CPCA Consultancy Report on Information Governance for the Cambridgeshire and Peterborough Combined Authority

Author: Ciaran Ward
October 2020

Contents

Abbreviations used in this report

CPCA – Cambridge & Peterborough Combined Authority
CRM – Customer Relationship Management
DPIA – Data Privacy Impact Assessment
DPA – Data Protection Act
DPO – Data Protection Officer
EEA – European Economic Area
ESFA - Education & Skills Funding Agency
EIR – Environmental Information Regulations
FOI – Freedom of Information
GDPR – General Data Protection Regulation
IAR – Information Asset Register
ICO – Information Commissioner's Office
IRG – Information Risk Group
NCSC – National Cyber Security Centre
SAR – Subject Access Request
SIRI – Serious Information Risk Incident
SIRO – Senior Information Risk Owner

Information Governance Consultation Report, October 2020

Summary

- Update policies where necessary
- Introduce Staff training programme to cover data protection and information/cyber security
- Introduce Data Privacy Impact Assessments (DPIAs) for all new projects which involve the processing of personal information
- Create new data protection section on CPCA website
- Merge all Records Retention policies into a single policy
- Quarterly report on information governance matters and key performance indicators to be presented to Audit & Governance Committee (or equivalent body)
- Encryption of emails and removal of auto-populate function, regular penetration tests
- Secure Public Sector Network (PSN) compliance or similar accreditation
- Draw up data sharing agreements with any third party organisations where information is shared
- Conduct information audit and update Information Asset Registers
- Review duplicated files
- Appoint Data Protection Officer (DPO) and Senior Information Risk Owner (SIRO)
- Convene monthly Information Risk Group meetings

Background

This report is based on evidence and facts obtained from a series of conference calls between the author and key members of staff at Cambridge & Peterborough Combined Authority ("the Authority) which took place from 18th to 21st August 2020.

The CPCA formed in 2017 is a relatively small authority with approximately 75 employees so it is important to maintain a sense of proportion with regard to any information governance programme. The Authority has the following areas of responsibility:

- Developing the local economy
- Promoting the building of affordable housing
- Promoting adult education in the local area
- Commissioning and funding the adult education budget provision for learners within the local region
- Improving local transport and digital links

The personal data (as defined the GDPR and the Data Protection Act 2018) held and processed by the Authority consists of:

- Employee HR data (name, job title, home address, bank details)
- Members of the public who have signed up to newsletters
- Prospective students on adult education courses
- Members of the public who have participated in surveys (IP addresses)
- Names, email, home and employer addresses, salary bracket) and medical data of individuals who have signed up the 100K Homes affordable housing scheme

Objectives (Scope of work)

The scope of work in relation to this consultation exercise as laid out in the consultation agreement is as follows:

1. To review the current data protection and information governance arrangements held by the client including all policies, procedures and systems, with a view to establishing compliance and adequacy of information security.

2. To develop an action plan for the client for data protection and information governance

3. To produce a findings and recommendations report for the Audit and Governance on Information Governance and Data Protection

4. To create new and/or revised systems, procedures, policies and practices as required

5. To provide a development plan for the client Data Protection Officer

6. To advise on the creation of an Information Risk Group, who will meet monthly and handling issues and make decisions

7. To advise on the creation of processes for handling and logging FOI/EIR/Subject access requests

8. To create a staff training plan, and advise on materials

9. To advise on the creation of an appropriate annual work plan for data protection and information governance arrangements, and committee reporting

10. To review the information security arrangements in place, and to advise on any necessary remedial actions

11. To report to the Chief Legal Officer/Monitoring Officer on the above

matters Policies mentioned above include but are not limited to the

following:

- ICT users' policy/Information Security Policy
- Records Retention & Disposal Policy
- Privacy Impact Assessment template for new projects which involve the processing of personal data – eg procurement of new software systems
- CCTV Policy – *(N/A – CCPA does not operate CCTVs)*
- Covert Surveillance/RIPA Policy – *(N/A)*
- Information Risk Register
- Information Asset Registers for each department
- Data breach handling procedure
- Email encryption guidance

Action Plan

The action plan will address each of the points listed in the scoping schedule.

