not in place for any IT area, for example IT security, data protection and remote working specifically for the Combined Authority.

We also noted issues with engagement between the Combined Authority and the ICT provider, including the fact that a contract/Service Level Agreement was not in place and periodic meetings were not being held between the Combined Authority and ICT provider to discuss service performance, although we understand this engagement was exited following our audit and a new provider appointed.

Moreover, despite repeated requests to the ICT provider and escalations through the Combined Authority executive management, we were not been provided with any evidence for this review and all of our work is based on enquiry alone.

Grants – COVID-19 Emergency Active Travel Fund (Capital) (8.20/21)

Final report issued

0







0

0

The result of our work is as follows:

I am satisfied that CPCA have paid over the sum of £93,553 to CCC and £34,933 to PCC in relation to the Covid-19 Emergency Active Travel Fund Grant No 31/*. We have been advised by the respective Chief Internal Auditors at CCC and PCC that they have carried out the appropriate investigations and checks, to ensure that in their opinion, in all significant respects, the conditions attached to the Covid-19 Emergency Active Travel Fund Grant No 31/**** have been complied with.***

Appendix A – Progress against the internal audit plan 2020/21

Assignment	Status / Opinion issued	Actions agreed			Target Audit Committee (as per previous audit committee)	Actual Audit Committee
		L	M	H		
Risk Management (1.20/21)		1	7	0	January 2021	January 2021
Impact of COVID-19 on Project Delivery (2.20/21)		3	2	0	Was June 2021, now July 2021	July and September 2021
Appointments to Boards and Committees including those sponsored by the Combined Authority (3.20/21)		2	2	0	Was April 2021, now June 2021	June 2021
Key Financial Controls – Accounts Payable (4.20/21)		5	3	0	Was April 2021, now June 2021	June 2021
IT Controls Assessment (5.20/21)		0	4	6	Was June 2021, now July 2021	July and September 2021
Follow Up (6.20/21)	Good Progress	0	1	0	June 2021	June 2021
COVID-19 Capital Grants (7.20/21)		1	2	0	June 2021	June 2021
Grants – COVID-19 Emergency Active Travel Fund (Capital) (8.20/21)	Final report issued	0	0	0	July 2021	July and September 2021

Appendix B – Progress against the internal audit plan 2021/22

Assignment	Timing / Status / Opinion issued	Actions agreed			Target Audit Committee (as per previous audit committee)	Actual Audit Committee
		L	M	H		
Fraud Risk Assessment	October 2021	0	0	0	January 2022	
HR Policies	October 2021	0	0	0	January 2022	
Adult Education Budget	November 2021	0	0	0	January 2022	
Use of Data	November 2021	0	0	0	January 2022	
Key Financial Controls	January 2022	0	0	0	March 2022	
Subsidiary Governance	January 2022	0	0	0	April 2022	
Risk Management	February 2022	0	0	0	March 2022	
Follow Up	March 2022	0	0	0	April 2022	
Additional audit: Payroll	TBC	0	0	0	TBC	

Appendix C – Other matters

Changes to the audit plan

There have been the following changes to the Audit Plan since the previous meeting;

Audit/Area	Change Proposed
Addition: Payroll	Following discussions with senior management, we have been asked to undertake a review of Payroll following some recent concerns identified. This review will be undertaken in collaboration with subject matter experts, RSM Employer Services Limited. The Audit Committee are asked to note the addition of this audit to 2021/22 internal audit delivery plan.

Annual Opinion 2021/22

The Audit and Governance Committee should note that the assurances given in our audit assignments are included within our Annual Assurance report. In particular the Audit and Governance Committee should note that any negative assurance opinions will need to be noted in the annual report and may result in a qualified or negative annual opinion. We have not finalised any reports to date, but we will provide further updates as the year progresses.

Information briefings and Sector updates

Coronavirus workforce survey

The Local Government Association (LGA) has published the latest findings from its monthly surveys of all councils in England and Wales collecting key workforce data on how the sector is responding to coronavirus. Key findings from the June 2021 survey includes:

- 35 per cent of councils reported recruiting additional staff in the week ending 4 June 2021;
- 84 per cent of councils stated that they were considering 'hybrid working';
- 25 per cent of councils reported that they had furloughed at least one member of staff. In total, responding authorities reported there were 2,682 staff furloughed in the week ending 4 June 2021; and
- councils were asked if they were experiencing significant difficulties recruiting for some posts or not: 114 (61 per cent) said they were.

Independent reviewers appointed for councils requesting financial support

The Ministry of Housing, Communities and Local Government (MHCLG) has appointed independent reviewers to undertake assurance reviews into eight councils, following decisions earlier this year to provide financial support to these authorities. The Chartered Institute of Public Finance and Accountancy (CIPFA) has been appointed to undertake the financial element of these external assurance reviews. The external assurance reviewers will provide a detailed assessment of each councils' financial position and management, making recommendations where necessary of how each council can take action to improve.

Central oversight of arm's-length bodies

The National Audit Office (NAO) has published a report focusing on the role of the centre of government (the Cabinet Office and HM Treasury) in supporting government departments and arm's-length bodies (ALBs). It examines:

- the ALB delivery landscape and the other delivery models available to government;
- the processes in place to support a department as it sets up an ALB;
- how ALBs are overseen by departments and the centre of government; and
- the Cabinet Office's plans for reform of the public bodies landscape.

The report concludes that in 2018/19, ALBs spent £265bn and employed around 300,000 people to deliver the government policies and public services that is dependent on in vital areas such as healthcare, education and housing. The UK's exit from the EU and the coronavirus pandemic have meant the UK government has assumed more responsibility for key functions in areas such as environmental protection and business support. The flexibility of arm's-length arrangements allows public bodies to develop technical expertise and operational independence, but it is important that ALBs remain accountable, are properly managed and have the necessary support. In some areas the centre of government and departments have improved how they work with, and support, ALBs.

The NAO notes that 'the continuing inconsistency in how ALBs are set up and overseen is a barrier to further improvement.' More needs to be done to share lessons across organisations, identify opportunities to improve the complex systems in which policies and services are delivered, and understand when a delivery model is no longer working effectively.

Appendix C - Key performance indicators (KPIs) for 2020/21 delivery

	Delivery				Quality		
	Target	Actual	Notes (ref)		Target	Actual	Notes (ref)
Audits commenced in line with original timescales following scoping	Yes	100%		Conformance with PSIAS and IIA Standards	Yes	Yes	
Draft reports issued within 15 days of debrief meeting	100%	100%		Liaison with external audit to allow, where appropriate and required, the external auditor to place reliance on the work of internal audit	Yes	Yes	
Management responses received within 15 days of draft report	100%	63%	*	Response time for all general enquiries for assistance	2 working days	100%	
Final report issued within 3 days of management response	100%	100%		Response for emergencies and potential fraud	1 working days	N/A	

Notes

* Our first draft report was issued on 11 December 2020 however, due to a combination of the Christmas break responses were not received within 15 days of the draft report.

Two further reports were issued in draft where further internal management discussions regarding the coverage of the review and some wider discussions with stakeholders external to CPCA were required prior to the receipt of formal management responses.

FOR MORE INFORMATION CONTACT

Daniel Harris – Head of Internal Audit

Email: Daniel.Harris@rsmuk.com

Telephone: 07792 948767

Jay Desai – Manager

Email: Jay.Desai@rsmuk.com

Telephone: 07436 268278

rsmuk.com

The matters raised in this report are only those which came to our attention during the course of our review and are not necessarily a comprehensive statement of all the weaknesses that exist or all improvements that might be made. Actions for improvements should be assessed by you for their full impact. This report, or our work, should not be taken as a substitute for management's responsibilities for the application of sound commercial practices. We emphasise that the responsibility for a sound system of internal controls rests with management and our work should not be relied upon to identify all strengths and weaknesses that may exist. Neither should our work be relied upon to identify all circumstances of fraud and irregularity should there be any.

Our report is prepared solely for the confidential use of Cambridgeshire and Peterborough Combined Authority and solely for the purposes set out herein. This report should not therefore be regarded as suitable to be used or relied on by any other party wishing to acquire any rights from RSM Risk Assurance Services LLP for any purpose or in any context. Any third party which obtains access to this report or a copy and chooses to rely on it (or any part of it) will do so at its own risk. To the fullest extent permitted by law, RSM Risk Assurance Services LLP will accept no responsibility or liability in respect of this report to any other party and shall not be liable for any loss, damage or expense of whatsoever nature which is caused by any person's reliance on representations in this report.

This report is released to you on the basis that it shall not be copied, referred to or disclosed, in whole or in part (save as otherwise permitted by agreed written terms), without our prior written consent.



Report title: Combined Authority Trading Companies

To: Audit and Governance Committee

Meeting Date: 24 September 2021

From: Robert Parkin
Monitoring Officer

Key decision: No

Recommendations: The Audit and Governance Committee is recommended to:

a) Comment upon, recommend any changes, and agree the terms of reference of the Committee in relation to the Combined Authority trading companies

Voting arrangements: a simple majority of all Members.

1. Purpose

- 1.1 This report provides the Committee with a draft terms of reference in relation to the review and assessment of the Combined Authority's trading companies in line with the statutory powers invested in the Committee.

2. Background

- 2.1 The Audit and Governance Committee's terms of reference describe its role as to:
- Review and scrutinise the authority's financial affairs
 - Review and assess the authority's risk management, internal control and corporate governance arrangements
 - Review and assess the economy, efficiency and effectiveness with which resources have been used in discharging the authority's functions; and
 - a) make reports and recommendations to the Combined Authority in relation to reviews; and
 - b) implement the obligation to ensure high standards of conduct amongst

Members.

- 2.2 The Combined Authority currently has six trading companies registered with Companies House. These are:

Angle Holdings Limited

Incorporated in September 2019, Angle Holdings was originally set up to be a holding company for all CPCA companies. It is, however, presently the holding company for Angle Developments (East) Limited and the Cambridgeshire and Peterborough Business Growth Service.

Angle Developments (East) Limited

Angle Developments (East) Limited is a housing development company incorporated in September 2019 and is owned in the main by Angle Holdings. It was incorporated with the intention of delivering affordable housing schemes and forming joint ventures with local developers in order to contribute to the housing element of the 2017 devolution deal for Cambridgeshire and Peterborough.

Cambridgeshire & Peterborough Business Growth Service Limited

Incorporated in August 2020 the Cambridgeshire & Peterborough Business Growth Company consists of three major services. These are:

The Business Growth Service: targeting places and companies that will have the most impact on our goal to shift to a more inclusive growth dynamic across sub-economies;

The Inward Investment Service: for a new all-economy foreign direct investment and capital investment promotion service for the promotion of employment space and employment property development opportunities to investors and companies from the UK and overseas; and,

The Skills Service: a digital and physical service connecting business with skills providers and talent, including targeted support to double the number of apprenticeships over five years.

Ownership of the Business Growth Service will shortly transfer to the Combined Authority.

One CAM Limited

One CAM Limited was incorporated in September 2020 and was established as a special purpose vehicle (SPV), as a necessary and best-practice step for delivering the infrastructure intended as part of the CAM.

Peterborough HE Property Company Limited

Incorporated in June 2020 the Peterborough HE Property Company Limited (Propco1) is a special purpose vehicle to deliver the new University on the embankment site in Peterborough. The Propco1 is the SPV for phase 1 of the programme and comprise of the Combined Authority, Peterborough City Council and the academic delivery partner, Anglia Ruskin University.

Peterborough R&D Company Limited

Incorporated In November 2020 for the construction of a Research & Development building which will deliver an Advanced Manufacturing Innovation Eco-System for Peterborough. The company is a joint venture between the CPCA and Photocentric Limited.

3. Terms of Reference

- 3.1 Decisions relating to the Combined Authority trading companies go to the Combined Authority Board, and the Combined Authority Board acts as shareholder. In this role, it carries out a range of roles around oversight, and review. Arrangements are in place in all shareholder agreements for reserved matters to be considered by the Combined Authority Board. Given this process of decision-making and as decisions relating to the companies go to the Combined Authority Board, the Audit & Governance Committee is invited to consider the proposed terms of reference, below, which are aimed at ensuring effective governance by way of bringing a robust and independent approach to the trading companies.
- 3.2 There have been two high profile failings in relation to Local Authority Trading Companies in recent times (Nottingham City Council and London Borough of Croydon) and the findings from these two cases naturally has prompted other local authority bodies such as the Combined Authority to reflect on whether it has confidence in the oversight and audit arrangements in place to ensure that it interest in the good governance of its subsidiaries, and its relationship to them, is promoted.
- 3.3 Considerations around whether the Combined Authority clearly understands the potential financial impacts of the activities and performance of its subsidiary companies are also raised as a result of these two failings. Therefore, there needs to be a robust and ongoing control and due diligence applied to the Combined Authority's investment in these subsidiaries and that includes a clear and defined role for the two statutory Committees of the Combined Authority.
- 3.4 The proposed terms of reference, below, have been considered by the authority's internal auditors who have made comment and suggested amendment, where appropriate. It should be noted the individual trading companies are not directly accountable to the Committee:

Terms of Reference for the Cambridgeshire & Peterborough Combined Authority Audit and Governance Committee in Relation to the Review and Assessment of the Authority's Trading Companies

- a) To ensure that all existing, and any future, trading companies established by the Combined Authority have robust, transparent governance arrangements in place
- b) To assist the Combined Authority in fulfilling its oversight responsibilities in relation to reviewing and monitoring activity
- c) Promote an expectation of high-quality financial information being provided by the trading companies through appropriate review and challenge.
- d) Ensure internal controls and risk management relating to the Combined Authority's trading companies are effective

- e) Commission the Combined Authority's internal audit function to undertake discrete activity relating to the Authority's trading companies, if appropriate.
- f) Ensure the processes for compliance with laws, regulations and codes of practice are in place for the Combined Authority, and also to promote an expectation of the same within the trading companies
- g) Provide assurance that the Combined Authority trading companies are operating in an effective control environment
- h) Ensure the adequacy of arrangements for the management of whistleblowing, complaints, freedom of information requests and compliance within and in relation to the trading companies
- i) Relative to (h) above ensure appropriate, proportionate and independent investigations are undertaken with appropriate follow-up action

4. Significant Implications

4.1 The two high profile failings in relation to Local Authority Trading Companies, referred to in 3.2 above, have potential relevance to the Combined Authority and these are highlighted below:

- The London Borough of Croydon's investments in its subsidiaries involved complex commercial transactions based on business cases taken to cabinet where they received very little challenge, including questioning:
 - The impact of each scheme on the long-term financial position of the council
 - Increased borrowing to schemes within a *Revolving Fund* with little regard to whether previous borrowing to the scheme had delivered intended benefits
 - Whether third parties' financial positions remained sound before providing further borrowing
 - Updated risk assessment to reflect changing market conditions
- Little evidence of members challenging breaches of its own prudential indicators (as part of its Treasury Management Strategy). With the lack of challenge indicating that specialist training for members is needed
- A subsidiary company had not registered as a Shared Ownership Provider indicating a lack of understanding of regulatory requirements
- Breaching of the original business case that the company should not be more than 50% financed by the Council
- Continued delay by a subsidiary being self-financing and repaying loans - to determine whether the council could afford to continue its investments
- Loan covenants not being met by subsidiaries e.g. requiring audited accounts within 90 days of the year end, interest payments due but not paid, loan repayments not received by the due date
- Increasing complexity of the group structures, the interaction between subsidiaries and the longer-term financial impact on the Council not being clearly understood
- A subsidiary being dissolved by compulsory strike off for failure to comply with filing accounts
- The Authority failing to establish adequate arrangements to govern its interests in subsidiaries

- 4.2 Links to the reports of the failings at Nottingham City Council and the London Borough of Croydon can be found here:

[Non-Statutory Review: Nottingham City Council](#)

[Non-Statutory Review: London Borough of Croydon](#)

5. Financial Implications

- 5.1 There are no significant financial implications to this activity.

6. Legal Implications

- 6.1 There are no significant legal implications, beyond those referred to in the body of the report.



Report title: One CAM Referral

To: Audit and Governance Committee

Meeting Date: 24 September 2021

From: Robert Parkin
Monitoring Officer

Key decision: No

Recommendations: The Audit and Governance Committee is recommended to:

- a) To consider, comment upon and agree the scope and methodology of the audit review
- b) Invite the internal auditor, RSM (UK) to commence the review and to report back to a future meeting of the Audit and Governance Committee

Voting arrangements: a simple majority of all Members.

1. Purpose

- 1.1 This paper provides the Committee with a potential scope for an internal audit review of a Mayoral decision.

2. Background

- 2.1 Two members of the Combined Authority Board wrote to officers seeking to invite the Audit and Governance Committee to conduct an audit of the decisions leading to the suspension of activity on the One CAM project. At the time of the referral, there was no formal process of reference – however, the Chair of the Audit and Governance Committee has expressed support for the review, and discussions have taken place with the internal auditor, RSM.
- 2.2 The two Members of the Board have requested: *clarity on the governance surrounding the cessation of work on CAM; who took the decision and how the decision was taken and what*

part/s of the Constitution were being relied upon to ensure the proper governance of actions taken? These questions relate to both the actions of CPCA officers as well as the Mayor.

- 2.3 The focus of the review is as to governance and whether due governance process has been followed.

3. Scope and Methodology

- 3.1 The draft scope, outlined below, has been prepared and shared with the internal auditors, RSM (UK). The Committee is invited to comment upon it:

Review Scope

The scope of this review is restricted to looking at:

- how the Mayor's actions are covered constitutionally in terms of Governance
- what part of the Constitution is being relied upon for the Mayor and/or senior officer delegations to have ordered the ceasing of activity?
- is there any spend/spending commitment from the Combined Authority itself on the CAM programme or has it all been directed through One CAM Ltd?
- whether delegated powers were undertaken correctly in terms of Combined Authority policy
- should the Combined Authority Board have been called to take the decision to cease operations
- any conflict of interest in terms of the Company and the Combined Authority in decision-making

Outside the scope of the review:

- the authority of the Board and the Executive of One CAM Limited

- 3.2 The methodology for the review is outlined below:

Methodology

- desk-based research, ie, collating emails, minutes, Board papers related to the decision, etc.
- interviews
- potential evidence sessions within a Committee setting
- Technical advice made be sought, where appropriate

- 3.3 Once agreed a timescale and milestones for the audit review can be established. Initial considerations have concluded the review will take approximately two months to conduct. This is dependent upon external advice that might need to be provided. The Committee will receive updates on progress.

4. Financial Implications

- 4.1 No immediate financial implications.

5. Legal Implications

5.1 There are no significant legal implications identified currently.

Audit and Governance Committee – Future Format of Business Board Meetings

To: Audit and Governance Committee

Meeting Date: 24th September 2021

Public report: Public Report

From: Robert Parkin
Chief Legal Officer and Monitoring Officer

Recommendations: The Audit and Governance Committee is recommended to:

- a) Note that the Business Board were asked to reconsider the recommendation from the Audit and Governance Committee, 'that there should be a presumption that meetings of the Business Board are carried out in public (unless otherwise determined by the Chair)'.
- b) Note that the Business Board agreed the proposed change in meetings format on 14th September 2021.
- b) Recommend the Combined Authority approve the proposed format change for future Business Board meetings.

1. Purpose

- 1.1 To seek agreement to the proposed format change to allow meetings of the Business Board to be carried out in public (unless otherwise determined by the Chair) and make recommendation to the Combined Authority Board to approve the change.

2. Background

- 2.1 On 5th March 2021, the Audit and Governance Committee considered the draft revised Local Assurance Framework. During that meeting, the Committee expressed concern that

meetings of the Business Board were held in private and requested that the Business Board made recommendations to address this concern. The minutes of that meeting record the following:

Committee members raised concerns around the open and transparent nature of the Business Board. Members felt there was a conflict between the Nolan Principles outlined within the Assurance Framework and the statement that all meetings of the Business Board would be private, except for the Annual General Meeting and other meetings as the Chair deemed necessary. The Committee were advised that there was no requirement within the National Assurance Framework to have the Business Board meetings held in public. The degree of openness was thus a decision for the CA Board, as the Accountable Body. The Committee were strongly of the opinion that the Combined Authority's policy of openness, in line with the Nolan Principles, should apply equally to the Business Board, as to all other Committees. The presumption should be that the Business Board would hold meetings in public, except where the Chair deemed there were reasons of confidentiality not to do so.

2.2 The committee resolved to:

(a) Recommended to the CA Board that the word 'not' be removed at point 4.1.7 of the Assurance Framework to read: 4.1.7: All other meetings of the Business Board shall be open to the public unless determined otherwise by the Chair.

2.3 On 24th March 2021, the Combined Authority considered the revised draft Local Assurance Framework, as recommended by the Audit and Governance Committee. In order to facilitate the decision of the committee detailed at 2.2 above, the Business Board would first need to consider and agree to the proposed change, prior to implementation by the Combined Authority. In consequence, the Combined Authority resolved to:

(f) Refer the recommendation of the Audit and Governance Committee, 'that there should be a presumption that meetings of the Business Board are carried out in public (unless otherwise determined by the Chair)', to the Business Board for comment and consideration.

2.4 On 30th June 2021, the Combined Authority further considered the recommendation from the Business Board that "Business Board meetings retain the current format, holding meetings in private with one public annual meeting each year, recognising the need to improve transparency but not at the expense of compromising confidentiality, and to work earnestly with the Overview and Scrutiny Committee to explore mechanisms to improve that".

2.5 The Mayor commented that prior to his election he had stated that the Business Board should meet in public. He now understood the more nuanced position, but in the course of time he would like to see more public sessions. On being put to the vote the recommendation was lost. It was agreed that Austen Adams (Chair of the Business Board) and John Pye (Chair of the Audit & Governance Committee) would meet to discuss a way forward in terms of a solution.

2.6 This meeting was held on 11th August 2021, and it was agreed that all meetings of the Business Board shall be open to the public unless determined otherwise by the Chair. This enables commercially sensitive and confidential items to be discussed and for open and

frank exchanges of information and views to be expressed that might not otherwise be offered in an open forum. This forms an important element within governance arrangements.

- 2.7 Reference is shown below from the Assurance Framework with the proposed amendment as a tracked change (removal in strikethrough):

4.1.7 All meetings of the Business Board ~~shall not~~ will be open to the public unless determined otherwise by the Chair. This enables transparency while allowing commercially confidential items to be discussed and ~~for open and frank exchanges of information and views to be expressed that might not otherwise be offered in an open forum.~~ This forms an important element within the Combined Authority governance arrangements.

Significant Implications

3. Financial Implications

- 3.1 There are no direct financial implications from this decision, as a decision to meet in public does not require meeting “in-person”. There would be a financial implication to in-person meetings, as appropriate space and AV resources would need to be acquired.

4. Legal Implications

- 4.1 The proposed change (as set out in para 2.7 above) to the Assurance Framework must be approved by the Combined Authority Board.

5. Other Significant Implications

- 5.1 None.

6. Appendices

- 6.1 None.

7. Background Papers

- 7.1 CA Board Meeting – 30th June 2021 - [CMIS > Meetings](#)



**CAMBRIDGESHIRE
& PETERBOROUGH**
COMBINED AUTHORITY

Agenda Item No: 10

Audit and Governance Committee - Work Programming Report

To: Audit and Governance Committee

Meeting Date: 24th September 2021

Public report: Public Report

From: Robert Parkin
Chief Legal Officer and Monitoring Officer

Recommendations: The Audit and Governance Committee is recommended to:

- a) Review and agree the updated terms of reference for the committee at Appendix 1
- b) Note the current work programme for the Audit and Governance Committee for the 2021/22 municipal year attached at Appendix 2
- c) Discuss the top five risks from the Corporate Risk Register and comment on risks needing further review by the Committee .
- d) Consider whether to hold an informal session to receive a *Horizon Scanning* update from Directors.

Voting arrangements: A simple majority of all Members

1. Purpose

- 1.1 The report provides the Committee with the draft work programme for Audit and Governance Committee to note at Appendix 2. Further, it requests that the Committee consider and review the updated terms of reference at Appendix 1, which deals with the referral of matters to the Committee to consider under their work programme.

- 1.2 At their meeting on the 30 July 2021 the Committee agreed they would like their work programme report to include the Top Five Risks from the Corporate Risk Register. This report outlines these risks for consideration.

2. Background

- 2.1 At the Audit and Governance Committee meeting of 25 June 2021 the Committee agreed that the Monitoring Officer would work with the Chair to develop ideas around how the Committee would develop their work programme. This included providing an updated terms of reference for referring matters to the committee and adding the top five risks from the Corporate Risk Register to the report for the Committee to consider.
- 2.2 The updated Terms of Reference are at Appendix 1 for review and approval.
- 2.3 The Committee requested that the top five risks from the Corporate Risk Register were included in the work programme report. This is to enable the Committee to consider whether these needed any further review. As there were two risks with the same score we have included both and there are therefore 6 top risks this month.

Top Five Risks – CPCA

Risk ID	Cause	Effect	Likelihood	Impact	Residual Score
1	External delivery partners unable to deliver on agreed commitments to CPCA projects	Projects are not delivered on time, budget, or to the required standard.	3	4	12
14	Covid-19 Pandemic (A)	Potential absence of significant numbers of Combined Authority staff undermining the ability to transact the operational business of the Combined Authority	3	4	12
16	Covid-19 Pandemic (B)	Economic impact of lockdown in response to Covid-19, may have implications for future government funding and for economic activity within the Combined Authority area in the short term.	3	4	12
19	Covid -19 Pandemic (C)	Economic impact of lockdown in response to Covid-19, may have implications for future government funding and for economic activity within the Combined Authority area in the long term.	5	2	10
17	Unbudgeted increases in cost for highways and transport schemes funded by the Combined Authority and delivered by partner agency	The unplanned increases in budget prejudice the Combined Authority's ability to manage its finances and could ultimately prejudice delivery of the Combined Authority's Business Plan and a balanced budget.	3	3	9
21	MHCLG Review of £100m Housing programme	£170m programme has shortage of anticipated capital and significantly	3	3	9

		reduced time and capability to deliver target of 2000 houses and the £100m programme within the £170m. Potentially significant reputational damage to CPCA housing programme likely.			
--	--	--	--	--	--

2.4 The Committee agreed that they would like to receive a Horizon Scanning report with detail from the different Directorates at the CPCA and the Committee are asked to consider if they would like an informal session to be arranged to meet and discuss this report with the relevant directors in October or if they would rather receive this report at their November meeting.

2.5 The current work programme is attached at Appendix 2 for members to note. Members are asked to note the additional meeting on 12th November 2021 to consider the Constitution for the CPCA and a virtual workshop on the same matter on the 28th October 2021.

3. Financial Implications

3.1 None

4. Legal Implications

4.1 None

6. Appendices

6.1 Appendix 1 – Updated Terms of Reference - A&G Committee

6.2 Appendix 2 – A&G Work programme

7. Background Papers

7.1 [Audit and Governance Minutes 25th June 2021](#)

7.2 [Audit and Governance Minutes 30th July 2021](#)

Audit and Governance – Referral Process

8. Requests to Audit and Governance

8.1. The Mayor or Combined Authority Board may ask the Committee to review any of its functions including:

- a) the authority's financial affairs;
- (b) the authority's risk management, internal control and corporate governance arrangements;
- (c) the economy, efficiency and effectiveness with which resources have been used in discharging the authority's functions;

9. Reference of Matters to Committees

9.1. Any of the following may request a matter to be included on the agenda of the Audit and Governance Committee provided it is relevant to the functions of the Combined Authority and not an excluded matter:

- (a) any Member of the Audit and Governance Committee;
- (b) any Member of the Combined Authority; and
- (c) any Member of a Constituent Council of the Combined Authority.

9.2. An "excluded matter" means any matter which is a local crime and disorder matter.

9.3. The request must be submitted to the Monitoring Officer who will arrange for the item to be placed on the agenda of the next available meeting. The request should state why the Member considers it appropriate for the Committee to exercise any of these powers in relation to the matter and the Committee must have regard to these reasons.

9.4. If the Committee decides not to exercise any of its powers it must notify the referring Member of its decision; and the reasons for it.

9.5. The Committee must provide the Member with a copy of any report or recommendations which it makes in connection with the matter.

AUDIT AND GOVERNANCE COMMITTEE WORK PROGRAMME 2021/22

Meeting Date 2020/21	Item	COMMENTS
DEVELOPMENT SESSION: TRADING COMPANIES		
24 Sept 2021 Venue: TBA	Combined Authority Board Update	Standing item on the agenda when a chief officer or by agreement once a year the Mayor for the Combined Authority provides an update on the activities for the authority.
	Minutes of the previous meeting	Standing item on the agenda for the committee to agree the minutes from the last meeting.
	Corporate Risk Register	Standing item by request of the committee to be considered at each meeting.
	Work Programme & Update Terms of Reference	Standing item for the committee to consider their upcoming work programme.
	Internal Audit – Progress Report	Report from the Internal Auditors to provide an update on the progress of the current internal audits.
	External Audit – Annual Audit Letter	The Committee receive the annual audit letter which communicates the key issues arising from external auditors work in carrying out the audit of the statement of accounts for the Cambridgeshire and Peterborough Combined Authority.
	Trading Companies	The Committee requested that a report on how the

		governance of Trading Companies would be arranged.
	Information Governance Update	Bi annual update on governance issues including FOI, Complaints, incidents of fraud and whistleblowing.
	One CAM Referral	
	Format of Business Board Meetings	
	Annual Accounts and AGS	Deferred from July meeting
Meeting Date	Item	Comment
28th October 2021 (Virtual)	Informal Session – Constitution Review	Committee to review the updated constitution
12th November 2021	Constitution Review	Committee to review the updated constitution
Meeting Date	Item	Comment
DEVELOPMENT SESSION: ROLE OF AUDIT ON MAJOR PROJECTS		
26th November 2021	Combined Authority Board Update	Standing item on the agenda when a chief officer or by agreement once a year the Mayor for the Combined Authority provides an update on the activities for the authority.
	Minutes of the previous meeting	Standing item on the agenda for the committee to agree the minutes from the last meeting.
	Corporate Risk Register	Standing item by request of the committee to be considered at each meeting.
	Work Programme	Standing item for the committee to consider their upcoming work programme.

	Internal Audit – Progress Report	Report from the Internal Auditors to provide an update on the progress of the current internal audits.
	External Audit – Draft Audit Plan	The Committee receive the draft Audit Plan and comment whether the planned audit is aligned with the Committee's expectations.
	Treasury Management Strategy Update	The Committee receive the report which provides the Audit and Governance Committee with an update on the Combined Authority (CPCA)'s Treasury Management Strategy.
	Assurance Framework	Committee agreed in May 2019 that the A/Framework be presented to Committee on 6-month basis.
	Guidance on Accounts	Report to come to Committee with an update on what guidance had been received from government on how to simplify accounts.
	Adult Education Budget	
	Terms of Reference for the Climate Change Working group	Terms of reference for the Climate Change Working group to be brought to the committee for consideration and to request that the working group advise how flooding considerations
	Governance Review	
28th January 2022	RESERVE MEETING	

Meeting Date	Item	Comment
DEVELOPMENT SESSION: A&G COMMITTEE SELF ASSESSMENT		
11 th March 2022	Combined Authority Board Update	Standing item on the agenda when a chief officer or by agreement once a year the Mayor for the Combined Authority provides an update on the activities for the authority.
	Minutes of the previous meeting	Standing item on the agenda for the committee to agree the minutes from the last meeting.
	Corporate Risk Register	Standing item by request of the committee to be considered at each meeting.
	Work Programme	Standing item for the committee to consider their upcoming work programme.
	External Audit – Audit Plan	The Committee receive and approve the final audit plan prepared by the external auditors
	Internal Audit Plan:	Details of audit activity for the following year.
	Treasury Management Strategy Summary	The Committee receive the report asks for comments comment on the draft Treasury Management Strategy.
	Assurance Framework	The Assurance Framework is a set of systems, processes and protocols, which along with standing orders, financial regulations, departmental procedures, and codes of practice is linked in a hierarchy of management and financial control procedures, which clearly define the responsibilities of members and the duties of the

		CPCA's officers, consultants and partners. – Approved annually.
	Information Governance Update	Bi annual update on governance issues including FOI, Complaints, incidents of fraud and whistleblowing.
Meeting Date	Item	Comment
27 May 2022	Combined Authority Board Update	Standing item on the agenda when a chief officer or by agreement once a year the Mayor for the Combined Authority provides an update on the activities for the authority.
	Minutes of the previous meeting	Standing item on the agenda for the committee to agree the minutes from the last meeting.
	Corporate Risk Register	Standing item by request of the committee to be considered at each meeting.
	Work Programme	Standing item for the committee to consider their upcoming work programme.
	Occurred Meetings – Work Programmes	
19 July 2019 Fenland District Council	Internal Auditors Annual Report	The Committee considered and endorsed the Annual Report and Opinion from Internal Audit for the year ended 31st March 2019
	Statement of Accounts 2018/19 and External Audit Final Results	The Committee resolved that: i) That the Chief Executive circulate the draft statutory notice to the members of the Audit and Governance Committee prior to publication. ii) That the Chief Executive liaise with all affected

	<p>constituent Councils and send a letter to government expressing their dissatisfaction with the auditors performance and the impacts this has had on each Council.</p> <p>iii) That the Chair of the Audit and Governance Committee write to the Partner leading the Ernst and Young Government and Public Sector Assurance team expressing the Committee extreme disappointment.</p> <p>iv) That the Committee receive and approve, in principle, the final Statement of Accounts.</p> <p>v) That the Committee agree to the additional recommendations below:</p> <p>a) Note that the Combined Authority's external auditors are not able to guarantee that they will have completed their audit of the accounts for 2018/19 before the statutory deadline of 31 July 2019 for the publication of the statement of accounts together with any certificate or opinion from the external auditors;</p> <p>b) Note that if it is not possible to publish the statement of accounts on time the law requires the Combined Authority to publish as soon as reasonably practicable on or after the deadline a notice stating that it has not been able to publish the statement of accounts and its reasons for this;</p>
--	---

	<p>c) Authorise the Chief Finance Officer in consultation with the Chair of Audit and Governance Committee, as and when the final Audit Opinion is provided by the external auditors, to make any minor amendments to the statement of accounts arising from the final Audit Opinion and to authorise the Chief Finance Officer and Chair of Audit and Governance to then sign and publish the statement of accounts together with any certificate or opinion from the external auditors;</p> <p>d) In the event that amendments arising from the final Audit Opinion would constitute a “material adjustment” to the final accounts as defined in the external auditor’s final audit plan a further report is to be brought to Committee; and</p> <p>e) That the Committee receive and approve the Annual Governance Statement 2018/19 as included within the statement of accounts.</p>
Chairman’s Annual Audit Report	The Annual Report of the Chair of the Committee be submitted to the Combined Authority Board was approved.
Internal Audit Plan	The Committee considered and endorsed the Annual Report and Opinion from Internal Audit for the year ended 31st March 2019.
Value for Money Report	The Committee noted the Combined Authority’s approach to delivering value for money.
Treasury Management Annual Report	The Committee reviewed the actual performance for the year to 31st March 2019, against the

		adopted prudential and treasury indicators.
	Human Resources Risk Reduction Update	The Committee noted the update.
	Work Programme	The Committee agreed updates to the work programme and noted the report.
Meeting Date 2019/20	Item	COMMENTS
27 September 2019 Cambridge City Council	Audit Results Reports & Statement of Accounts 2018/19	The Committee received the audit results report for the year ended 31st March 2019.
	Transport Acceleration and Risk Report	The Committee noted the officers' assessment of the impact of the accelerated delivery strategy on project risk and the wider measures put in place by the Authority to manage project risk.
	Medium-Term Financial Plan and Business Plan	The report was noted.
	Combined Authority Board Update	The Committee noted the update.
	Business Board Update	The Committee noted the priorities and objectives of the Business Board.
	Internal Audit Update	The progress report from Internal Audit was considered. Internal Audit would provide timelines and progress indicators in future reports and seek The Committee's approval to any programme changes.
	Governance Review Report	The proposed new governance arrangements for the Combined Authority had been considered and the Committee's Work Programme be amended to include a future report to the Committee reviewing the effectiveness of the proposed new governance arrangements.
	Risk Register and Performance Update	The Committee noted the Performance Reporting

		<p>processes that are in place for the Combined Authority.</p> <p>The Committee requested that the Performance Reporting Dashboard is presented to the Board on a quarterly basis and recommend any proposed changes be noted.</p> <p>The Committee requested that the proposed changes to the Corporate Risk Register be reported to the next Board meeting for approval.</p>
	Report on Freedom of Information, Whistleblowing and Fraud	The Committee would advise how the Combined Authority communicated the Whistleblowing Policy and encouraged its use.
	Response to National Audit Office Consultation	The proposed changes to the Code of Audit practice and the potential impact on reporting to the Committee for local audit work was noted.
	Work Programme	The update was noted.
Meeting Date 2019/20	Item	COMMENTS
16 December 2019 South Cambridgeshire District Council	Assurance Framework	<p>A paper will be produced for Audit & Governance Committee meeting in March 2020.</p> <p>The Committee noted the revised Assurance Framework</p>
	Corporate Risk Register	The proposed revised Strategy and changes to the Corporate Risk Register were recommended.
	Data Protection Policy	<p>An update from the Data Protection Officer be put on Audit & Governance Committee Work Programme for December 2020.</p> <p>That the Combined Authority would keep an eye on implications on data protection after Brexit.</p>

		The Data Protection Policy report was recommended
	Internal Audit Progress Report	<p>That an update report be brought back to Audit & Governance Committee in March 2020, including a procedure for urgent items.</p> <p>That a reminder email be sent to Members regarding themes for internal auditors for the following year.</p> <p>The Committee noted the report.</p>
	Adult Education Budget and Assurance Programme	<p>An annual insight to be received by the Committee every year.</p> <p>A briefing session to be organised for the Committee in summer/autumn 2020.</p> <p>The Adult Education Budget Audit and Assurance Programme, along with the arrangements, was noted.</p>
	Treasury Management Strategy Update	The update was reviewed by the Committee.
	Combined Authority Board Update	The Committee noted the update.
	Work Programme	The Committee agreed updates to the work programme and noted the report.
Meeting Date 2020/21	Item	COMMENTS
26 May 2020 Remote Meeting	Confirmation of Membership of the Audit & Governance Committee	<p>Membership was the same as in the last municipal year and there had been no changes amongst substitute members. The Committee noted Fenland DC Annual General Meeting was to be held on 17 June, which could signal change in Fenland DC membership of the Committee.</p>
	Combined Authority Board Update	The Committee noted the update.

	Statement of Accounts 2019/20	The statement of accounts to be presented at the 31 July 2020 meeting of the Committee will be circulated to members two-weeks in advance of the meeting.
	External Audit Update	A further report will be received at the 31 July 2020 meeting of the Committee.
	Internal Audit Update	The Internal Audit with opinion be received at the 31 July 2020 meeting of the Committee.
	Draft Annual Report of the Chair of the Audit & Governance Committee	The report was approved by the Committee for submission to the CA Board meeting on 5 August 2020, subject to the correction of a typographical error.
	Corporate Risk Register	The Committee recommended climate change is included on the on the Risk Register in future.
	Complaints Procedures	The Committee noted the revised procedures and, with the addition of the contact details of 'street scene' issues for the borough, city and district councils, approve them to the CA Board.
	Treasury Management Strategy	The Committee noted the strategies.
	Trading Companies	A development session on the trading companies be held, possibly in autumn 2020.
	Revised Guide for Project Management	The Committee received and noted the revised guide.
	Work Programme	The Committee requested greater clarity on the work programme for future meetings.
	Urgent Item: Lancaster Way	The Committee responded positively to the request for an independent review. and that this has no impact on the delivery of the project. The Committee is open to an Extraordinary meeting, if necessary, with the proviso that sufficient time is afforded to enable the Committee to have all the background information it requires.