Review of Policies

The Authority's policies are generally well-written and fit for purpose, but I have picked up on a few points which require addressing:

Document Management Policy

Needs updating to reflect provisions of the current Data Protection Act 2018 rather than the old 1998 Act (page 2).

Requires more detail on the secure disposal of electronic and paper records. For example there is no specific reference to shredding of obsolete paper records either on or off-premise, or secure destruction of hardware – further details on page 14 of this report below.

Data Security Policy

The Data Security policy should be amended and updated to reflect the recent appointment of the Deputy Monitoring Officer as the Combined Authority's Data Protection Officer – see below:

2.2. Our Privacy Officer is responsible for ensuring compliance with GDPR and with this policy. Your manager can advise you who our Privacy Officer is. ***If we have cause to appoint a Data Protection Officer (an official appointment) or use a different title for a Privacy Officer, we will let you know and any reference to Privacy Officer shall include reference to a new title or a Data Protection Officer.*** *Any questions or concerns about the operation of this policy should be referred in the first instance to the Privacy Officer.*

Section 5 "Risks to Confidential Data" (page 3) should cross-reference the business records classification standards at section 5 (page 4) of the CPCA Document Management Policy.

8.4."If you are processing Confidential Data or Sensitive Data, consider who can see your screen whilst you are working (even if you are at home). If you are in a public place, e.g. on a train or whilst sitting in a café, take extra care that no one can see your screen and never leave a screen open on unattended Equipment"

The option of using a privacy screen to fit to one's device in such circumstances should be encouraged.

6.4."Use a secure password on Equipment to prevent unauthorised access and change your password regularly".

It is recommended that passwords should automatically require changing every 90 days and should contain at least 10 alpha-numeric characters for added security (as set out in the 3C ICT Policy, page 174).

Data Protection Policy
The section on transferring data overseas (page 4) requires amending:

"**Transferring information overseas**
If ~~you're~~ your personal information is transferred outside the European Economic Area (EEA) for processing or storage purposes the Cambridgeshire and Peterborough Combined Authority will ensure that safeguards are in place to protect it to the same standard we apply. We will ensure that any transfer only takes place if:
a. The European Commission has decided that the country or the organisation we are sharing your information with will protect your information adequately.
b. The transfer has been authorised by the relevant data protection authority, and/or
c. We have entered into a contract with the organisation with which we are sharing (on terms approved by
the European Commission), to ensure your information is adequately protected."

As Mailchimp and Survey Monkey (both based in the USA) are used for collecting data (by Energy Hub and Comms team respectively) this statement is inaccurate. I have recommended below that the Authority either stops using these providers or documents this usage as an official risk (eg to be added to Corporate Risk Register). Either way the above statement from the Data Protection Policy needs to be amended.

The Data Protection Policy should also be updated to include brief sections on the following of a paragraph each in length:

- Roles of the DPO and SIRO
- Data Privacy Impact Assessments (See Appendix 5)
- The reporting and handling of data breaches

Company Owned Mobile Device Policy
This policy is generally adequate, but I would recommend some additional wording.

I would recommend adding the following paragraph to section 5 ("Security") to ensure that security measures are not bypassed:

"Mobile communications equipment supplied by the Authority must not be altered or added to in any way including:

- **Unauthorised upgrades**
- **Addition of components**
- **Removal of components – including transferring an Authority SIM card to a personal phone**
- **Altering configuration or security settings**
- **Installation of non-approved applications"**

Processes for handling and logging FOI/EIR/Subject access requests

FOIs are currently logged on excel spreadsheets using a numerical naming system. The authority receives an average of 30 FOI/EIR requests per year. Therefore there is currently no financial justification for procuring an FOI management system.

If feasible however, it may be worth looking into using an existing Customer Relationship Management (CRM) System for the recording of such requests.

FOI requests are generally answered by the service area responsible and logged by the Governance Assistant.

It is important to have a clear distinction between FOI and EIR requests. Although they can be kept on the same database and given a similar code, requests should be clearly designated – especially when dealing with exemptions and when an internal review is launched. EIR requests for example may be related to the environmental impact of house building or development of transport infrastructure.