Meeting Date 2020/21	Item	COMMENTS
31 July 2020 Remote Meeting	Appointment of a Vice-Chairman of the Audit & Governance Committee	A Vice-Chairman of the Committee would be appointed at the meeting on 31 July as the Combined Authority Board Annual Meeting was not until 3 June and a decision on a Vice-Chairman appointment would be ratified at that meeting.
	Combined Authority Board Update	Standing item on the agenda when a chief officer or by agreement once a year the Mayor for the Combined Authority provides an update on the activities for the authority.
	Minutes of the previous meeting	Standing item on the agenda for the committee to agree the minutes from the last meeting.
	Corporate Risk Register	Standing item by request of the committee to be considered at each meeting. The report to be presented to the 31 July 2020 meeting of the Committee to include the top three to four risks that are improving/getting worse.
	Work Programme	Standing item for the committee to consider their

		upcoming work programme.
	Internal Audit 2020/21	A separate paper on how the Combined Authority is to take Internal Audit forward after the Service Level Agreement with Peterborough City Council concludes was requested for this 20 meeting.
	Internal Audit – Annual Report	A report provided by the Internal Auditors on the effectiveness of the Authority's systems of governance; risk management and internal control.
	External Audit Final Results	The Committee receive the audit results report from the external auditors.
	Annual Governance Statement	Explains how the Combined Authority has complied with the Local Code of Governance and meets the requirements of the Accounts and Audit (England) Regulations 2015 Regulation 6.1(b) – usually received along with the Annual Financial Report.
	Draft Financial Statements 2019/20	The Committee receives the report which asks them to: a) approve the audited Statement of Accounts 2017/18 b) Receive and approve the Annual Governance Statement 2017/18
	Independent Commission on Climate Change	Committee to receive a report on the procedures undertaken in the appointment of the Independent Chair of the Commission
Meeting Date 2020/21	Item	COMMENTS
2 October 2020	Combined Authority Board Update	Standing item on the agenda when a chief officer

Venue: TBA		or by agreement once a year the Mayor for the Combined Authority provides an update on the activities for the authority.
	Minutes of the previous meeting	Standing item on the agenda for the committee to agree the minutes from the last meeting.
	Corporate Risk Register	Standing item by request of the committee to be considered at each meeting.
	Work Programme	Standing item for the committee to consider their upcoming work programme.
	Internal Audit Plan 2020/21	Report from the Internal Auditors on the Internal Audit Plan for the municipal year.
	Financial Statement 2019/20 and External Audit Update	
	Treasury Management Strategy Review	The Committee receive the report which review the current performance against the prudential indicators included within the Treasury Management Strategy.
27 November 2021 Virtual Meeting		
	DEVELOPMENT SESSION	VALUE FOR MONEY
	The Mayor of the Combined Authority	Mayor James Palmer will be in attendance
	Combined Authority Board Update	Standing item on the agenda when a chief officer or by agreement once a year the Mayor for the Combined Authority provides an update on the

		activities for the authority.
	Lancaster Way Update	
	Minutes of the previous meeting	Standing item on the agenda for the committee to agree the minutes from the last meeting.
	Corporate Risk Register	Standing item by request of the committee to be considered at each meeting.
	Work Programme	Standing item for the committee to consider their upcoming work programme.
	Internal Audit: Internal Audit Plan	Report from the Internal Auditors to provide an update on the progress of the current internal audits.
	External Audit and Opinion 2019/20	To receive the External Audit and Opinion from Ernst & young for the previous financial year.
	End of Year Financial Statements 2019/20	
	Adult Education Budget	



Report title: Review of Corporate Risk Register & Risk Management Strategy

To: Audit and Governance Committee

Meeting Date: 24 September 2021

From: Robert Parkin
Monitoring Officer

Key decision: No

Recommendations: The Audit and Governance Committee is recommended to:

- a) Note and review the Combined Authority's Corporate Risk Register (Appendix 1)
- b) Recommend any proposed changes to the Corporate Risk Register to be reported to the next Combined Authority Board meeting for approval.

Voting arrangements: Item a) Note only, no vote

Item b) a simple majority of all Members.

1. Purpose

- 1.1 The Audit and Governance Committee's terms of reference include monitoring the Combined Authority's risk management arrangements including the risk register.
- 1.2 This report provides the Committee with an update on the Corporate Risk Register.
- 1.3 In the interests of good governance, the Committee is requested to review the Corporate Risk Register and suggest any changes they would like to put forward as a recommendation to the Combined Authority Board.

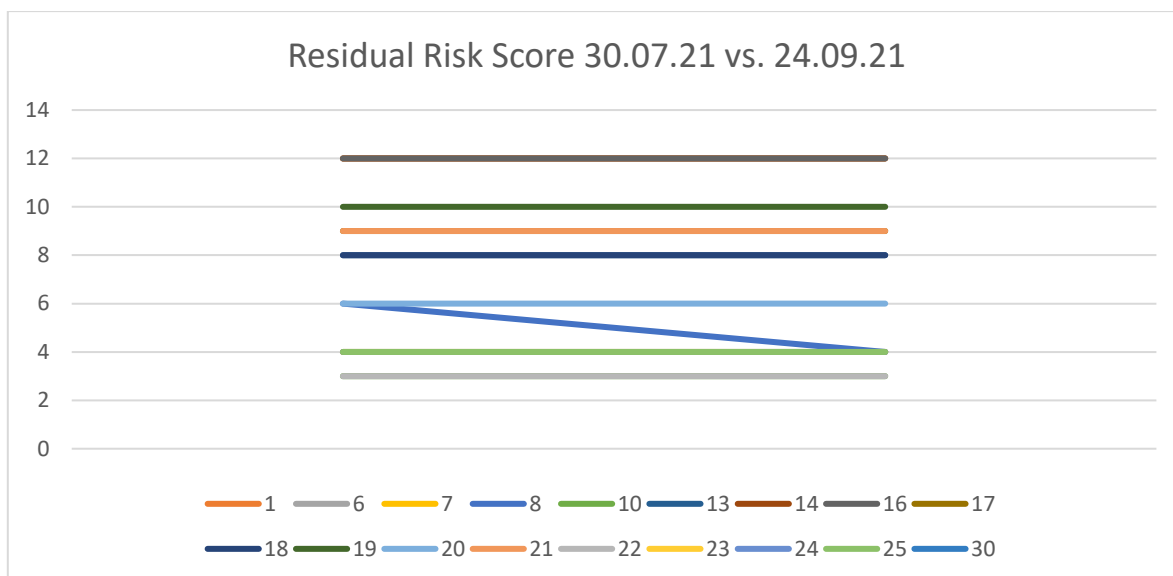
2. Background

- 2.1 The Corporate Risk Register is populated by reference to individual project risk assessments and over-arching corporate risks.
- 2.2 The Corporate Risk Register is reviewed by the Corporate Management Team, any risks which arise, or which become more significant between their meetings are escalated to the next Corporate Management Team meeting.
- 2.3 The same risk register template and terminology are used by all Project Managers during the reporting process for each project. Any risks that score over the agreed threshold on an individual project register will then also appear on the main risk register so that it can be monitored accordingly. Again, the report of the internal auditor on risk includes some recommendations around the corporate risk register.
- 2.4 Officers are currently working with RSM to examine the current Risk Strategy, and to work with the Corporate Management Team to ensure that it represents an effective and efficient approach which fits the needs of the Combined Authority. Once this work is concluded, any revisions will be reported to this committee, and (once adopted) the revised Risk Strategy will be the subject of training for officers across the organisation.

Significant Implications

- 2.5 Directors and directorates have reviewed the risk register and affirmed the currency of entries and considered the necessity for new items. New items are discussed at meetings of the CPCA Corporate Management Team.
- 2.6 Risk ID 21 – MHCLG Review of £100m Housing Programme:
The mitigation plans and actions on this risk have been amended following meetings with MHCLG.
- 2.7 Risk ID 27 – One or more constituent councils issuing s.114 notices:
This risk was discussed at the Combined Authority Corporate Management Team meeting on 8 September and this risk has now been merged into Risk ID 1 as the risk associated with it are inherent within Risk ID 1.
- 2.8 Risk ID 29 – Financial Services Level Agreement with Peterborough City Council is out-of-date:
This risk was escalated by the Chief Finance Officer and presented on the risk register at the previous meeting of the Committee on 30 July 2021. This risk has now been downgraded and, thus, deleted from the register.
- 2.9 Risk ID 30 – Insufficient Internal Resource to Deliver the Authority's Priorities:
This risk has been escalated by the Director of Delivery and Strategy and relates to some lines of work currently being either un- or under-resourced.
- 2.10 The Committee agreed at its last meeting that the residual risk for Climate Change (Risk ID 18) should be considered by the CA Board at their next meeting to determine whether the significance of the risk had been properly calibrated. This meeting will take place on 29 September 2021 and will be reported back to this Committee.

- 2.10 Below is a graph demonstrating the changes in residual risk score from the previous Audit and Governance Meeting on 30 July 2021 to the current Audit and Governance meeting. This reflects the changes noted above.



3. Financial Implications

- 3.1 All of the work has been carried out in-house, therefore, there are no significant financial implications to this activity.

4. Legal Implications

- 4.1 No significant legal implications.

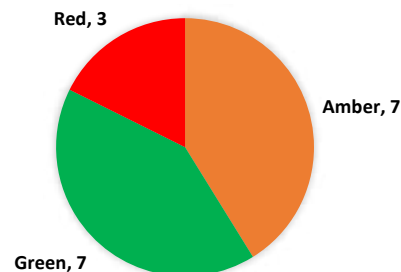
6. Appendices

- 6.1 Appendix 1 – Corporate Risk Dashboard
- 6.2 Appendix 2 – Corporate Risk Heat Map
- 6.3 Appendix 3 – Corporate Risk Register

Risk ID	Risk Event	Risk Status	Residual RAG Score			Movement
			Impact	Likelihood	Score	
1	External delivery partners do not meet deadlines, budget or qualitative requirements of their agreements with the Combined Authority.	Open	4	3	12	↔
6	Lack of structural resilience / insufficient internal resources	Open	1	4	4	↔
7	Potential impact of Brexit on delivery of the Combined Authority's Growth Ambition Programme in the short term.	Open	2	2	4	↔
8	Ambitious and long stalled programmes can not proceed due to lack of government funding and or private investment. The levelling up fund has been announced and provides a £4b opportunity for CPCA bid a list is being prepared.	Open	2	2	4	↓
10	Absence of Resource Planning & Financial Management	Open	3	1	3	↔
13	Access to Gainshare funding called into question by the Gateway Review evaluation of Gainshare	Open	4	2	8	↔
14	Disruption to the operation of the Combined Authority	Open	4	3	12	↔
16	Disruption of the delivery of the Combined Authority objectives in regard to the short term economic objectives	Open	4	3	12	↔
17	Unplanned significant increases in costs lead to requests for additional funding to the Combined Authority to enable schemes to proceed.	Open	3	3	9	↔
18	Climate change related events, policies and political pressures e.g. policy designed to reduce carbon emissions that restricts growth	Open	2	4	8	↔
19	Disruption of the delivery of the Combined Authority objectives in regard to the long term economic objectives	Open	2	5	10	↔
20	Potential impact of the new Trade Deal on delivery of the Combined Authority's Growth Ambition Programme in the long term	Open	3	2	6	↔
21	Up to £45m of Government funding not provided, change of end date of £100m Housing Programme from 31st March 2022 to 31st March 2021 and potential programme loss of 243 housing units at Northstowe which MHCLG may not recognise.	Open	3	3	9	↔
22	Grant funding which is expected to be treated as capital expenditure is required to be treated as revenue expenditure by CPCA, as a result of a determination by a partner delivery authority.	Open	3	1	3	↔
23	Shortfall in the provision of an adequate ICT platform for future need - including software and systems, and equipment. Failure to have access to an application/system needed for the delivery of the CPCA project, programme, or service.	Open	1	4	4	↔
24	Changes in Political Management and change in priorities for the CPCA	Open	2	2	4	↔
25	No access to finance systems	Open	2	2	4	↔
30	Insufficient internal resource to deliver the Authority's priorities	Open	2	4	8	↔