Subject Access Requests (SARs) - ie requests for personal information from the individual data subject concerned are rarely received. Any such requests are currently held on a confidential spreadsheet. This practice should be maintained as long as current trends continue – subject to standard security measures – ie restricted access only for those employees who require access.

Privacy Notices

All information gathering processes where data from members of the public is collected will require a privacy statement.

The CPCA already employs privacy statements for 100k Homes, Transport Plan and Adult Education Budget, as well as a general authority-wide privacy notice.

100k Homes

This is the service area responsible for promoting affordable housing for local residents and previously came under the jurisdiction of East Cambridgeshire Community Housing.
Although now part of the CCPA, 100K Homes has a separate website from the main CPCA website

100K Homes collects personal information on members of the public (mostly names, email, home, employment addresses and salary bracket) – but in some cases medical data – eg clients with mobility issues requesting a basement flat – so they can be added to the mailing

list – approximately 2500 individuals at the time of writing. The main condition for processing is consent.

In the case of information relating to the health or medical conditions of the applicant (which falls under GDPR definition of "special category" data) it is recommended that a policy document is completed to determine conditions for processing and other compliance- related factors such as retention and disposal – as set out on Schedule 1, Part 2 of the Data
Protection Act 2018. It should also be made clear on the form whether the collection of such data is compulsory or optional for the purposes of the project in hand.

The Data Protection Act 2018 (DPA 2018) outlines the requirement for an Appropriate Policy Document (APD) to be in place when processing special category data under certain specified conditions. So if 100k Homes requires the collection of medical or health-related information from clients a policy document should be completed to ensure GDPR compliance. Further details are available on the ICO website.

Privacy Notice for 100k Homes - https://www.100khomes.co.uk/privacy.htm
As the server for HubSpot (the software system used by 100K Homes for storing personal data) is based in the Republic of Ireland, this privacy statement should be amended as per below – ie change "United Kingdom" to "European Economic Area".

Transfer of data from the UK to the EEA is considered safe up until the end of the Brexit transition period on 31 December 2020.

*"**Who we share your personal information with***
We routinely share the personal data outlined above with HubSpot. HubSpot is a customer relationship management (CRM) provider, which stores your information securely on behalf of the CPCA.
This data sharing enables us to keep your information secure and accessible only to authorised persons.
We will share personal information with law enforcement or other authorities if required by applicable law.
We will not share your personal information with any other third party. We do not transfer your personal data outside the ~~United Kingdom~~.European Economic Area"

Recommendations for 100k Homes:

- Retrospective DPIA required to cover the risks of processing personal information (See Appendix 5)
- Information Asset Register to be updated as it still refers to the previous parent organisation East Cambridgeshire Community Housing

- Policy Document to be completed to ensure GDPR compliance concerning processing of “special category” personal data – see guidance on ICO website:

Adult Education Budget (AEB) Team

This service area collects data on adults (name, address, date of birth) in the local area who wish to register for education courses at local colleges. The data is inputted from a government website the Education & Skills Funding Agency (ESFA) using a CSV file and then stored within a secure Sharepoint file.

The data collecting procedure is governed by a privacy statement/fair processing notice. However there is no evidence of a Data Privacy Impact Assessment (DPIA) having been completed in order to assess the potential risks and compliance levels.

Recommendations:

- DPIA to be completed for this data processing exercise – see Appendix 5
- Draw up data sharing agreement with ESFA to ensure GDPR compliance

To advise on the creation of an appropriate annual work plan for data protection and information governance arrangements, and committee reporting

Recommendation: Quarterly report to Audit & Governance Committee (or equivalent body) on performance – eg number of data breaches and how they were handled, number of complaints received, timing of FOIs, cases referred to the ICO, etc – to be presented to board by DPO - and subsequently published on CCPA website in the interests of public transparency. An example of such a report (containing a Freedom of Information/Subject access update and a GDPR update can be found on the Guildford Borough Council website.

To review the information security arrangements in place, and to advise on any necessary remedial actions

It would be advisable for CPCA to obtain some form of cyber-security accreditation such as Cyber Essentials or ISO 27001, and to procure a recognised anti-malware package such as F- Secure.

Passwords should have ten characters consisting of one uppercase, one numerical and one special character – and as outlined in 3C IT user policy - should be changed every 90 days.

ICT

The Authority's IT services are outsourced to 3C ICT who also provide for three other local authorities in the region.

All three local authorities have Public Sector Network (PSN) compliance, but this does not apply directly to the Combined Authority.

3C ICT has an Acceptable Use of ICT Policy for staff and users.

Recommendation: CPCA to use this policy as a template for implementation of its own acceptable use of ICT policy with specific application to the Authority. CPCA to look into securing PSN compliance (time and resource complaints permitting).

General Recommendations

- To facilitate public transparency and confidence this report recommends the creation of a data protection section on the CPCA website. This section should include links to relevant policies and authority privacy statements and information rights which members of the public are entitled to – eg right of access, right of erasure, etc

- Staff training in both data protection and cybersecurity – either electronic (eg Workrite provide an efficient and user-friendly online GDPR training package) or through face-to-face classroom-based session – should be made mandatory – and co-ordinated by HR. Staff specialising in FOI or DP should undertake more detailed specialised training. The fact that an estimated 90% of all data breaches are caused by human error (according to data received by risk consulting firm Kroll) underlines the crucial need for an effective staff training programme.

- Annual penetration tests to be carried out on CPCA infrastructure – this responsibility should come under ICT. (A penetration or "pen" test is an authorised simulated cyber-attack on a computer system designed to test the security of that system). Annual pen tests are standard procedure within many organisations. Further guidance can be found on the NCSC website.

- Purchase an email encryption tool like Egress (Budgetary restraints permitting).

- Retrospective due diligence/Data Privacy Impact Assessments to be carried out for external software providers:
    - Hubspot (CRM system) – holds data on approximately 6000 individuals
    - Citrus (HR system)
    - Agresso (Finance system) – DPIA is incomplete (the "Action to be taken" table on the last page has all dates for completion of actions listed as "tbc", no contact details or names of authorised officers are provided) and sign-off is required by an appropriately authorised officer so the process can be properly documented (see Appendix 5)

- **Privacy by design** – ensure that all external software providers have functions to enable data to be deleted easily and efficiently when it is no longer required (see DPIA guidance above)

- Any corporate decisions made with regard to information governance should be appropriately documented within an official record to ensure

adequate transparency and accountability (see Appendix 4 – Official Record of a Decision)

- Introduce a procedure around employees who have left – ie accounts/passwords to be disabled immediately following their final day of employment. Procedure to be integrated into HR Privacy Notice

- Confidential HR hard copy records are currently stored at the Ely offices. Non- confidential records are kept in a specialised container. Although most of these records are less than 5 years old a review of the disposal dates, and if required a purge of redundant records is recommended. The purpose of this recommendation is two-fold – to save on storage costs, and to ensure GDPR/data protection and FOI compliance.

  A DPIA assessing any risks within the physical storage facility would be advisable especially with records being kept at two different locations. This should also be reflected in the Authority's Business Continuity Plan.

- As the organisation is a relatively new one it is unlikely to have much in the way of outdated or obsolete records. However, it is important to regularly delete "Redundant/Obsolete/Trivial" (ROT) emails and other records. Obsolete emails, for example can easily accumulate quickly in an inbox and this can have an impact on GDPR compliance and the efficient delivery of FOI/SAR requests. Ideally emails which still have a business value should be archived on a standard storage platform such as Microsoft 365 or Sharepoint, rather than in the employee's inbox.

  It is unrealistic however to expect employees to regularly transfer emails to these platforms, but there are various options which could be explored by the ICT team. As a minimum requirement, staff should be encouraged to delete redundant emails on a regular basis.

- Laptop hard drives must have full disk encryption applied with a minimum of 128 bit AES (NB this is a suggested standard and should not be taken as definitive – please contact CCPA's IT rep for advice)

- Create Information sharing agreements with partner organisations – ie central government, other local authorities to document all instances where personal data is shared with third parties - eg the sharing of adult education-related information with ESFA.