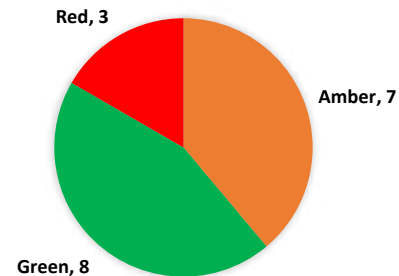
Total RAG Count - Meeting X

Total RAG Count - Meeting 30.07.21

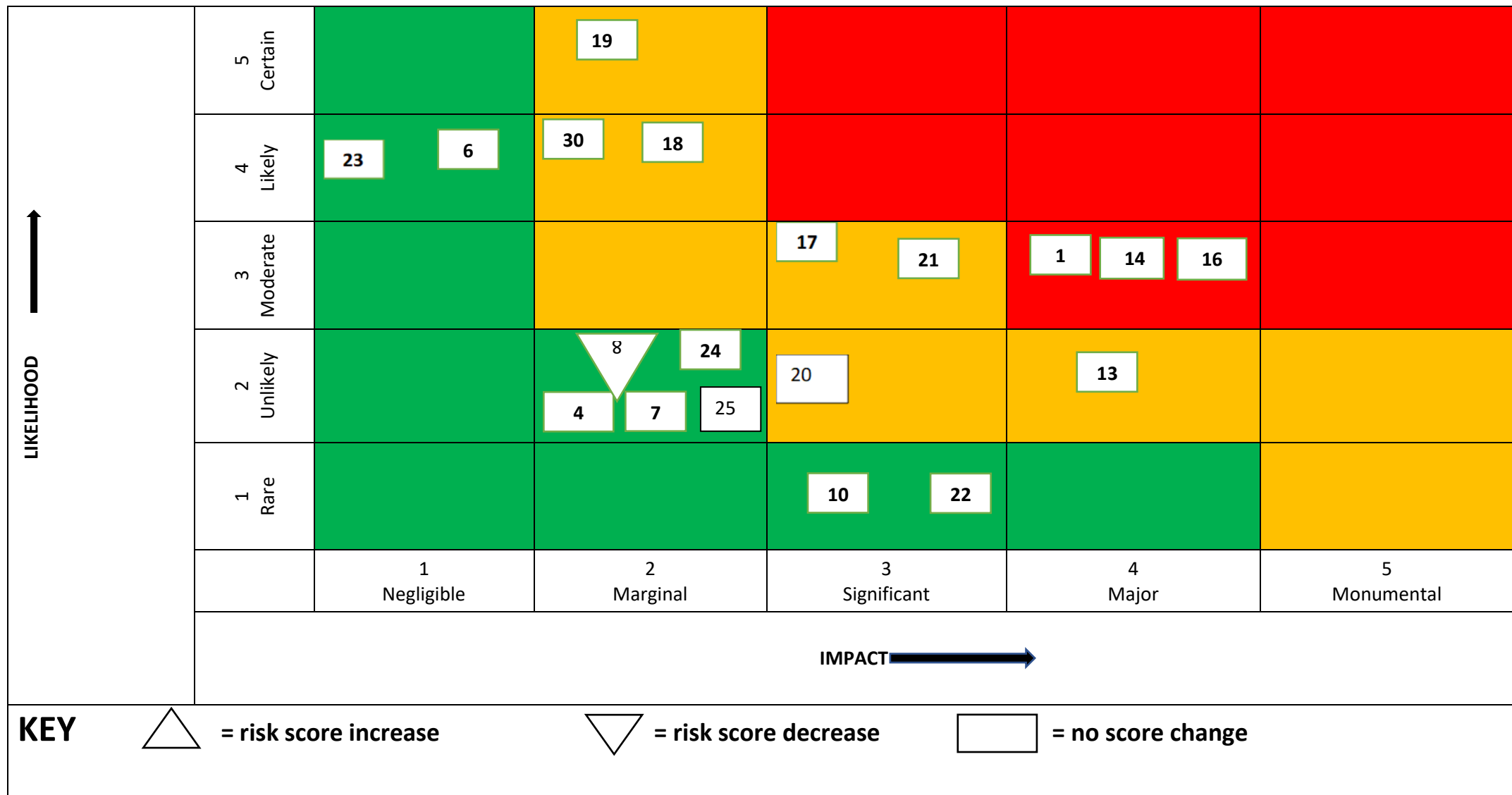


Total RAG Count - Meeting X

Total RAG Count - Meeting 24.09.21



Combined Authority Corporate Risk Heat Map



Corporate Risk Register																						
Risk ID	Date Identified	Cause(s)	Risk Event	Effect(s)	Risk Type	Risk Status	Risk Proximity	Likelihood (1-5)	Impact (1-5)	Inherent RAG score	Date Last Review	Mitigation Plan (Current Controls)	Mitigation Action (New Controls)	Action Owner	Date Action Closed	Likelihood (1-5)	Impact (1-5)	Residual score	Comments/Notes / Assumptions	Risk Owner	Escalating Required	Date Closed
										Total								Total				
1	01/09/2019	External delivery partners unable to deliver on agreed commitments to CPCA projects	External delivery partners do not meet deadlines, budget or qualitative requirements of their agreements with the Combined Authority.	Projects are not delivered on time, budget, or to the required standard.	Strategic	Open	Imminent	5	4	20	09/06/2021	Close working with delivery partners through best-practice project and programme management. Political and senior leadership engagement with partners to ensure effective communication, early warning, and timely and effective escalation of issues.	(i) Ensuring compliance with CPCA project management guidance (ii) Monthly project highlight reporting (iii) Monthly budget monitoring (iv) Creation of programme boards to engage partners at senior level in managing larger areas of work (v) regular project reporting to Board and Committees (vi) minimising delivery partner risk on some projects by direct in-house contracting with the supply chain (vii) achieving increased clarity about roles and responsibilities in the partner landscape (viii) targeted Mayor-level political engagement with delivery partners on some projects	CMT Members, PMO, Project Managers		3	4	12	CCC (key delivery partner) now introducing project management approach, but at an embryonic stage. Cost and timing risks still crystallising on legacy projects.	Director of Delivery & Strategy	N/A	
6	01/09/2019	Change in government policy around devolution	Lack of structural resilience / insufficient internal resources	Failure to maintain BAU due to the devolution white paper and known changes of transferring of the transport teams from PCC and CCC. Including changes in SLA requirements. Increase in subsidiary companies requiring increased employment to accelerate programmes e.g. CAM	Strategic	Open	Close	4	2	8	09/06/2021	Employed a strategy team to consider and report on the impacts. HR function to allow recruitment of additional transport function. Ensuring we have sufficient funding to allow employment.	The Directors meet weekly and are responsible for signing off recruitment to new posts The HR team has been increased to support the organisational structure and recruitment of candidates of calibre. There are staff dedicated to programme management with a system of monthly project highlight reporting. This enables Directors to move resources to higher risk projects. We are in the process of standardising documentation to create a single source of information which builds resilience in case of individual staff members incapacity	Chief Executives		4	1	4		Chief Executives	N/A	
7	01/09/2019	Potential impact of the new Trade Deal with the EU on delivery of the Combined Authority's Growth Ambition Programme (A)	Potential impact of Brexit on delivery of the Combined Authority's Growth Ambition Programme in the short term.	Potential financial uncertainty and economic instability leading to insufficient investment in priority projects in the short term.	Strategic	Open	Close	2	4	8	09/06/2021	Establish a permanent and continuous econometric insight programme to monitor sector and place impacts of Trade Deal conditions Engagement with business organisation (FSB, CBI etc) stakeholders to augment resources, including business advice and monitoring of sentiment through Chambers Development of an economic recovery strategy from both COVID and BEXIT that stimulate growth in relatively unaffected firms and sectors, whilst alleviating the impacts for thos effected by the trade deal	Monthly monitoring of sector economic impacts and daily monitoring of business sentiment and impacts. Weekly monitoring of bulletins from MCHLG, BEIS, HMRC to ensure information is accurate and up to date, recognising funding streams relevant to need Engagement with LEP Network and CLGU on funding for additional resources. Monitor for possible impacts resulting from the Trade Deal.	Director of Business & Skills [Brexit Lead]		2	2	4	Assumption being that CPCA re-calibrate our objectives to a new GVA figure. With the advent of a trade deal the main residual risk relates to the long term reduction in attractiveness of the UK as an inward investment destination, especially from Europe.	Director of Business & Skills [Brexit Lead]	N/A	
8	01/09/2019	Absence of funding of historic ambitious and long stalled Programmes	Ambitious and long stalled programmes can not proceed due to lack of government funding and or private investment.	There are major programmes that will require clear and innovative funding strategies if they are to progress. CPCA funding has been used to develop the feasibility and Strategic Outline Business Cases/Outline Business Cases for such schemes. CPCA funding is intended to act as a catalyst and an enabler in bringing these schemes forward.	Financial	Open	Close	3	3	9	09/06/2021	Work is progressing at developing the business cases. Stakeholders across the wider geography are working together to tackle the issues around the growth agenda. Getting Board agreement and matching resources will help get a coordinated approach to priorities and bidding for resources. Funding sources have been identified for key sources and CPCA resources allocated to move projects to those funding decisions.	Strong budget process and funding allocation within CPCA MTFP and Business Plan Business Case approval by CPCA Board and Stakeholders Ongoing discussions with Whitehall departments about access to national funding programmes, such as LLM	Directors		2	2	4		Chief Finance Officer	N/A	
10	01/09/2019	Lack of Resource Planning & Financial Management practices	Absence of Resource Planning & Financial Management	The organisation has no clear budget and capital programme that sets out how resources will be deployed and managed within. This is fundamental to any proper management process and any reporting that will be required by CPCA Board, Stakeholders and Government. Without this, no prioritisation takes place and there is no clear measurement of outcome v ambition. It is the framework for sound decision making).	Financial	Open	Imminent	1	5	5	09/06/2021	A comprehensive Medium Term Financial Plan was approved at Board in January which focussed on refreshed priorities to support economic recovery. Regular financial and budget update reports are provided to Committees and to the CPCA Board. Internal Management reporting is being developed alongside the PMO highlight reports.	Monthly Budget monitoring reports All business cases for capital spend is approved at Board CFO and Monitoring Officer to sign off all business cases and reports Corporate approach to Monitoring & Evaluation and Action.	Chief Finance Officer		1	3	3		Chief Finance Officer	N/A	
13	01/09/2019	First 5 Year Gateway Review of Gainshare Funding (Mar 2021)	Access to Gainshare funding called into question by the Gateway Review evaluation of Gainshare	The Combined Authority is unable to access Gainshare funding	Strategic	Open	Approaching	3	5	15	09/06/2021	Provision of persuasive evidence to the Gateway Review demonstrating the good management and value for money delivered through Gainshare funding. External and internal communication plans to manage either positive or negative outcome.	CMT members to seek intelligence from MHCLG about potential notification of the review outcome. PR to brief Communications team.	CMT Members, PMO Programme Manager, Analysis and Evaluation Manager		2	4	8		Director of Delivery & Strategy	N/A	
14	01/03/2020	Covid-19 Pandemic (A)	Disruption to the operation of the Combined Authority	Potential absence of significant numbers of Combined Authority staff undermining the ability to transact the operational business of the Combined Authority	Operational	Open	Imminent	4	4	16	09/06/2021	Developed a business continuity plan based on technological advances (digital transformation) Communication with both suppliers and delivery partners All Combined Authority staff are now working from home, with support for remote meetings. Developed on digital transformation on virtual exhibitions and online Committee / Board meetings. Liaison with suppliers to ensure continuity of supply chains.	HR support to staff working remotely. Communication with both suppliers and delivery partners All Combined Authority staff are now working from home, with support for remote meetings. Developed on digital transformation on virtual exhibitions and online Committee / Board meetings. Liaison with suppliers to ensure continuity of supply chains. Liaison with delivery partners to ensure continuity	Chief Executives		3	4	12		Chief Executives	N/A	
16	01/03/2020	Covid-19 Pandemic (B)	Disruption of the delivery of the Combined Authority objectives in regard to the short term economic objectives	Economic impact of lockdown in response to Covid-19, may have implications for future government funding and for economic activity within the Combined Authority area in the short term.	Strategic	Open	Imminent	4	4	16	09/06/2021	Support to local businesses to weather the Covid-19 lockdown - in co-ordination with the constituent councils Following government guidelines and working with local resilience forum to plan the recovery and restoration of services. Additional budget announcements from govt.	Business Restoration and Business Recovery Groups Board reports - MTFP re-prioritisation towards economic recovery Membership of the SCG (Strategic Recovery Group) - weekly transport recovery group. Mayoral forum Chaired economic recovery group Local economic recovery strategy - will be implemented in October 2020 CSR (3 year) - submitted with Covid-19 mitigating asks. CPCA grants	Chief Executives		3	4	12		Chief Executives	N/A	
17	15/05/2020	Unbudgeted increases in cost for highways and transport schemes funded by the Combined Authority and delivered by partner agency	Unplanned significant increases in costs lead to requests for additional funding to the Combined Authority to enable schemes to proceed.	The unplanned increases in budget prejudice the Combined Authority's ability to manage its finances and could ultimately prejudice delivery of the Combined Authority's Business Plan and a balanced budget.	Financial	Open	Imminent	5	3	15	09/06/2021	Close working with delivery partners through best-practice project and programme management. Political and senior leadership engagement with partners to ensure effective communication, early warning, and timely and effective escalation of issues. Particular focus on the relationship between scheme design and cost at an early stage.	(i) Ensuring compliance with CPCA project management guidance (ii) Monthly project highlight reporting (iii) Monthly budget monitoring (iv) creation of a Transport Programme Board (v) stronger discipline around the composition and working of project boards for individual projects (vi) regular project reporting to Board and Committees (vi) review of historic overruns to establish cause. (vii) updating project management guidance inline with audit recommendations e.g. Lancaster Way	Director of Delivery & Strategy		3	3	9		Chief Executives and Chief Finance Officer	N/A	
18	31/07/2020	Climate Change	Climate change related events, policies and political pressures e.g. policy designed to reduce carbon emissions that restricts growth	Unable to double GVA	Strategic	Open	Close	4	4	16	09/06/2021	CPCA funding an independent climate change commission to provide advice and recommendations on how to delivery Combined Authority ambitions and to achieve net-zero Strategic combined authority policies require business cases for the delivery of projects to be consistent with the net-zero ambition.	Preparing an implementation plan for the CPICC recommendations. Communicating the CPICC headlines, especially that its recommendations are consistent with an ambitious growth trajectory. Accommodation, travel and internal policies to reduce scope one & two emissions	Strategic Planning Manager, Head of Comms, Chief Executives		4	2	8		Chief Executives	N/A	
19	11/11/2020	Covid -19 Pandemic (C)	Disruption of the delivery of the Combined Authority objectives in regard to the long term economic objectives	Economic impact of lockdown in response to Covid-19, may have implications for future government funding and for economic activity within the Combined Authority area in the long term.	Strategic	Open	Imminent	4	4	16	09/06/2021	Support to local businesses to weather the Covid-19 lockdown - in co-ordination with the constituent councils Following government guidelines and working with local resilience forum to plan the recovery and restoration of services. Additional budget announcements from govt.	Business Restoration and Business Recovery Groups Board reports - MTFP re-prioritisation towards economic recovery Membership of the SCG (Strategic Recovery Group) - weekly transport recovery group. Mayoral forum Chaired economic recovery group Local economic recovery strategy - will be implemented in October 2020 CSR (3 year) - submitted with Covid-19 mitigating asks. CPCA grants	Chief Executives		5	2	10		Chief Executives	N/A	
20	11/11/2020	Potential impact of the New Trade Deal with the EU on delivery of the Combined Authority's Growth Ambition Programme (B)	Potential impact of the new Trade Deal on delivery of the Combined Authority's Growth Ambition Programme in the long term	Slowing of baseline growth sufficiently to undermine CPCA current and planned interventions, rendering them unable to produce enough additive growth to hit the doubling of GVA target	Strategic	Open	Approaching	2	4	8	09/06/2021	Establish a permanent and continuous econometric insight programme to monitor sector and place impacts of Trade Deal conditions Engagement with business organisation (FSB, CBI etc) stakeholders to augment resources, including business advice and monitoring of sentiment through Chambers Development of an economic recovery strategy from both COVID and BEXIT that stimulate growth in relatively unaffected firms and sectors, whilst alleviating the impacts for those effected by the trade deal	Monthly monitoring of sector economic impacts and daily monitoring of business sentiment and impacts. Weekly monitoring of bulletins from MCHLG, BEIS, HMRC to ensure information is accurate and up to date, recognising funding streams relevant to need Engagement with LEP Network and CLGU on funding for additional resources. Monitor for possible impacts resulting from the Trade Deal.	Director of Business & Skills [Brexit Lead]		2	3	6	raised from green to amber on the basis of business insight being received from firms, esp SMEs, that sales are being adversely impacted by new regulations. Need to monitor whether solutions are developed by firms to adapt or not	Chief Executives	N/A	
21	11/11/2020	MHCLG Review of £100m Housing programme	Up to £45m of Government funding not provided, change of end date of £100m Housing Programme from 31st March 2022 to 31st March 2021 and potential programme loss of 243 housing units at Northstowe which MHCLG may not recognise.	£170m programme has shortage of anticipated capital and significantly reduced time and capability to deliver target of 2000 houses and the £100m programme within the £170m. Potentially significant reputational damage to CPCA housing programme likely.	External	Open	Imminent	5	5	25	14/09/2021	Outcome of proposed 2021/22 programme is now known. The original programme was closed on 31st March 2021, funding decisions successfully prioritized to those schemes that could start by 31st March 2021 and 733 starts were achieved. MHCLG offered a new programme from 1st April 2021 to 31st March 2022 subject to certain conditions which have been accepted by the CPCA Board. A programme for over 1,700 units was proposed by CPCA requiring £42.5m of new money. The Minister has advised that government is prepared to support a programme for 1,189 units with £18.7m of new money for 2021/22. £2m of that new money expected to be received in Oct 2021. The practical arrangements are being worked upon. MHCLG has also advised that they will not be able to offer CPCA a direct funding programme beyond March 2022.	Meetings ongoing with MHCLG to work out the details on how the 2021/22 affordable housing programme meeting and reporting with MHCLG will work up to March 2022	Chief Executive/ Housing Portfolio Holder/Housing Director		2	3	6	Mitigation ongoing with MHCLG discussions to work out practical details of future monitoring, progress reports and providing evidenced claims to enable authorisation of future funding payments.	Housing Director	N	
22	06/01/2021	Delivery partner authorities determining that costs incurred in relation to CPCA capital funded projects should not be treated as capital expenditure for the purposes of the relevant finance rules.	Grant funding which is expected to be treated as capital expenditure is required to be treated as revenue expenditure by CPCA, as a result of a determination by a partner delivery authority. The risk would be a consequent shortfall in revenue funding to meet the commitment.	Revenue funding deficit	Financial	Open	Approaching	2	3	6	09/06/2021	Discussions with Delivery Partners including constituent authorities. Ensure that grant determination letters are explicit in the expectation that capital grant funds will be used only for capital purposes.		All Directors		1	3	3		Chief Finance Officer		
23	25/03/2021	Lack of capacity/resilience in the ICT provision to the CPCA	Shortfall in the provision of an adequate ICT platform for future need - including software and systems, and equipment. Failure to have access to an application/system needed for the delivery of the CPCA project, programme, or service.	Programme, project, or service disruption.	Operational	Open	Approaching	2	4	8	09/06/2021	The CPCA is in discussions with the current service provider to understand the level of service offer available to the CPCA. The CPCA has commissioned the specialist consultancy "SOCITM" to undertake an ICT needs assessment and future provision plan.	Examination of options for interim support to stabilise the service provision.	All Directors		1	4	4		Chief Executives	N/A	
24	09/06/2021	Post-election onboarding	Changes in Political Management and change in priorities for the CPCA	Impact on funding, contractual arrangements and investor confidence in the CPCA	Strategic	Open	Approaching	4	2	8	09/06/2021	Clearly around existing priorities and contractual obligations.	MTFP, Business Plan, Leaders Strategy meetings following the election	Chief Executives		2	2	4	Following the election of Mayor Johnson, programmes/priorities are reviewed.	Chief Executives	N/A	
25	03/11/2020	Financial SLA out of date	No access to finance systems	Not able to record transactions or to provide management reports and to create statutory returns to government (including VAT). Ability to draft year end financial statements would be compromised. A statutory requirement to keep proper accounting records	Financial	Open	Approaching	2	3	6	08/06/2021	Ongoing discussions with PCC. PCC to provide draft SLA mid-June 2021	Review system options	CFO		2	2	4	Verbal agreement with PCC to continue using their system and support until such time as CPCA have identified and moved to preferred future system	Chief Finance Officer	No	
30	15/09/2021	Insufficient internal resource to deliver the Authority's priorities	Key priorities not delivered	Key priorities, especially new ones identified for the new Mayoral term, would remain unaddressed.	Delivery	Open	Approaching	4	4	16	15/09/2021	Recruitments under way for vacant posts and new posts on climate change and analysis being established and recruited to	Recruitments under way and MTFs bids being considered	CMT		2	4	8	Assumes recruitments are successful	CEO	No	



**CAMBRIDGESHIRE
& PETERBOROUGH**
COMBINED AUTHORITY

Agenda Item No: 11

Information Governance Update

To: Audit and Governance Committee

Meeting Date: 24 September 2021

Public report: Public Report

From: Rochelle Tapping
Deputy Monitoring Officer

Recommendations: The Audit and Governance Committee is invited to:

- a) Note the Information Governance Update
- b) Note the data on corporate complaints and freedom of information requests for June 2021 to August 2021
- c) Note the new GDPR Policies for the Combined Authority set out at Appendix 1 to 7.
- d) Recommend to the Combined Authority board that it approves and adopt the GDPR policies
- e) Recommend the Combined Authority delegated authority to the Monitoring Officer to make consequential amendments to those Policies as required.

Voting arrangements: A simple majority of Members.

1. Purpose

- 1.1 To update the Audit and Governance Committee on the current position with regards to the GDPR Policy and Information Governance Policy as recommend by the Information Governance Report prepared in October 2020 and put before the Audit and Governance Committee on the 5 March 2021.
- 1.2 To provide data related to the number of corporate complaints and Freedom of Information requests for the period of 1 June 2021 to 31 August 2021

2. Background

- 2.1 The Committee agreed that six-monthly reports should be presented on the number of data breaches and how they were handled, number of complaints received, timings of FOI's and cases referred to the ICO. These reports are set out below.
- 2.2 At its meeting on 16 December 2019 the Audit and Governance Committee reviewed the Combined Authority's Data Protection Policy which was adopted by the Combined Authority Board at its meeting on 29 January 2020. The Data Protection Policy should be reviewed and updated from time to time, and this is underway with the support of GDPR officers at Peterborough City Council under a service level agreement.
- 2.3 As the Committee is aware Combined Authority's IT service has been outsourced to an external provider called Socitm Advisory.
- 2.4 The table shows the main recommendations of the Information Governance Report, progress to date and the target completion date.

Recommendation	Progress and Target Date for Completion (TDC)
Update policies where necessary	<p>The GDPR Policy has been updated. This update Policy is shown at Appendix 1.</p> <p>Socitm Advisory are going to provide a baseline set of IT policies as well as IT procedures. These policies will include:</p> <ul style="list-style-type: none">• acceptable usage agreement• Device loan agreements• Backup and storage policy• Data policy including portable media etc• IT disaster recovery <p>TDC Autumn 2021</p>

Introduce Staff training programme to cover data protection and information/cyber security	<p>All officers within the Combined Authority must undertake mandatory online Data Protection training run by Cylix Limited by the 24th September. This is to ensure all officers are aware of their responsibilities under the Data Protection Act 2018. Currently 52% of all officers have completed this learning.</p> <p>Officers have undertaken IT security training run by Barclays Bank. Further IT security training is being finalised for delivery across the organisation.</p>
Introduce Data Privacy Impact Assessments (DPIAs) for all new projects which involve the processing of personal information – A Data Protection Impact Assessment (DPIA) is a process to help identify and minimise the data protection risks of a project. A DPIA must: • describe the nature, scope, context and purposes of the processing; • assess necessity, proportionality and compliance measures; • identify and assess risks to individuals; and • identify any additional measures to mitigate those risks	The DPIA Policies and forms have been created. Training will be given to use these forms and policies. The Policies are shown at Appendix 3 to 7.
Create a new data protection section on CPCA website	Now the Policies have been created these will be added to the CPCA's website and the webpage further developed. TCD end of 2021
Merge all Records Retention policies into a single policy	New Retention Policy has been created. The new Policy is shown at Appendix 2.
Encryption of emails and removal of auto-populate function, regular penetration tests Penetration tests which is a process whereby an external specialist company is commissioned to investigate your environment for vulnerabilities i.e., attempting to hack the system.	Socitm Advisory have just promoted the Combined Authority's Microsoft licenses that include additional security features, one in particular is data sensitivity tagging an example would be marking a document / email as "sensitive". Controls can be applied to that tag to stop forwarding, printing, editing, copy and pasting, and now taking screen shots. Socitm are also looking at exchange and boundary encryption to compliment this. Socitm are currently reviewing the processes needed to remove the cached address book on people's machines for external only emails. This will remove the risk of

	<p>accidental data breaches where incorrect contacts have been used.</p> <p>Socitm have secured CPCA a 3-year agreement to provide a centrally managed corporate antivirus solutions that protects the Combined Authority's devices from infection but also protects the users when browsing the web (website checker).</p>
Secure Public Sector Network (PSN) compliance or similar accreditation PSN compliance is a way to report security arrangements. It is how the CPCA could demonstrate to Government that its security arrangements, policies and controls are sufficiently rigorous for Government to allow the CPCA to interact with the PSN and those connected to it. The CPCA would have to apply for certification demonstrated by meeting compliance. Holding a valid PSN compliance certificate would give the CPCA permission to interact with the PSN in a specific, pre-agreed way.	Socitm have advised that unless the Combined Authority are dealing with sensitive data from example, the Department of Working Pensions, then the PSN would serve no additional benefits. There is also a challenge in that the CPCA work mainly in a remote environment, as the PSN network is a physical connection deploying this would be unachievable.
Conduct information audit and update Information Asset Registers An asset register records assets, systems and applications (e.g. word documents, archived emails, spreadsheets, databases, etc) used for processing or storing personal data across the organisation and was introduced as a requirement by the GDPR	This is referred to in the Data Protection Policy. It is yet to be implemented. TCD by the end of 2021.
Review duplicated files	Socitm are currently investigating the right IT solution to use to review and deal with duplicated files.
Convene monthly Information Risk Group meetings	This has yet to be implemented but is being finalised. TDC Autumn of 2021

2.5 Freedom of Information (FOI) and Environmental Information Regulations (EIR) requests

During the period 1 June 2021 to 31 August 2021 the Combined Authority received 12 requests for information under the Freedom of Information Act and a further 1 request for information under the Environmental Information Regulations. All requests and responses have been published on the Combined Authority's website. The topics of the requests upon which FOI and EIR requests were made are:

- Business expenditure and IT matters
- Details on the Mayor – salary, what income is he receiving as a doctor
- IT Cyber Security within the CPCA
- HR issues – staff secondments from 2017 – 2021
- Spend information on the website
- Meetings with Chinese Companies
- Chief Exec salary – information why the CEO is paid £204,000
- How many media, press and Comms Officers within the CPCA.
- Total number of looked after Children
- Antisemitism
- Funding - Homes England
- Adult Education Budget Allocations/Budget
- Transport - junction improvement at Horsey Toll

Performance for this period was as follows:

All of the FOI and EIR requests were responded to within the timeframe of 20 working days save for 1 response which was 1 day late.

2.6 Whistleblowing Disclosures

The Combined Authority has received 0 whistleblowing disclosures for the period up to 31st August 2021

2.7 Corporate Complaints

During the period of 1 June 2021 to 31 August 2021 the Combined Authority received 0 complaints.

Significant Implications

3. Financial Implications

3.1 None

4. Legal Implications

4.1 The Data Protection Act 2018 and the UK General Data Protection Regulations governs UK data protection following withdrawal of the UK from the EU.

5. Other Significant Implications

5.1 None

6. Appendices

- 6.1 Appendix 1 - Data Protection Policy
- 6.2 Appendix 2 – Retention Policy
- 6.3 Appendix 3 – Data Impact Assessment Guidance
- 6.4 Appendix 4 – Data Protection Impact Assessment
- 6.5 Appendix 5 – Data Incident Reporting Policy
- 6.6 Appendix 6 – Data Protection Impact Assessment Checklist
- 6.7 Appendix 7 – Data Incident Reporting form

7. Background Papers

None.



**CAMBRIDGESHIRE
& PETERBOROUGH**
COMBINED AUTHORITY

DATA PROTECTION POLICY

Type of document:	Policy
Document produced by:	Cambridgeshire & Peterborough CA Data Protection Officer
Document approved by:	Cambridgeshire & Peterborough Combined Authority Board
Version :	Version 1
Issue date:	
How is this shared?	Email
Date due for review:	Annually April
Reviewer:	Rochelle Tapping Susan Hall

Data Protection Contact		
Contact Details	Email	Phone
Rochelle Tapping	dpo@cambridgeshirepeterborough-ca.gov.uk	07923250218

“If you only read this page then...”	5
Introduction.....	6
Why do we have a policy?	6
Who does the policy cover?	7
What are our responsibilities?	7
Lawful basis for processing.....	8
What are your responsibilities?	9
People have rights	9
The Right to be Informed	9
The Right of Access	9
The Right of Rectification	10
The Right to Erasure	10
The Right to Restrict Processing	10
The Right to Data Portability	10
The Right to Object	10
Rights related to automated decision making including profiling	11
What does ‘it’ mean?.....	11
Personal Information	11
Special Categories of Personal Information.....	11
Data Controller	11
Joint Data Controller	11
Data Processor	12
Data Controller-Data Processor Relationship - Contracts	12
When data is lost or goes missing.....	12
Keeping Information	12
Location of our information.....	13
How we handle information.....	13
The Sharing of Personal Information	13
Disclosures permitted by law	13
Information sharing agreements	13
Testing of systems	14
Privacy and the value of information	14
Data Protection Impact Assessments (DPIA)	14
Only use what you need to use.....	14
Anonymisation of data.....	14
Pseudonymisation.....	15
Information as an asset.....	15
Roles	15
Chief Executive	15
Senior Information Risk Owner (SIRO).....	15
Data Protection Officer	15

Information Risk Group	16
Responsibilities of Managers	16
Additional responsibilities for Managers - Temporary Staff	16
Responsibilities of Members	16
Responsibilities of all staff	16
Policy Review	16
Monitoring Compliance	16
Training	Error! Bookmark not defined.

“If you only read this page then....”

Do ask for only the information you need to do the job and only keep it for as long as you need to

Do be clear about why you are collecting the data

Do only use information for the reason it was collected and seek advice if you need to use it for something else

Do dispose of paper records and emails securely

Do use strong passwords to protect devices and data

Do use secure and encrypted devices

Do make sure you know who you are talking to and check their identity if you need to

Do check someone's email or postal address before you send anything and make sure you always update records to make sure they are accurate

Do check what is in an envelope or email before you send

Do use the report if any data is lost/misplace/misused, for advice or if someone asks to see information held about them or wants their information deleted

Don't share personal information unless you are sure you can and you know who is asking

Don't assume that someone's consent last forever and covers everything

Don't leave PCs, laptops and phones unlocked or share your passwords

Don't leave personal information on show on desks or in vehicles - make sure it's secure

Don't open emails or click on links if you don't recognise the sender - speak to IT

Don't write comments about an individual that we cannot defend - they have a right to see them

Don't ignore a possible data breach - the sooner it is reported, the sooner it can be dealt with

Don't think data protection does not matter, it does!

Introduction

We need to collect and use different types of information about people that we provide services for and communicate with in order to deliver those services. These could include service users, both adult and children, current, past and prospective employees, contractors, and suppliers.

In addition, we may occasionally be required by law to collect and use certain types of information to comply with the requirements of government departments for business data.

The UK General Data Protection Regulation and Data Protection Act 2018 are pieces of law which will call ("UK GDPR") and ("DPA 2018") respectively, together, "**data protection legislation**". These explain the requirements and safeguards which we must be applied to personal data to ensure the rights and freedoms of living individuals are not compromised.

Data protection means when we record and use personal information then we must be open about how the information is used and keep it secure. It applies to how we collect, use, shared, keep, delete and destroy personal information. s we use and decide how we use personal information, we have to ensure we comply with data protection legislation.

This policy applies to all personal data held by or on our behalf. It includes manual/paper records and personal data that is electronically processed by computer systems or other means such as CCTV systems.

Why do we have a policy?

The purpose of this policy is to make sure that we:

- Comply with the law in respect of the data we holds about people
- Protect our customers, service users, employees and other individuals
- Protect the organisation when a data breach happens
- Follow good practice

We recognise we have a responsibility to make sure we comply with all of our data protection duties. We also have to ensure that all of our employees and suppliers not only understand but comply with data protection legislation.

Who does the policy cover?

This policy applies to anyone accessing or using personal information, including for example: employees, temporary or contract staff, volunteers, work placements, contractors, suppliers, services providers or other partners or agencies.

We have to make sure that anyone delivering a service on our behalf complies with this policy and others to make sure our data is safe.

What are our responsibilities?

There are seven Data Protection Principles with which we must comply with in relation to personal information. In summary these are that personal information will be:-

- 1. Processed fairly and lawfully in a transparent way**
- 2. Obtained only for one or more specified and lawful purposes and not further processed in a manner incompatible with that purpose**
- 3. Adequate, relevant and limited to what is necessary**
- 4. Accurate and where necessary, kept up to date**
- 5. Not be kept for longer than is necessary**
- 6. Protected by appropriate technical and organisational measures**
- 7. We are accountable and take responsibility for what we do with personal data**

This means that we will:-

- a) make sure that when we ask for information then we are fair to the people whose information we ask for and use,
- b) explain why we are asking for the information and what we will do with it,
- c) make sure we only ask for the information we need,
- d) make sure the information we hold is up to date and accurate,
- e) make sure we only keep it for as long as we need to,
- f) ensure that we have processes in place to protect the information whether it is on paper or electronic,
- g) ensure that we won't send information abroad unless there are the proper safeguards,
- h) make sure that people can exercise their data protection rights.

In addition we will also:-

- have someone with specific responsibility for data protection (Data Protection Officer, or DPO),
- make sure all employees know that they are responsible for data protection and know what good practice is,
- train staff to manage and handle information correctly,
- support staff to manage and handle personal information correctly,
- respond to any queries about handling personal information promptly and courteously,
- review how we use personal information to make sure we are always complying,
- ensure staff know when they can share information with others.

Lawful basis for processing

We must have a lawful reason to use personal information and special category data. This will be one of the six legal bases in Article 6 of the UK GDPR for personal information:

- (a) Consent:** the individual has given clear consent for you to process their personal data for a specific purpose.
- (b) Contract:** the processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract.
- (c) Legal obligation:** the processing is necessary for you to comply with the law (not including contractual obligations).
- (d) Vital interests:** the processing is necessary to protect someone's life.
- (e) Public task:** the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.
- (f) Legitimate interests:** the processing is necessary for your legitimate interests or the legitimate interests of a third party, unless there is a good reason to protect the individual's personal data which overrides those legitimate interests. (This cannot apply if you are a public authority processing data to perform your official tasks.)

For special category data then this will be one of the ten legal bases in Article 9 of the UK GDPR:

- (a) Explicit consent:** the individual has given clear consent for you to process their special category data for a specific purpose.
- (b) Employment, social security and social protection:** if authorised by law and we have identified a condition in Part 1 of Schedule 1 of the DPA 2018
- (c) Vital interests:** the processing is necessary to protect someone's life.
- (d) Not-for-profit bodies:** who process special category data in connection to the activities of charity, clubs, political parties, churches etc,
- (e) Made public by the data subject**
- (f) Legal claims or judicial acts** if necessary to establish, exercise or defend legal claims.
- (g) Reasons of substantial public interest** with a basis in law and we have identified one of the 23 specific substantial public interest conditions set out in Part 2 of Schedule 1 of the DPA 2018.
- (h) Health or social care** with a basis in law and we have identified a condition in Part 1 of Schedule 1 of the DPA 2018
- (i) Public health** with a basis in law and we have identified a condition in Part 1 of Schedule 1 of the DPA 2018
- (j) Archiving, research and statistics** with a basis in law and we have identified a condition in Part 1 of Schedule 1 of the DPA 2018

We should be able to say which applies. If you are not sure then you should speak to the Data Protection Officer.

What are your responsibilities?

All of us, whether permanent or temporary, are required to read, understand and accept any policies and procedures that relate to the personal data that we may handle in the course of our work.

All of us must:

- understand the main points of the Data Protection legislation,
- identify and report any risks their line manager,
- make sure that customers understand their rights,
- identify any breaches or loss of data and report them,
- identify and report any rights requests to the Data Protection Team.

People have rights

Data protection legislation has introduced a set of rights for people. These are explained below and how we meet these.

All requests received should be directed to:

The Data Protection Officer

The Mayor's Office

72 Market Street

Ely

Cambs

CB7 4LS

Telephone: 07923250218

Email: dpo@cambridgeshirepeterborough-ca.gov.uk

The Right to be Informed

This means that people have a right to be told what we are doing with their information. We need to be clear and transparent about what we do because this helps build understanding and trust about what we do.

The way we normally tell people about what we do is in what we call a privacy notice. Our privacy notice is available on our website at the link <https://cambridgeshirepeterborough-ca.gov.uk/wp-content/uploads/documents/governance/transparency/codes-ofconduct-and-policies/Data-Protection-Policy.pdf> so that people can easily find it.

The Right of Access

If we hold information about a person, then they have a right to see their own information. There are a few exceptions to this rule, such as data held for child protection or crime detection / prevention purposes, but most individuals will be able to have a copy of the data held on them. We may have to redact some of the information if we cannot share something with a person.

The Right of Rectification

If a person believes that any of the information that we hold about them is inaccurate, then they have a right to request that we restrict the processing of that information and to rectify the inaccurate personal information. Please note that if the request is to restrict processing their information, we may have to suspend the services provided. We have to respond with a month.

The Right to Erasure

This is popularly known as the “right to be forgotten”. It means that people can ask us to delete or remove information if there no strong reason for us to keep it.

We don't have delete information. The below table indicates when we may agree to delete and when we will not

To delete...	Or not to delete...
We no longer need the information	to exercise the right of freedom of expression and information
We should not have the information	We need to keep it to comply with a legal obligation
Our customer withdraws their consent	We need to keep for public health purposes
Legally we should have deleted it	It is of public interest for scientific/historical research or statistical purposes
Our customers objects to what we are doing, and we cannot justify keeping the information	We need to keep it for the defence of legal claims

We always need to listen and understand why someone asking us to delete. We may have to keep some information, for example it is about safeguarding or health and safety. We should still take into account the customer's concerns and look what we can do to help reduce any distress or concerns they may have.

The Right to Restrict Processing

A person has the right to block or suppress the use of their information. If someone does ask us to restrict the use of their information, then it means that we can retain the information but not use it any further.

We will need to keep some information to ensure that we maintain the restriction.

The Right to Data Portability

Where we have requested a person's permission to process their personal information or they have provided us with information for the purposes of entering into a contract with us, then they have a right to receive the personal information you provided to us in a portable format.

The Right to Object

An individual can object to what we are doing with their data where if it is based on:

- our legitimate interests or
- public interest or statutory duty or
- direct marketing or
- purposes of scientific/historical research and statistics.

The objection must relate to the person's particular situation.

Rights related to automated decision-making including profiling

A person has the right to not be the subject of a decision if it is based on automated processing and it produces a legal effect or significant effect on them.

The right does not apply where processing is necessary for the performance of a contract, authorised by law (including fraud) or there is explicit consent.

What does 'it' mean?

Personal Information

Personal information is information about a living individual who you can identify directly or indirectly from that information. It may also be possible to identify an individual from that and other information which is in the possession of, or likely to come into our possession. It also includes any expression of opinion about the individual and any indication of our intentions.

It is also important to note that information to identify a living person is not limited to names and full addresses. Mapping point data can also potentially identify a person as can limiting the address to postcode.

Special Categories of Personal Information

Special categories of personal data, formerly known as sensitive personal data, means personal data consisting of information as to -

- the racial or ethnic origin of the data subject,
- his/her political opinions,
- his/her religious beliefs or other beliefs of a similar nature,
- whether he/she is a member of a trade union
- genetics
- biometrics
- his/her physical or mental health or condition,
- his/her sexual life,
- sexual orientation

In addition, we would consider the following to be sensitive:

- the commission or alleged commission by him/her of any offence,
- any proceedings for any offence committed or alleged to have been committed by him/her, the disposal of such proceedings or the sentence of any court in such proceedings,
- credit card/debit card details pertaining to the data subject

Data Controller

The Combined Authority is a data controller and will be responsible for ensuring compliance with data protection legislation. It means, on some occasions, that we determine what data is collected and how it is used.

Where someone acts completely on behalf of the authority then we are still the data controller.

You should refer to the contract for providing a service to understand who the data controller is.

Joint Data Controller

There will be occasions where two or more controllers jointly determine what information is collected and why. This could be with Cambridgeshire County Council or Peterborough City Council for example. We need to make sure that customers understand when this is the case.

You should refer to the contract for providing a service to understand when joint controllers exist.

Data Processor

A data processor is the person/service who use the information as per the controller's instructions. A data processor does not own the data and cannot use it for purposes other than stated in the contract or where permitted. Any use or sharing of data should not be done without the written consent of the data controller.

You should refer to the contract for providing a service to understand who the data processor is.

Data Controller-Data Processor Relationship - Contracts

Where the controller and processor are not the same i.e. the Combined Authority and Cambridgeshire County Council, the relationship must be underpinned by a contract.

It is very important that we have a contract in place for us to deliver services or for something to be done on our behalf. The contract has a really important role to play because it makes sure that all concerned understand what should be delivered.

Any contract must contain detailed schedules of the data to be processed as well as the clauses regarding the arrangements for the use, storage, retention and deletion of data by that external party. In all cases, Legal Services will review every contract and ensure that it meets requirements. The contract between the authority and suppliers will make clear that the liabilities and duties of data protection legislation which must be complied with

This kind of terms will be defined in the contract.

Advice on the process for buying and providing services can be obtained from the Data Protection Officer.

When data is lost or goes missing...

We hold information which can be personal and sensitive information but also, for example, commercially sensitive information or simply data.

We must take every care to avoid a data breach by protecting personal information but also by taking steps to avoid losing any data.

In the unlikely event of data being lost or shared inappropriately, it is vital that appropriate action is taken to minimise any associated risk as soon as possible. You should refer to our data incident reporting policy which covers the process and complete the data incident reporting form.

You must report any breaches, suspected or confirmed, to the Data Protection Officer.

Keeping Information

We may have to keep information, but it must only be kept for as long as we need to.

We will store personal information securely in our IT systems or in hard copy in line with our retention schedule.

We will destroy hard copy personal information securely by using confidential waste bins and electronic records via IT.

More can be found in our Retention Policy.

Location of our information

It is important that we understand where our information is. This does not mean just it's on our devices or on the authority's network. We have to think about where that information really is and the same applies to any data we share or provide to others. This means where servers are or where a cloud/data centre is.

When the UK left the EU, this meant that transfers of information needed to be *permitted* under the UK GDPR. There are provisions in the UK GDPR to enable this flow of information. In order for information to flow from EEA countries, UK needed to be provided with an *adequacy decision* by the EU which it currently has. The UK has also recognised the EU adequacy decisions for non-EEA countries - Andorra, Argentina, Faroe Islands, Guernsey, Isle of Man, Israel, Jersey, New Zealand, Switzerland., and Uruguay.

If the information is being transferred to a country where there is no adequacy decision, such as USA, then we must ensure that we have appropriate safeguards in place. If this is the case, then you should speak to the Data Protection Officer and Legal.

How we handle information

Whenever we handle information then we should do so securely. This should mean that information we store is securely in systems protected by usernames and passwords or filing cabinets that are locked. It also means making sure that only people who should see that information have access. When we share or send information then we should make sure that it is secure.

The sharing of personal information must be by secure means such as secure email or secure file sharing may also be used after review by IT and in line with our IT policy. Failure to comply with this policy will result in the appropriate action being taken under either the relevant policy or contract.

The Sharing of Personal Information

We will only share personal information where a legal gateway exists, or consent has been obtained. Sharing means telling someone some information about them or another person and sharing means giving a supplier a list of people.

You should make sure you know whether you should share and consult the Data Protection Officer if you are not sure. We should not use personal information to plan of service provision.

Disclosures permitted by law

There will be occasions where the disclosure of personal information will be permitted in law such as for the prevention and detection of crime or safeguarding of vulnerable individuals. We will always seek a written request confirming the reason for the disclosure where consent has not been obtained and will evaluate that request before responding. Equally we need to make our own requests in a lawful and proper way.

Information sharing agreements

Any sharing of personal information between organisations may be best supported by an agreement that makes clear what is being shared, why and how. It helps us ensure we are complying with data protection legislation.

Further guidance on the completion of Information Sharing Agreements can be obtained from the Legal department of the Combined Authority.

Testing of systems

We may need to test that computer systems are developed to bring greater efficiency, benefits, and security work appropriately. In order to do so then we will need to consider using personal data in that testing. The first consideration will always be whether personal data is required for testing and the default will be that it is not with anonymised or randomly generated data being used. However, this may not fully test the functionality of a system, therefore consideration must be given to the use of a data snapshot from the live or current system.

We will undertake a data protection impact assessment prior to the use of any current or identifiable data to ensure that this is appropriate and that the appropriate safeguards are in place prior to the export, import and testing. The data will only be held in the test system for the period of testing and then removed. If the testing of the system is being undertaken by a partner or a processor then the same process will apply.

Privacy and the value of information

Data protection is all about privacy. When we use information about people then we have an impact on their privacy in some way.

This could be when we think about buying a new IT system or running a new project or service. It means we need to think about the impact on our customers; how will it affect them? Will it make a change on their lives? Are there any risks that we need to think about? The changes in data protection in 2018 made it mandatory that we have to consider the impact and show that we have. Please refer to the Data Protection Impact Guidance for further information.

Data Protection Impact Assessments (DPIA)

There are two levels of a DPIA; the screening process to work out whether you do need to do a DPIA is the starting point. This should always be completed whenever there are projects, new or changed service activities, or new ICT that could potentially impact on the privacy of individuals.

The completed screening checklist should be shared with the Data Protection Officer to determine whether any further assessment is required. They will inform you as to whether a DPIA is needed.

These can be published so it is important to make sure we have assessed impact and risk.

Only use what you need to use

It can be helpful to think about what level of information you need to use. Do you need to use every bit of information we hold about a person? Can you limit what you do use? You may only need ages and post code for example rather than their name, address, date of birth, NI number, health details and ethnicity.

There are other ways of using personal information without sharing who that person is.

Anonymisation of data

Data can be anonymised i.e. removal of information which could lead to the identification of an individual. It should be almost statistical because there should be no way that you can identify any individual person. It is not enough to remove the name and address. You should approach the Data Protection Officer for more detailed guidance.

Pseudonymisation

Where it is not necessary to share personal data but anonymised is not sufficient, then consideration should be given to the pseudonymising approach. This means when information is supplied it is not identifiable to the user but the individual producing the information has a “key” to identify.

Information as an asset

When information is organised, stored, used, and analysed then it is an asset that we can use. This means that we need to make sure it is managed properly. This management means that we know what we hold, where it is held, how long for and its qualities. This will help us use the information we have much more efficiently and better because we will understand it more.

Each service will have an Information Asset Owner (IAO) who is responsible for understanding that information, making sure it is only disclosed appropriately and is securely held.

Roles

Chief Executive

The Chief Executive has overall accountability and responsibility for data protection. The Chief Executive is required to provide assurance that all risks relating to data protection and information security are effectively managed and mitigated.

The Chief Executive has delegated responsibility for compliance with the Data Protection Act (including the implementation of this policy and other related policies) to Senior Information Risk Owner.

Senior Information Risk Owner (SIRO)

Robert Parkin is our SIRO. A SIRO is responsible for:

- leading and fostering a culture that values, protects, and uses information for the success of the organisation and benefit of its customers,
- overall ownership of the Information Governance policies,
- Act as the champion for Information Governance and provide written advice to the on the status of matters within the authority,
- owning the organisation's overall information risk policy and risk assessment processes and ensuring they are implemented consistently by IAOs,
- advising the Chief Executive or relevant accounting officer on the information risk aspects of his/her statement on internal controls,
- owning the organisation's information incident management framework, and
- ensuring that they receive appropriate training to fulfil the SIRO role.

Data Protection Officer

The Data Protection Officer will:

- manage the compliance with data protection legislation and FOIA,
- maintain an awareness of all IG/IM issues within the authority,
- review and update policies in line with local and national and best practice requirements,
- review and audit all processes and procedures where appropriate and on an ad-hoc basis,
- ensure all line managers and staff are aware of the requirements of these policies and guides,
- set a list of minimum expectations for security standards for IT systems.

Information Risk Group

The authority has a group chaired by the SIRO and attended by representatives of all services. This is a key group to determining strategy and having oversight of all things data protection.

Responsibilities of Managers

All managers are required to ensure that they and their staff understand this policy and any associated procedures. They are responsible for ensuring that staff are informed and updated on any changes made to this policy.

All managers must identify and report any risks or breaches to the Data Protection Officer.

All line managers must ensure that their staff undertake data protection training and refresher training which will be undertaken annually.

Additional responsibilities for Managers - Temporary Staff

It is a requirement that all temporary staff, agency staff, volunteers, work placement students and all managers requesting access to systems for these temporary workers, should read, and undertake to comply with these compliance guidelines. Managers should ensure that any such staff are trained and understand data protection responsibilities.

Responsibilities of Members

All Members have responsibilities in their own right and when considering the use of personal information for any particular purpose, they should take into account the context in which that information was collected to decide whether their use of the information will be fair and lawful.

Members should also refer to the relevant "Code of Conduct", which is intended to promote high standards of behaviour amongst the Members of the authority, and which is available on our website.

Responsibilities of all staff

All staff have a responsibility have a duty to abide by the authority's policies and procedures in handling personal data as well completing any mandatory training provided. They must report any risks or breaches to the Data Protection Officer.

Any breach of this policy or linked to data protection may be considered under the authority's disciplinary policies.

Policy Review

A review of this policy will take place annually to take account of any new or changed legislation, regulations or business practices.

Monitoring Compliance

Compliance with this policy and related standards and guidance will be monitored and findings will be reported to the Data Protection Officer.



**CAMBRIDGESHIRE
& PETERBOROUGH**
COMBINED AUTHORITY

Retention Policy

Type of document:	Guidance
Document produced by:	Cambridgeshire & Peterborough Data Protection Officer
Document approved by:	Cambridgeshire & Peterborough Combined Authority Board
Version :	Version 1
Issue date:	
How is this shared?	Electronically
Date due for review:	Annually April
Reviewer:	Rochelle Tapping Susan Hall

Data Protection Contact		
Contact Details	Email	Phone
Rochelle Tapping	dpo@cambridgeshirepeterborough-ca.gov.uk	07923 250218

Contents

Introduction.....	4
“If you only read this...”	4
Quick questions.....	4
How do I know how long to keep a record?	4
What do I do if I am not sure?	4
Should I use email as a place to keep records?	4
How do I destroy securely?	5
Whose responsibility is records management?	5
The Retention Schedule.....	5
Storing records.....	5
Accessing Records	5
Destroying records	5
Non personal information	5
Hard copies of records	5
Electronic files	6
Destruction record keeping.....	Error! Bookmark not defined.
Changing the way we hold information	6
Missing records	6
Who does what?	6
All of us	6
Data Protection Officer	6
SIRO	6
Registers	7
Monitoring and Review.....	7
Appendix A- Records Disposal Form	Error! Bookmark not defined.

Introduction

Information can be one of our most important resources we have. We have to manage it and that means making sure we keep information for the right length of time and destroy it securely when we don't need it any more. The implementation of good records management and records retention practices will benefit the authority in many ways.

It's not just about Data Protection Act 2018 ("DPA") or the UK General Data Protection Regulations ("UK GDPR"). The Freedom of Information Act 2000 plays a part as well and places a legal obligation on us to make available information we hold.

However, neither the Data Protection Act / UK GDPR nor the Freedom of Information Act tell you how long to keep something for. There is usually another piece of law that tells us that like HMRC rules or acts relating to children for example.

This policy applies to all records held whether they are paper copy, CD, on the network, cloud or computer systems.

"If you only read this..."

Do know how long you should keep a record

Do keep a record of what has been kept and where

Do make sure you destroy securely

Do make sure you destroy when you should

Do keep a record of what you destroy and when

Do ask the Data Protection Officer for advice and help

Don't keep personal information just because it could be useful

Don't ignore retention schedules, it is all part of good records management

Quick questions

How do I know how long to keep a record?

There is no hard and fast one timescale fits all approach. It will depend on the type of record and what legislation like HMRC rules says. Check the schedule for what the document is about and then we can determine how long we should keep it for.

What do I do if I am not sure?

Ask. It is better to double check and help make sure our retention schedule guidance is up to date.

Should I use email as a place to keep records?

No. You should not keep personal information about customers or staff you manage in your email. It should be saved to a line of business system or a network folder. If you leave, the authority still has a need to gain access to that information.

How do I destroy securely?

We have a shredding bag at Ely where you can securely dispose of paper. Records can be deleted from a system either by the team who support the system or the provider.

Whose responsibility is records management?

All of us.

The Retention Schedule

We have a retention schedule that sets out what we have and how long we keep it for. It should also list where the information is and it is important that this is updated when we move information.

You can access the retention schedule via our intranet pages. The schedule will be based on the LGA schedule here <https://retention.esd.org.uk/guidance>.

If you become aware of a new legal requirement, or code of practice, with respect to a specific type of record then please let the Data Protection Officer ("DPO") know.

If you see that something is missing, then please let us know. This is a live document and can change as we collect new information.

The DPO will provide advice, guidance and training where necessary.

Storing records

It is important that we have a few rules about storing records:

- We should know what records we hold and who they are about
- We should know where records are
- We should make sure they are secure and safe so we know who can access them
- We have someone who knows the above and keeps the schedule updated
- If we cannot find one then we have an audit trail of who accessed it last or what the last thing done was

Accessing Records

When we give access to records then we should make sure that we know why someone has should access them. It means knowing that they have a genuine business reason to do so. Just because someone is interested does not mean that they have a reason.

If you hold paper copies then you should have a system in place for recording what file has been accessed or removed, by who and when. It should then be marked back as returned. A bit like a library book.

Destroying records

Always take care when destroying information and make sure that it is ok to destroy.

If it has personal information in then check the retention schedule. If it doesn't then you should make certain that we can destroy it.

Non personal information

This could be emails, letters, circulars or documents. It may not contain personal information but it may contain confidential or business sensitive material. You should make sure that it is not still needed for audit purposes and then destroy it securely in the same way as personal data described below.

Hard copies of records

Paper records should be destroyed securely using the confidential waste bags. The authority has shredding bags at Ely which are dealt with under a contract and ensures that the paper copies are shredded professionally. If you have large amounts then you should speak to the Data Protection Officer who will assist in identifying a way you can do this. If a company is storing them on our behalf then we will ask for a certificate of destruction.

Please keep a list of what has been destroyed, when and by who.

Electronic files

All services will have electronic records held on secure systems. Access to these will be restricted to those who have a legitimate requirement for access and this access will have specific security processes like usernames and passwords.

Systems and databases will be subject to the business continuity policy, corporately and at departmental level, which ensures routine back ups and contingency plans are in place to maintain the records.

Where a case is closed or a record is no longer needed, it will be subject to the appropriate retention period and will then be securely deleted by either the support team or provider.

Please keep a list of what has been destroyed, when and by who.

Changing the way we hold information

If any records are being transferred such as being scanned then the previous versions can be disposed of securely. You should discuss this with the DPO and consider whether a data protection impact assessment is needed. This would help you identify and manage any of the risks.

If the records are being transferred to another organisation, it is essential that secure transporting arrangements are in place regarding the transfer. Contact the DPO for further information.

Missing records

We hope that we won't lose records but sometimes it happens. If this happens then you must report this immediately following the process described in our guide to what to do if we have lost some data.

After any incident, you should review what happened and why so that we can change or update processes to prevent recurrence. The DPO will help with this and help implement changes where necessary.

.

Who does what?

All of us

We need to think about whether we need to keep information, what we keep, where we keep it and how long for.

Data Protection Officer

The DPO will provide advice and guidance as well as maintaining the retention schedule, advising on timescales and helping ensure that information is kept securely.

SIRO

The SIRO is the senior officer with responsibility for security, risk and data. This means that they will receive reports on any issues such as lost files, incorrect records, or insecure storage.

Registers

The DPO will maintain the retention schedule and register of destruction.

Monitoring and Review

This policy shall be reviewed annually after implementation.



**CAMBRIDGESHIRE
& PETERBOROUGH**
COMBINED AUTHORITY

Data Protection Impact Assessments Guidance

Type of document:	Guidance
Document produced by:	Cambridgeshire & Peterborough CA Data Protection Officer
Document approved by:	Cambridgeshire & Peterborough Combined Authority Board
Version :	Version 1
Issue date:	
How is this shared?	Electronically
Date due for review:	Annually April
Reviewer:	Rochelle Tapping Susan Hall

Data Protection Contact		
Contact Details	Email	Phone
Rochelle Tapping	dpo@cambridgeshirepeterborough-ca.gov.uk	07923250218

Table of Contents

Introduction.....	4
“If you only read this...”	4
Who needs to do one?	5
What do I need to do?.....	5
Quick Questions – and quick answers!	5
We are just commissioning a service so we won’t be collecting the information ourselves?	5
We are only getting anonymised data from the provider to help us review their performance.	5
The project involves many partners so who does this and do we need more than one?	5
If I need help then is there someone to help me?	5
Is it a bit hard?	5
What is the process?.....	6
The Screening Checklist	6
Data Protection	7
Minimised? Pseudonymised? Anonymised?	7
Flows, Controllers, processors... ..	7
Checklist Yes or No’s	7
The DPIA.....	7
Project Information	7
Parties Involved	8
Data Flow.....	8
People.....	8
Legal Basis	8
Risks	8
Unmitigated & High Risks	8
Who does what?	8
All of us	8
Data Protection Officer	8
SIRO	8
Registers	9
Monitoring and Review.....	9

Introduction

Data protection is all about using information about people responsibly and transparently. Every time we use a piece of information about someone then we will have an impact on their privacy. This is because the information we hold about them is personal to them so if we misuse or lose it then their private information could become public or we make decisions which affect their life.

When we start using new systems, collecting new information, or providing a new service then we will need to think about the impact on our customers' private life.

We need to think "Privacy By Design" which means we build protecting our customers' privacy into every project. It means we balance what we want to do against someone's right to privacy – what is good for us is not necessarily good for them. You can find out more about the idea of Privacy By Design later in this policy.

To help us to do all of this then we need to think about how we assess that impact; such as making sure that we have considered the risks of what we are planning, how we will reduce those risks and importantly is what we are doing fair. This is called a Data Protection Impact Assessment or DPIA for short.

"If you only read this..."

Do make sure that you have completed a DPIA screening checklist before you start your project

Do explain clearly what the project is because not everyone is an expert in your area

Do make sure you confirm whether a DPIA is needed

Do make sure you know what the risks are and how you will mitigate them

Do ask the Data Protection Officer for advice and help

Don't think because we are commissioning a service that we are not responsible for the personal information

Don't think that this is for the Data Protection Officer to worry about, it's your responsibility

Who needs to do one?

Any one of us who is responsible for a project and/or managing a project needs to think about a DPIA. The project could be something brand new like a new service or new system or it could be changing a current service or system.

What do I need to do?

The change in data protection legislation made it mandatory for us to consider the potential impact on privacy that the project or service could have. The first step is to complete a screening checklist so that the Data Protection Officer (DPO) can determine whether you need to do a further assessment.

When do I need to do one?

You should do one at the start of the project or before you commission a service so that you have considered all the risks from the outset and can design processes that reduce or remove those risks.

Quick Questions – and quick answers!

We are just commissioning a service so we won't be collecting the information ourselves?

Maybe not but you are asking and paying someone else to do it on our behalf. They wouldn't do it if we weren't asking them to. This means that we have a responsibility for the use of that data.

We are only getting anonymised data from the provider to help us review their performance.

See above answer – to give you that data, they need to have collected the actual personal information that we asked them to. We have a responsibility for it.

The project involves many partners so who does this and do we need more than one?

No. The lead organisation needs to take ownership with the support of the other partners so there is just one DPIA but which covers all.

If I need help then is there someone to help me?

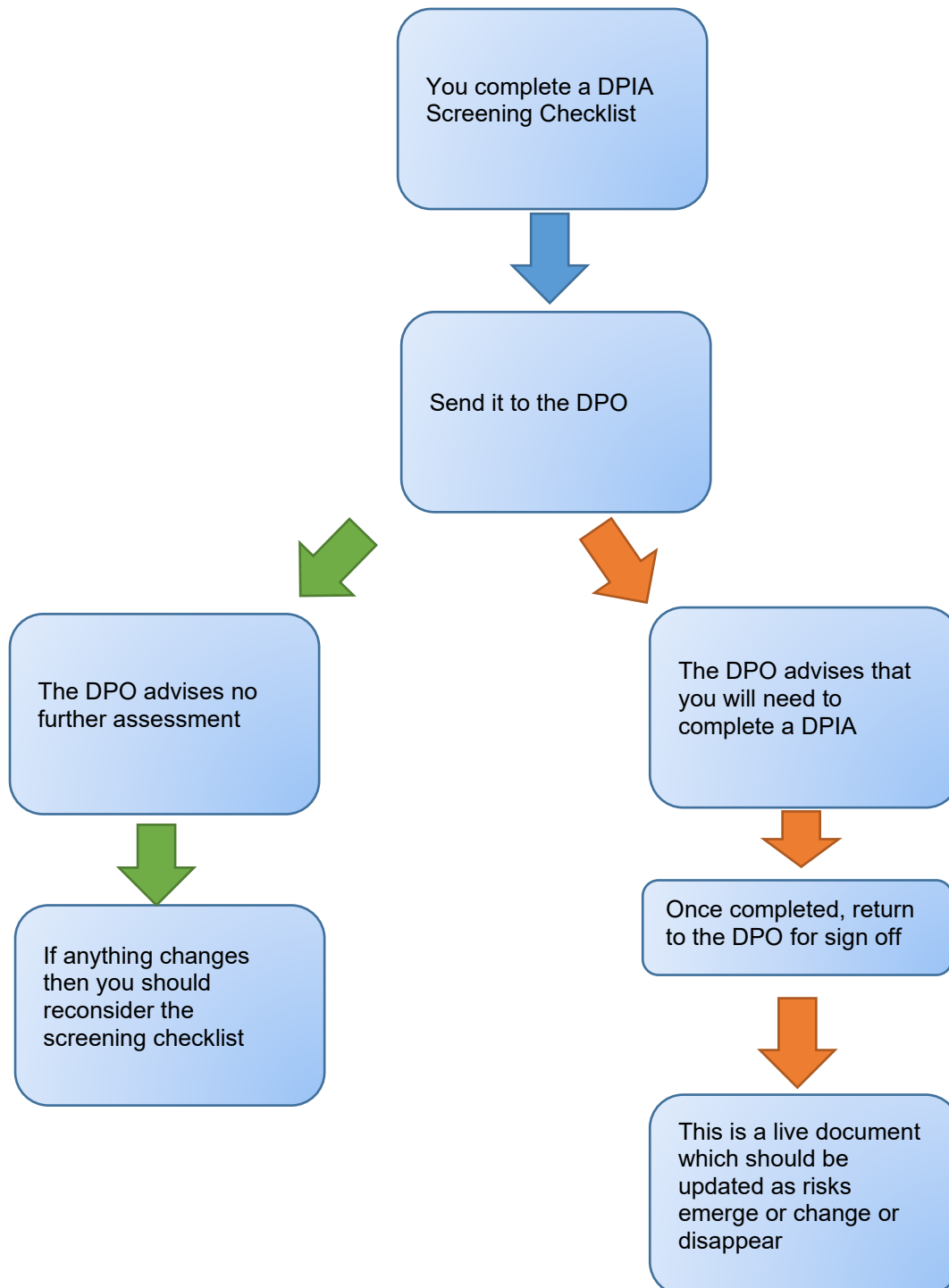
Yes the DPO is here for that. All we ask is that you explain in simple terms what your project is – what is about, what information is being used, about who and why. Remember you are the person who knows the most about your service, not us.

Is it a bit hard?

It may look like another bit of bureaucratic paperwork but actually it helps you understand what your risks may be beyond cost or deadlines. Knowing these and how you resolve them could help your project be even better.

What is the process?

The flowchart below shows the outlined process and links to further sections.



The Screening Checklist

This helps to show that you have considered privacy in your project. We need a clear and simple explanation of what your project is about. As well as the objective, we need you be clear on who is involved, what the benefits are and importantly what the risks are.

Remember we will not necessarily understand your service like you do so acronyms or abbreviations may not make sense.

Data Protection

It is also at this stage that we ask you to consider what information you actually **need** to use and **not** what is easiest or **not** just what you want. Just because using the full data on 1000 people is easier than having that data anonymised or pseudonymised does not make it right. It may also help you avoid more paperwork!

Minimised? Pseudonymised? Anonymised?

Minimised means that you have stripped back as much as you can. If you only need age and postcode then that is what you use rather than name, address and date of birth.

Pseudonymised means that we have replaced any data which could identify someone with a code known to us. So instead of John Smith we say Person 5TVRA. It means that we can back and re-identify John Smith if we need to.

Anonymised information means that we will not be able to identify anyone even if we wanted to.

Flows, Controllers, processors...

It is also here where we need to think if information is being shared between parties and why. This is important because along with why we have this project or why we have commissioned the service, then it helps determine who is a controller and who is a processor.

Checklist Yes or No's

There are then a series of questions we need you to answer yes or no to. There are four situations where a DPIA is mandatory – regular profiling and automated decision making, using special category data on a large scale, undertaking regular monitoring of public space and high risk processing.

In the screening checklist, you will see how these are explained. Whilst the first three are each a question, the definition of high risk processing could be a number of factors.

There is a second category where a DPIA may not be required but could prove useful and helps understand the information we are collecting and the risks with it. There may be some discretion here as to whether a DPIA is done but remember the DPIA can be a very useful way of making sure that we have thought of all the possible risks and benefits to our service users. It shows that we have thought about our service users and their privacy.

The DPIA

If a DPIA is required then we want this to be something that you can complete without it being too onerous or difficult.

The form covers a number of areas in more detail than the screening checklist but you can take some information from that to include in the DPIA.

Project Information

This covers much of what was in the screening checklist but also identifies why a DPIA is being completed.

Parties Involved

You should include all internal parties including the likes of Finance, Legal and ICT. Remember that all of these will have an input from costs to contracts to the system and its impact on the network.

It is also key to make sure that you have noted all external parties especially those who are acting on behalf of a party e.g. Serco acting on behalf of PCC or LGSS for CCC.

Data Flow

This section is really important. This is where we identify where information is coming from and going to, what we are doing with it and why, who will have access and why, how we will protect it, where it will be stored and how long for.

People

This is about the people whose data we are processing. We need to understand who they are, how we will explain what we are doing and how we make sure that we can meet their rights under data protection.

Legal Basis

Anything we do with personal information must be lawful. This means that we have a reason to do something with that data and we can say what that is. There are six reasons for processing personal information and ten for processing special category data. We need to pick one of each.

Risks

Whenever we process personal information, there will be risks and it is useful to identify those. Once we identify a risk then we need to say how we will mitigate or limit its impact and how we will know that this has been successful.

Unmitigated & High Risks

The assessment should highlight any risks we think we may encounter. It should also ensure that we have plans to reduce or eliminate those risks. If you believe that you have identified a risk which cannot be mitigated or even despite that mitigation remains high then speak to the DPO. We may have to discuss with the ICO if we want to go ahead with something which has such high risks.

Who does what?

All of us

We all need to think about a DPIA. We need to consider risks and how we mitigate them. Project managers and sponsors should ensure that a DPIA screening checklist is completed and any further assessments are also completed.

Data Protection Officer

The DPO will assess the screening checklist and determine the next action – no further action or a DPIA. They are also there to advise you and challenge you in the nicest possible way. Their job is to help you consider risks, mitigation and compliance. They may discuss the matter with the Information Risk Group.

SIRO

The SIRO is the senior officer with responsibility for security, risk and data. The SIRO will review and agree a full DPIA where necessary.

Registers

The DPO will maintain a register of screening checklists and DPIAs. They will also ask services to consider what information needs to be added to the Information Asset Register.

Monitoring and Review

There will be a quarterly report to the Data Protection Officer This will inform training and risk assessments.

This policy shall be reviewed annually after implementation.



DATA PROTECTION IMPACT ASSESSMENT

Key Information

Project Name:	
Project Manager:	
Responsible officer:	
This DPIA has been completed by:	

Project Information

This should include what the objectives are, the benefits and risks to the authority and service users plus explain why a DPIA has been completed.

--

Parties involved

Please provide a list of all internal parties involved and consulted

(include teams such as Finance, IT, Legal, Audit, Information Governance)

Please provide a list of all external parties involved and consulted

Is there or will there be a contract or similar between the authority and external parties which covers this work?

This is important to show that we have properly formed relationships which have robust agreements in place to protect the authority and our data.

Have you established if there are any sub-contractors involved and that suitable agreements exist

We need to be sure that we know who is processing our personal information and that we know about any subcontracting.

Data Flow

This is important because we need to show that we understand what is being collected or shared, who by and why, and how we make sure that this is all securely done.

What information is being collected? <i>It will help to provide a list and identify what special category data is collected</i>	
How will that information be collected and who will collect it? <i>Is the information being collected by email, application form, from another party etc</i>	
How will that information be used? <i>You should be clear on how it is going to be used. Will there be any profiling or automated decision making?</i>	
Who will information be received from? (internal and external) <i>This may be many sources but we need to understand the information flow between parties</i>	
Who will the information be shared with? (internal and external) <i>This may be many sources but we need to understand the information flow between parties</i>	
If information is being shared, how will it be shared securely? <i>You should identify how the information will be shared e.g direct access into a system, secure email, SFTP,</i>	
Who will have access to the information? <i>Access should be limited to only those required to have access</i>	

Where will the information be stored? <i>This should include the name of the systems for all partners, whether it is cloud or server based and if it is hosted by someone else</i>	
What security measures are in place? <i>Individual user accounts, passwords, two factor authentication, firewalls, restricted access, audit functions of the system or partner, locked cabinets</i>	
Do any of the parties have security or IG certification such as Cyber Essentials, Cyber Essentials Plus, ISO270001?	
How long will the information be kept for? <i>You should have a retention period specified by all partners.</i>	
How will it be destroyed? <i>You should have a process for how unneeded information will be disposed of, both for electronic and paper records.</i>	

People

This section is about the people whose data it is and how we will meet their rights under legislation

How many people will this affect? <i>This can be an estimate</i>	
What categories of people are they? <i>Children, adults, employees for example</i>	

How will people be informed about how their data is being used? <i>Will you be using a privacy notice, explaining to people when they sign up to a service or attend a meeting?</i>	
What plans are there to ensure that people's rights are met? <i>These are the rights of access, erasure, restriction, rectification, objection, automated decision making, data portability</i>	
<ul style="list-style-type: none"> • Can you delete data if required to? 	
<ul style="list-style-type: none"> • Can you produce all information about a person if required to? And in what format? 	
<ul style="list-style-type: none"> • Can you amend a record if required to? 	
<ul style="list-style-type: none"> • Can you restrict any action being taken on a records? 	
<ul style="list-style-type: none"> • Can you audit to see who has accessed records? 	
<ul style="list-style-type: none"> • If the system has automated decisions, can you override these if you need a human to make the decision? 	
<ul style="list-style-type: none"> • Can you stop processing if needed? 	
Will there be any consultation of affected individuals and if so how will you conduct this consultation? <i>Will you be contacting and discussing with people before implementation?</i>	

Lawful Basis

To process any information about person then we need to have a lawful basis or reason for doing so. We have to state this clearly in privacy notices for customers. This can be the most technical part of the DPIA so if you are not sure which is lawful basis it is then speak to the DPO and we will work with you. We need to identify the right one and we will help with that.

What is the purpose of collecting the information? <i>This is key because to process any personal information then we need a legal basis i.e. what allows us to do something so knowing the purpose is really key.</i>		
What is legal basis for processing the personal information? <i>It is most likely that you will be obtaining consent, having a contract with say an employee or a statutory duty. If it is a statutory duty then state what law or code of conduct makes it statutory.</i>	We will obtain or have obtained recorded consent	
	We have a contract with individuals to deliver this service	
	We have a legal obligation to process the information	
	We have a statutory duty to deliver the service	
	This statutory duty is named....	
	It relates the protecting someone in a life or death situation	
	We have a legitimate interest in processing this information and have completed a legitimate interest impact assessment.	
What is the legal basis for processing special category information? <i>You also need to specify a basis when we are using the special category data like health, ethnicity, sexuality or religion.</i>	We will obtain or have obtained explicit consent in writing	
	It relates to employment or social security. This includes health and safety, maternity/paternity and sickness	
	It relates the protecting someone in a life or death situation	
	It relates to the work of a not-for-profit body like a charity, political party or charity	
	The information has already been made public by the person	
	It is required for us to make or defend legal claims	
	We have a statutory duty to deliver this service	
	This statutory duty is named....	
	It is to deliver social care or health including occupational health	
	It is for public health reasons including monitoring and statistics or vaccination programmes	
	It is for archiving or research purposes	

Risks

Provide a list of risks and how you will manage, solve and mitigate these. To help you think about these, then we have broken down types of risks you may think of which include how they link to the principles of Data Protection.

<u>Lawful and fair use of data</u> Is the legal basis correct? Are you using an opt out model? Is it clear to people what you are doing with their data?	<u>Purpose</u> Have you explained what the purpose is to customers? How will you ensure that data is not used for different purposes that a person may not expect?	<u>Data minimisation</u> Is there any risk that data is being collected which is not required? Is there any risk that more data could be shared with partners or the authority than is needed?	<u>Accuracy</u> Are there any risks around receiving or sharing inaccurate or old data? What could happen if data is not updated or is collected incorrectly?
<u>Retention</u> Is there a risk that information could be kept too long? Or too short? Could partners keep information without us knowing?	<u>Security</u> Is there a risk of people accessing information that they should not? Is there a risk that information will not be stored or shared securely? Is there a risk that information could be misused?	<u>Accountability</u> Is there any risk about how service users understanding how their data is being used? Is there a risk that privacy notices are not clear or people cannot exercise their rights?	<u>Risks to the authority</u> There may be risks associated with what we are doing which could impact on the authority's reputation or systems.

Issue/Risk (indicate whether a risk to the individual or the authority)	Solution/Mitigation	Expected Outcome	How will this be monitored/evaluated

INFORMATION GOVERNANCE USE ONLY

	Sections	Comments
1	Project Information Are the aims and outcomes clear? Have benefits been identified?	
2	Parties Involved– Have all relevant services/teams have been identified and informed? Have all external parties been identified? Are contracts or ISAs in place?	
3	Data Flow Has all information to be processed been identified? Have all sources and means of processing been identified? Has appropriate security been identified? Has records management been considered?	
4	People Do we know who this will affect and how will they be told? Can their rights be met?	
5	Lawful Basis Has the lawful basis for processing been stated?	
6	Risks and Benefits Have all risks been identified? are risks sufficiently mitigated? What controls need to be introduced? Has a balance between the two been found? Is there a plan for monitoring?	

IG	Overall assessment What needs to change? if anything	

SIGN OFF			
Sign off	Title	Signature	Date
	Lead Officer		
	Director/Senior Responsible Officer		
	Data Protection Officer		
	SIRO		



**CAMBRIDGESHIRE
& PETERBOROUGH**
COMBINED AUTHORITY

Data Incident Reporting Policy

Type of document:	Guidance
Document produced by:	Cambridgeshire & Peterborough CA Data Protection Officer
Document approved by:	Cambridgeshire & Peterborough Combined Authority Board
Version :	Version 1
Issue date:	
How is this shared?	Electronically
Date due for review:	Annually April
Reviewer:	

Data Protection Contact		
Contact Details	Email	Phone
Rochelle Tapping	dpo@cambridgeshirepeterborough-ca.gov.uk	07923 250218

Table of Contents

Introduction.....	4
“If you only read this...”	4
The important bits	4
What is a data breach?	4
What kind of incidents do you mean?	4
When does it become a breach?	5
How do I report something?	6
What happens after I report something?.....	6
Contacting those affected	6
Roles and Responsibilities	6
All staff.....	6
The Data Protection Officer.....	6
The Affected Service.....	6
The Service Lead	6
Contacting the ICO.....	7
Complaints about breaches	7
Putting it right for good	7
How does the DPO assess impact and risk?.....	7
Monitoring and Review.....	8
Appendix A – Data Incident Reporting Form	9

Introduction

We have to protect the data that we have. We have a lot of data on different customers and staff. This can include personal and sensitive information but also, for example, commercially sensitive information or simply data. We have to have processes in place to do this but sometimes things do go wrong.

When information is lost or shared inappropriately, it is vital that appropriate action is taken to minimise the impact and risk as soon as possible.

“If you only read this...”

Do make sure that you know who you are talking to

Do make sure you only share information with the right person

Do make sure you check envelopes or emails to make sure they have the right information

Do check postal and email addresses before you send

Do know what to do if something goes wrong

Do report any concerns

Don't ignore a breach

Don't ignore a customer complaining about a breach

The important bits

If we get it wrong, then our customers and residents could be at risk

If we get it wrong, then we could be fined the equivalent of £17.5 million or 4% of total worldwide income by the Information Commissioner

If we get it wrong, then people can sue us if they suffer detriment

If we get it wrong, then we have to spend more time fixing the problem than it would have taken to make sure we were not getting it wrong

What is a data breach?

A data breach is something which affects people's rights and freedoms.

When something is reported then we will call it a data incident until we have assessed it as a breach. If we say it is a breach, then it must be reported to the Information Commissioner within 72 hours and if it's a high risk then people whose data it is.

All reports will be considered as a data incident until we can determine the risk to the data subjects

What kind of incidents do you mean?

A data incident is more than if we just lose some information. It can be where:

- personal information is disclosed to someone who does not have the right to see it. It could be documents, a spreadsheet or just an email.
- The loss of information
- The corruption of information
- The unavailability of information
- The data being incorrect

It can be caused by

- Loss or theft of data or equipment on which data is stored
- Deliberate or accidental action by someone
- Not having the right access controls allowing unauthorised use
- Equipment failure
- Human error
- Unforeseen circumstances such as fire or flood or power cut
- Hacking
- 'Blagging' offences where information is obtained by deception
- Alteration of personal data without permission
- Virus attacks

If there is personal information and/or sensitive personal information as defined in this policy contained within the document, email etc. then this must be reported.

Data could also be disclosed which is not personal but reveals information of a commercially sensitive nature or is confidential. This can also have an impact on us but would not need to be reported to the ICO.

When does it become a breach?

We will consider that all incidents have an element of risk to someone and take the same actions in all cases.

Once we have the facts then we will determine what that level of risk is.

The Data Protection Officer (DPO) along with the SIRO (Senior Information Risk Owner) will determine this. This will include a risk assessment which will cover the following:

- **Whether any personal data has been lost or whether it is a loss of data**
- **The potential harm or risks to the data subject as a result of the incident**, including any distress the data subject may suffer as a result of the incident
- **The volume of the data involved** – this must be determined by the facts and extent of the breach
- **The sensitivity of the data involved** – where the data is classed as sensitive personal data and the release of that data can lead to the data subject suffering substantial harm.
- **Assess the impact of the breach such as:**
 - How could the loss of control over the personal data affect someone?
 - Could it cause discrimination?
 - Could it cause identity theft or fraud
 - Could it cause financial loss?
 - Could it cause embarrassment and upset?
 - Could it cause damage to reputation?
 - Could it cause loss of confidentiality?

The DPO along with the SIRO and Chief Executive will decide if we need to inform the Information Commissioner's Office (ICO) and/or the people concerned.

Please refer to The IG Risk Assessment to ensure that the incident is appropriately categorised. The DPO will assess the breach using the Assessment Form. Where an incident indicates a risk, it may be necessary for other services to be informed.

How do I report something?

Use Appendix A and send this to dpo@cambridgeshirepeterborough-ca.gov.uk.

If it is urgent then phone to speak to the Data Protection Officer on 07923 250218.

If the incident occurs or is discovered outside normal working hours, the investigation and notification of relevant officers should begin as soon as is practicable either by text or email.

What happens after I report something?

The DPO will make an initial assessment based on what they have been told. They, in conjunction with the affected service, will determine what steps are taken.

Contacting those affected

When we contact customers to tell them what has happened then we need to be clear on what has happened, how and what we are doing to put it right.

The Responsible officer should do this when it is decided that people are at sufficient risk.

Roles and Responsibilities

All staff

All of us have responsibility to report a concern. The service manager/lead will have responsibility for reporting an incident/breach directly to the DPO and establishing what has happened/informing the DPO of the incident details.

The service manager/lead, or someone in their absence, should take immediate action to recover any documents, whether electronic or hard copy, and put measures in place to prevent future breaches.

The Data Protection Officer

They will maintain a central log of all breaches as reported and provide advice on actions to be taken.

An investigation will only be undertaken by the DPO when requested to do so by the director or Chief Executive and only in specific circumstances.

In the event of a complaint being made to the ICO, the DPO will act as the collator of information to provide the response in conjunction with the IG.

The Affected Service

When an incident occurs then the service affected will undertake an investigation or review. They will nominate an individual to lead on investigating and gather information which should be at the level of manager or above. We can call them the **Service Lead**. Their role helps to add background and context to an incident that only someone from the service can give. They will need to gather information on what has happened and liaise with the DPO to determine what actions should be taken.

The Service Lead

The Service Lead will be responsible for any communication with data subjects who have been affected by the data breach. Any response must be checked by the DPO, responses should be as

quickly as possible and no later than 10 working days. The Service will initiate disciplinary action / provide supervision or training if required (as appropriate)

Contacting the ICO

Once we decide this then the DPO or deputy will complete the referral.

The 72 hour clock starts from the moment we determine a breach. There may be a delay between the incident being reported and that decision while we gather information. We will explain the reasons for this to the ICO in the referral.

Complaints about breaches

Sometimes customers make complaints about data breaches to a central complaints team or as part of a wider complaint about a service. The DPO should be made aware of such complaints however the service should take the responsibility for investigation and review as they would in any event, and liaise with the DPO/IG on the response to this aspect of the complaint.

Complaints officers must ensure that they inform the DPO of any suspected incident as soon as they become aware of it to ensure that we can still meet our timescales.

Putting it right for good

Regardless of whether there was a risk or not, we have to make sure that we do not repeat mistakes.

We need to look at the processes and systems which may have caused the incident and work out what we can do to stop it repeating.

This may mean:

- Reviewing how information is held and shared
- Looking at what extra security checks we can put in place
- Introducing peer checks of envelopes
- Providing extra training on systems
- Raising awareness through meetings
- Restricting access and auditing systems, implementing technical and organisational measures, e.g. disabling autofill.

The DPO will assess the risks, impact, changes needed and discuss the implementation of changes with the Service Lead. The DPO and the Service Lead will ensure that change is implemented to prevent repeats.

How does the DPO assess impact and risk?

The impact of the breach will be assessed by the DPO using the Impact assessment. We will look at the following kinds of questions:

Was any data lost or compromised in the incident?
--

For example, if paperwork was in the wrong envelope or the email went to the wrong person. However, if you lost an encrypted laptop or phone then there may not be an issue unless you were logged in when you lost it.
Was personal data lost or compromised? This means is the data about living individuals such as customers or employees. This makes a data protection incident.
If yes, was <u>sensitive</u> personal data compromised? This is the really sensitive stuff like health, sexual life, political or religious beliefs, potential or actual criminal offences. If this happens then it is more serious.
What is the number of people whose data was affected by the incident? Large numbers of people affected can be more serious but equally a very sensitive piece of information about one person can also be serious.
Is the data breach <u>unlikely</u> to result in a risk to the individual/individuals? This means is anyone unlikely to be affected; this means that although data has been lost, it is unlikely to have an affect if we can recover the information or contain the issue.
Did people affected by the incident give the information to the authority in confidence? People often do expect it to be confidential even if it is not particularly sensitive
Does this incident put anyone at risk of physical harm? If it does then this makes it a more serious matter because we have to make sure customers and employees are kept safe
Is there a risk that the incident could lead to damage to individuals e.g. via identity theft/ fraud? If we lose bank accounts details or ID documents, then these could be used by to commit crimes.
Could the incident damage an individual's reputation, or cause hurt, distress or humiliation e.g. loss of medical records, disciplinary records etc.? Even if the loss does not put them at risk of physical harm or fraud, it can still cause distress if information about a person is made public. It can cause upset and hurt which we need to consider properly
Can the incident have a serious impact on the authority's reputation? The authority has to keep the trust of its customers. If we don't then they may stop working with us. Media stories can also cause this as can referrals to the ICO.
Has any similar incident happened before in the section? A one off error may be unavoidable but repeated incidents of the same kind in service or team can show that we have to change processes to stop repeats.
Do HR need to be involved or referred to? This is maybe because the issue is one of capability, or because of deliberate and malicious actions to cause the breach.
If this incident involves the loss or theft of IT Equipment has an urgent call been logged with ICT? The sooner we can block or wipe the device, the better.

Monitoring and Review

There will be a quarterly report to the Data Protection Officer and an annual report to the CA Board.

This will inform training and risk assessments.

This policy shall be reviewed annually after implementation.

Appendix A – Data Incident Reporting Form

Once completed, please send a copy to dpo@cambridgeshirepeterborough-ca.gov.uk and retain a copy for your records.

	To be completed
Reported by	
Responsible officer	
Department	
Team within Department	
Date and time of when the incident occurred	
Date and time reported to DPO	
Date and time you become aware of the incident	
Reason for delay if any	
Does this incident affect any other parties?	
How did you become aware of the incident?	

What kind of incident is this?	
How many individuals could this incident affect?	
Subject names and details	
What kind of people are affected?	
Are these people aware?	
Ease of identification of individuals	
Type of data lost* Delete where applicable	
Summarise the incident and the information that has been lost	
Actions Taken by service to mitigate, recover etc.	
What impact does this have on the individuals involved? What is the risk to them?	
Risk to subjects	
What is the impact on the authority and its business?	
Temporary or Permanent Loss	

Please complete the following checklist to confirm what actions you have taken:

Have you informed your director? (include name of director)	
Has an extensive search for any physical loss been undertaken?	
Have you been able to retrieve the lost data?	
Has the lost data been destroyed?	
Have you reviewed procedures to prevent recurrences?	
Is there likely to be media interest as a result?	

Data Protection Impact Assessment

Screening Checklist

(To be used by the officer planning to commission a service, only where a large volume of Personal Data is expected to be handled or high-risk projects will be undertaken in relation to Personal Data)

This form will allow you to establish whether your project or commissioned service is likely to need a DPIA as well as what you are sharing and why. It will also help with the procurement and contract because it gathers information we need to know what clauses we need to include to protect the authority and its customers. Once completed send to the DPO for record retention.

Key Information	
Project Name:	
Project Manager:	
Responsible officer:	
This checklist has been completed by:	

Project Information
What does the project aim to achieve? <i>This needs to be in clear and simple language. Remember people reading this are not subject matter experts in the way you are.</i>
Who are the parties involved? <i>This could be the authority, service providers, health partners or internal colleagues.</i>
What the benefits will be to the organisation? <i>This could be a better service, streamlining the process, making savings or enabling our staff to work more effectively</i>
What are the benefits to service users?

<i>This should carry out equal weight to the benefits to the authority. It could be a better service because it helps coordinate all the different people working with a client or making it easier to contact us.</i>
Are there any risks to the service user and/or the authority? <i>This is about identifying any risks such as sharing too much information, storing information in the cloud, sharing with new partner. This is important because we need to say what we will put in place to prevent these impacting on service users or the authority.</i>
Is this a new project? If so, then what is the expected go live date

The next questions are asked because we need to understand what information is being used and whether this is about people. Whether we are dictating exactly what someone does with the information or whether we are asking them to deliver a service on our behalf or whether they will just be sending us some performance data, someone is using data about a person.

Data Protection	
Will anyone in this project collect, share or use information about people? Such as service users, employees, customers. NO - If the answer is no, you do not need to complete this form – a DPIA is not required. YES - If the answer is yes, please continue.	
Describe what kind of information will this project/service need? <i>You should also think about whether you do need full, minimised, pseudonymised or anonymised information. If you state that it needs to be anything other than anonymised then you need to list what it kinds of information it will use e.g. names, addresses, health, social care and so on.</i>	
Describe what if any information the authority will share with any party and why? <i>This could be referring a customer to a provider so we need to give the provider that information to deliver the service</i>	
Describe what if any information the provider/party will share with the authority and why? <i>This could be feeding back into a social care case, providing performance statistics or a report on progress of the service</i>	
Are we asking another party to do the work as if we were delivering it? <i>This is important for us to understand the way the service is going to be delivered</i>	
Do we specify exactly what they can do with any data they collect, or can they determine what they do? <i>This is helps us understand who is a controller and who is a processor.</i>	

--

Mandatory data protection impact assessments If one of the following situations apply then you must complete a DPIA			
	Example	Yes	No
Are you going to be regularly using software to analyse and predict behaviour which helps to make significant decisions about people?	<i>This could be software which we use every week or month to look at personal data and analyse what people are doing so that we can tailor services to them</i>		
Are you using sensitive personal data like health, sexuality or criminal offence data on a large scale?	<i>This could be using introducing a new system to use lots of information about social care service users</i>		
Are you regularly monitoring a public space on a large scale?	<i>This will most likely be CCTV or other such monitoring systems</i>		

High Risk Processing It is also mandatory to complete a DPIA where what we are doing could be considered <i>high risk</i> . If one of the following situations applies then we will also need to complete a DPIA			
Question	Example	Yes	No
Are you using new technology like artificial intelligence or “internet of things” devices like smart meters?	<i>This may be information that we already hold but we are going to use new technology to do something different with it</i>		
Are you using software to profile and make automated decisions as a one off to make decisions on whether someone can access a service?	<i>This means that we use software to analyse data we hold and automatically decide whether someone should get a service from the authority</i>		
Are you using sensitive personal data like health, sexuality or criminal offence data to make decisions on whether someone can access a service?	<i>This means that we use sensitive information about people to decide whether they should receive our support. This could be social care, SEN or youth offending data. It could be the most private data about them.</i>		
Are you going to be analysing or predicting behaviour of lots of people?	<i>This may be a one off piece of work but we may use software to look at hundreds of people and try to analyse their actions</i>		
Are you going to be using biometric or genetic data?	<i>This could be DNA we collect or using fingerprints as a means of authenticating access to a system</i>		

Are you going to be data matching from a number of sources?	<i>This could be combining different data sets to create a single one such as identifying people who have not registered for something</i>		
Are you going to use personal data without informing the people whose data it is?	<i>We should explain to people what we are doing with a privacy notice however there are some situations such as fraud investigations when we will not tell people.</i>		
Are you going to track someone's online or offline locations or behaviour?	<i>We could be taking IP addresses, access to apps or social media for example to track where service users are and understand their activities</i>		
Are you going to be using the personal information of vulnerable children and/or adults?	<i>We have to take greater care when we are using data about those who are most vulnerable</i>		
Are you making decisions about people who we have power over and would not ask them for the consent?	<i>We have power over our employees or others because of the contract we have with them which means we can make decisions without their consent</i>		
Are you going to be using children's personal data to analyse behaviour, make any automated decisions, offer marketing or services directly to them?	<i>Anything that involves gathering information directly from children means that we need to take greater care</i>		
Are you processing the kind of personal information which could put someone at risk of harm if it was misused or lost?	<i>This means that if this information was lost, could it cause someone distress or damage? Could they be at risk of identity fraud?</i>		

People focussed DPIA			
Whilst it is not mandatory, it can be helpful if we are doing something new to think about it			
	Notes	Yes	No
Are you going to be obtaining new information from people?	<i>This could mean we are starting a new service and need to obtain information from people for the first time</i>		
Are you going to take information we already have and use it for something new?	<i>We may hold a list of people who have been consulted about a property development and want to use it in transport planning project</i>		
Are we obtaining information about people from new organisations?	<i>We may be entering a new partnership and be sharing information with a new provider, as well as getting it back</i>		
Are we sharing information about people with new organisations?			
Data Protection Contact			
Contact Details	Email	Phone	
Rochelle Tapping	dpo@cambridgeshirepeterborough-ca.gov.uk	07923250218	

Data Incident Reporting Form

Once completed, please send a copy to dpo@cambridgeshirepeterborough-ca.gov.uk and retain a copy for your records.

	To be completed
Reported by	
Responsible officer	
Department	
Team within Department	
Date and time of when the incident occurred	
Date and time reported to DPO	
Date and time you become aware of the incident	
Reason for delay if any	
Does this incident affect any other parties?	
How did you become aware of the incident?	
What kind of incident is this?	

How many individuals could this incident affect?	
Subject names and details	
What kind of people are affected?	
Are these people aware?	
Ease of identification of individuals	
Type of data lost* Delete where applicable	
Summarise the incident and the information that has been lost	
Actions Taken by service to mitigate, recover etc.	
What impact does this have on the individuals involved? What is the risk to them?	
Risk to subjects	
What is the impact on the authority and its business?	
Temporary or Permanent Loss	

Please complete the following checklist to confirm what actions you have taken:

Have you informed your director? (include name of director)	
Has an extensive search for any physical loss been undertaken?	
Have you been able to retrieve the lost data?	
Has the lost data been destroyed?	
Have you reviewed procedures to prevent recurrences?	
Is there likely to be media interest as a result?	



CAMBRIDGESHIRE & PETERBOROUGH COMBINED
AUTHORITY –
DRAFT MINUTES

AUDIT AND GOVERNANCE COMMITTEE: MINUTES

Date: 24th September 2021

Time: 10:30am

Location: Fenland District Council

Present:

Mr John Pye
Cllr Ian Benney
Cllr Tony Mason
Cllr Graham Bull
Cllr Mike Sargeant
Cllr Graham Wilson
Cllr Shaz Nawaz
Cllr David Brown

Chairman
Fenland District Council
South Cambridgeshire District Council
Huntingdonshire District Council
Cambridge City Council
Cambridgeshire County Council
Peterborough City Council
East Cambridgeshire District Council

Officers:

Robert Parkin
Anne Gardiner
Jon Alsop
Louise Davis
Robert Fox
Amina Adebayo
Adam Goldsmith

Monitoring Officer
Scrutiny Officer
Chief Finance Officer (S73 Officer)
Internal Auditors (RSM)
Governance Officer
Legal Governance Officer
SOCITM

1. Apologies for Absence and Declarations of Interest

- 1.1 No apologies received.
- 1.2 No declarations of interest were made.

2. Chair's Announcements

- 2.1 Annual Accounts and AGS

We were expecting to bring the final version of the 2020/21 financial statements and Annual Governance Statement to this Committee meeting for final approval, along with the external auditors' Audit Results Report. Members would recall from the last meeting that we were waiting to receive the actuary's IAS19 report on the final pension balances to complete the final version of the accounts and for EY to complete their audit.

We had recently been informed by EY that as a result of "commentary by regulatory bodies" to other audit firms, EY needed to update their procedures around verification of data. Mark Hodgson, the EY partner responsible for the CPCA audit advised that due to their requirement for additional audit evidence, they could not provide assurance that they would be able to issue and sign the audit opinion by the date of this Committee meeting.

Given the uncertainty of the audit position, I decided to withdraw the financial statements and external audit papers from the agenda, and to reschedule them for the November meeting.

The auditors also had a requirement to review the Annual Governance Statement for completeness, compliance and consistency with the financial statements, so the final approval of the Annual Governance Statement would also be deferred until the November Committee meeting.

- 2.2 Informal Session to review the Constitution prior to the Committee's next meeting to be scheduled.

3. Minutes of the last Meeting

- 3.1 The minutes from the meeting held on the 30th July 2021 were agreed as a correct record.
- 3.2 The Actions from the previous meeting were noted.

4. Combined Authority Board Update

- 4.1 The Chair advised that the Chief Executive was unable to attend the meeting but had advised the Chair that there was nothing to report in addition to the information contained within the reports going to the Combined Authority Board on the 29th September 2021.

5. Internal Audit Progress & Annual Report

- 5.1 The Committee received the report which provided the annual internal audit report for 2020/21 and requested that the Committee note the progress being made against the internal audit plan for 2021/22.
- 5.2 The Chief Finance Officer introduced the reports stating that the two reports were those deferred from the last meeting. The first report was the Annual report that included references to the ICT review which had been given minimal assurance; the Combined Authority took immediate action to employ SOCITM who had been working on the issues raised within the review.

The second report was an update on the Internal Audit Plan – officers had received a question prior to the meeting regarding the payment review – this had been approved by CMT earlier in the week to respond to concerns around recent payroll errors including pension contributions – the Combined Authority had requested that RSM review the current arrangements and agreements and whether there were sufficient in house capabilities.

- 5.3 The Head of ICT for SOCITM was in attendance to respond to queries regarding the ICT Review and advised that SOCITM contract was in place until January 2022 with the possibility of an extension of three months if required whilst the CA went out to

tender. A lot of progress had been made and SOCITM would have completed all the actions required from the audit by the end of the contract.

The Monitoring Officer advised that the CA were looking to go out to market and were confident that the timeline would be met.

The Committee were advised that there was no internal ICT at the Combined Authority and that senior officers had requested that RSM look into the ICT arrangements to ensure things were being done correctly.

The Monitoring Officer provided some clarity around the ICT situation – SOCITM was operating as a service provider for the Combined Authority; the items around the ICT review had not yet been re-audited following the intervention of SOCITM but there was every confidence that once this had been carried out there would be a positive assurance provided by the Internal Auditors which would be reported to the Committee.

- 5.4 In response to a query about the audit on risk the Monitoring Officer advised that there was a piece of work being undertaken by the governance team where RSM had been invited to work with the CA to ensure that risk within the Combined Authority was operating properly and this should be completed in the next 6-8 weeks and any changes to the strategy would be brought back to this committee.
- 5.5 The Committee were advised that the way the Head of Internal Audit formed his opinion was based on whether actions were being taken on any review that received minimal assurances and whether issues were being effectively addressed. Although there may be a minimal assurance the Internal Auditor could still give a positive assurance for the whole organisation if it was seen the Authority was taking action to address outstanding issues.
- 5.6 The Chief Finance Officer advised that RSM had recently been appointed as the Combined Authority Internal Auditors; they had reviewed all the risk registers for the Authority to highlight where the key areas of risk were. There were some areas which had been fast tracked such as the ICT and Payroll, but there would be ongoing work for the auditors as they reviewed risks that were up and coming for the Authority.
- 5.7 The Committee queried whether RSM also provided an advisory role for the Combined Authority as well as providing the recommendations from their reviews; RSM advised that this was an area they could get involved with. The Committee requested feedback on how the Internal Auditors could become involved in the development of policies and project management at the CPCA be provided within the next Internal Audit update.
- 5.8 The Committee AGREED to:
 - a) Receive and note the annual internal audit report for 2020/21 as provided by the Combined Authority's internal auditors, RSM Risk Assurance Services LLP (RSM).
 - b) Receive and note the internal audit progress report for 2021/22 as provided by RSM
 - c) The Committee requested that feedback on how the Internal Auditors could become involved in the development of policies and project management at the CPCA be provided within the next Internal Audit update.

6. Combined Authority Trading Companies

- 6.1 The Committee received the report from the Monitoring Officer which provided draft terms of reference in relation to the review and assessment of the Combined Authority's trading companies in line with the statutory powers invested in the Committee.
- 6.2 In response to a query – the MO advised that the new Terms of Reference could be presented to the CA Board to enshrine them and ensure that the shareholder transmits them onto the companies. In addition, it could be put into the Constitution that the formation of any new company for the CPCA should include asking the A&G Committee to comment on the proposed governance arrangements.
- 6.3 The Committee needed to continue to explore the arrangements for each of the companies, and information would be provided to the members to aid this. There was a role for the Audit and Governance Committee to assess the CPCA's governance relationship with the companies.
- 6.4 In response to a question about whether the Committee could change the relationship between the CPCA and a company, the Chair advised that the Committee's role was to consider the appropriateness of the governance and controls that the CPCA put in place. The companies were independent entities operating within their own legal framework.
- 6.5 The Committee raised a concern around the wording that stated that the Committee 'ensures the internal controls' of a company. Officers were asked to re-consider the wording and number of points in the Terms of Reference to make sure they align with the A&G function. The Committee would be operating at arm's length with no direct relationship with the companies and how they operated.
- 6.6 One member suggested that officers should seek advice and investigate what other councils did to define the governance arrangements of their companies.
- 6.7 The Chair stated that this had been a useful discussion and had highlighted some issues with the Terms of Reference which officers needed to address before they were included within the Constitution review.
- 6.8 The Committee RESOLVED not to accept the terms of reference of the Committee in relation to the Combined Authority trading companies as they had been presented but to request that:
 - 1) Officers consider the wording of the Terms of reference to reflect the position and role of the Committee at the CPCA in relation to the relationship with trading companies.
 - 2) Officers reach out to other combined authorities and councils to seek their experiences of governance in this area and report back any findings to the Committee.
 - 3) Internal Audit be approached to discuss their potential involvement with the governance arrangements for trading companies and to provide an insight into a possible way forward.
 - 4) An update on these above actions should be provided at the next meeting.

7. One CAM Referral

- 7.1 The Committee received the report on the potential scope for an internal audit review of a Mayoral decision to pause the One Cam project in advance of the consideration of such a decision by the Combined Authority Board.

- 7.2 The Committee were advised that that the purpose of the review was to assess whether or not the decisions made were within the powers vested in those involved, The nature of the decisions was outside the scope of the review. In other words, did the decision-makers have the authority (competency) to make the decisions.

The officers agreed that the 'outside the scope of the report' would be re-worded to reflect that it was the competency of the decisions made by the CA Board and Executives of One CAM that would be in scope.

- 7.3 The Committee requested that the scope be amended to:

a) remove the third bullet point stating: 'is there any spend/spending commitment from the Combined Authority itself on the CAM programme or has it all been directed through One CAM Ltd' be removed from the scope as it was not relevant.

b) that it was the nature of the decisions made by the Mayor, CA Board and Executives of One CAM that would be out of scope.

- 7.4 The Committee AGREED subject to the above amendments to approve the scope for an internal audit review of a Mayoral decision.

8. Business Board – Format of Meetings

- 8.1 The Committee received the report which sought agreement to the proposed format change to allow meetings of the Business Board to be carried out in public (unless otherwise determined by the Chair) and make recommendation to the Combined Authority Board to approve the change.

- 8.2 The Committee were advised that the Business Board, as the LEP for the area, was not subject to the same regulations set out in the 1972 Local Government Act that other committee and council meetings were; the amendment which had been accepted by the Business Board captured the switch in the presumption which the Audit and Governance Committee had requested – there was no request to import detail on the protocol to how that would be applied.

- 8.3 The Chair advised he had met with the Business Board Chair, who was quite open to Audit and Governance Committee members attending any meeting of the Business Board. He had emphasised that the Business Board was keen to demonstrate that they operated as transparently as the nature of their business allowed..

- 8.4 The Committee requested that a vote be taken for the recommendations.

Following a vote with 6 votes FOR and 1 AGAINST the Committee AGREED to:

a) Note that the Business Board were asked to reconsider the recommendation from the Audit and Governance Committee, 'that there should be a presumption that meetings of the Business Board are carried out in public (unless otherwise determined by the Chair)'.

b) Note that the Business Board agreed the proposed change in meetings format on 14th September 2021.

c) Recommend the Combined Authority approve the proposed format change for future Business Board meetings.

9. Work Programme and Updated Terms of Reference

- 9.1 The Committee received the report which provided the Committee with the draft work programme for Audit and Governance Committee to note and requested that the

Committee consider and review the updated terms of reference at Appendix 1, which deals with the referral of matters to the Committee to consider under their work programme.

9.2 The Committee AGREED:

- a) the updated terms of reference for the committee.
- b) to note the current work programme for the committee.
- c) to hold an informal session to receive a Horizon Scanning update from Directors.
- d) to hold an informal session the week commencing the 25th of October to consider the constitution review.

10. Corporate Risk Register

- 10.1 The Committee received the report which provided an update on the Corporate Risk Register.
- 10.2 The Committee requested that the CA Board consider whether they were satisfied that officers had considered the effect of increasing energy prices and the impact on supply chains when factoring the scores for the risks.
- 10.3 The Committee noted the Corporate Risk Register.

11. Information Governance Update

- 11.1 The Committee received the report which updated the Audit and Governance Committee on the current position with regards to the GDPR Policy and Information Governance Policy as recommended by the Information Governance Report prepared in October 2020 and put before the Audit and Governance Committee on the 5 March 2021 and provided data related to the number of corporate complaints and Freedom of Information requests for the period of 1 June 2021 to 31 August 2021.
- 11.2 In response to a question about whether constituent councils or external partners were signed up to the Combined Authority Data Protection Policy, the Monitoring Officer advised that GDPR would form part of any contract between any external organisation that the CA worked with.
- 11.3 In response to a query about how the reference to 'service users' was applied to the Combined Authority as a strategic body, the Committee were advised that this was relevant in the context of the passenger transport function which the Combined Authority had recently taken on.
- 11.4 The Committee AGREED to:
 - a) Note the Information Governance Update
 - b) Note the data on corporate complaints and freedom of information requests for June 2021 to August 2021
 - c) Note the new GDPR Policies for the Combined Authority set out at Appendix 1 to 7.
 - d) Recommend to the Combined Authority board that it approves and adopts the GDPR policies
 - e) Recommend the Combined Authority delegated authority to the Monitoring Officer to make consequential amendments to those Policies as required.

12. Date of next meeting

- 12.1 The next meeting would be held on the 26th November 2021

Venue: New Shire Hall Alconbury

Session to be arranged for Horizon Scanning with Directors – a face to face meeting if possible.

Session to be arranged w/c 25th October – Constitution review.

Meeting Closed: 12:45pm