Data Privacy Impact Assessments (DPIAs) - A standard template Privacy Impact Assessment form for new projects which involve the processing of personal data – eg procurement of new software systems – should be agreed on by the IRG and communicated to staff. The ICO website provides a ready-made form:

https://ico.org.uk/media/about-the-ico/consultations/2258461/dpia-template-v04-post-comms-review-20180308.pdf

On completion the DPIA should be approved by the DPO and signed off by the Information Asset Owner or Project Manager as well as by an appropriate director/senior manager.

See Appendix 5 for a sample DPIA.

Information Mapping and Data Flow - Based on the findings of this report, the only service area within the CPCA which has an Information Asset Register (IAR) - also known as a "Record of Processing Activity" (ROPA) - at present is Community Housing. The IAR is a legacy of the East Cambs Trading Company and therefore needs updating to reflect the present set-up. See Appendix 2 for a worked example.

Each service area of the Authority should therefore submit a spreadsheet containing details of its information assets and data processing which should be approved by the DPO and retained for future reference. It is of crucial importance that the Authority is able to justify all processing of information according to the conditions for processing under the Data Protection Act 2018 and the six lawful bases as stated in the Article 6 of the GDPR.

More detailed email encryption guidance for staff required – Pages 4-6 of the general Document Management Policy contain guidance on the classification and mark-up of business records.(ie restricted/confidential/ general/ public). This guidance is generally sound. However with regard to email, while there is guidance on specifying classification level within the email subject field, there is no mention of any email protection system such as Egress, nor is there advice on protecting or encrypting attachments within emails.

Draw up data sharing agreements with any third party organisations where information is shared – eg ESFA, other local authorities, applicable central government departments

The setting up of an Information Risk Group to meet monthly for handling issues around and making decisions (see above for details)

Merge all Records Retention policies into a single policy – The HR department currently has its own policy on retention separate from the overall Authority policy. The reasons for this are largely historic in that the Authority's HR policies were based on the existing policies used by Peterborough City Council.

It is recommended however that the two should be merged into an overall authority-wide policy for the sake of consistency and transparency.

The two policies also contain conflicting guidance.

For example the general policy (the “Document Management Policy”), on page 8 states the following retention period for employee leave records:

“Process of monitoring staff leave and attendance - Destroy 2 years after action completed” –

Whereas the HR policy (page 2) confusingly lists leave records within the same category as general employment contract data and states the following:

“While employment continues and for 6 years after the last day of the last complete tax year during which they worked, except if any claim is made within that time, in which case the claimant's data will be held until completion of the claim.”

Similarly, regarding recruitment-related records (page 2) the HR policy advises deletion ***“6 months from the date of offer or rejection, except if any claim is made within that time, in which case the claimant's data will be held until completion of the claim.”***

The general policy (page 8) does not make reference to potential claims, but simply states that such records should be destroyed ***“1 year after recruitment has been finalised”.***

To ensure GDPR compliance and good records keeping practice, it is important the contents of the two policies is harmonised. Cross-reference should also be made to the 3C ICT Policy’s guidance on the secure disposal of hardware (page 68) which makes the following statements:

“the equipment or media must have any information and software irreversibly removed. It must be physically inspected by IT staff or their agents to determine that this process has been successful.”

“If the appropriate precautions are not taken to carefully remove all sensitive information from hard disk drives, memory and accompanying storage media the risk of exposing confidential or sensitive information is very high. Simple file deletion is generally not sufficient and the files must be totally removed or overwritten by a separate utility program to ensure they are unable to be retrieved. In some cases total destruction may be the preferred option.”

Cyber Essentials certification

Cyber Essentials is a government backed scheme which assists organisations in protecting their networks against common cyber threats.

https://www.ncsc.gov.uk/cyberessentials/overview

Carry out an information Audit (see appendix for worked example of Information Asset Register) to include a record of:

- all categories of data held by each service area
- format – eg held within a cloud-based database, within CPCA system – word, excel, hard copy, etc
- level of sensitivity
- who has access to it
- retention/disposal period

This is essential for GDPR compliance as well as in answering FOIs/SARs as it is important for any organisation to know what data it holds, and where this data is located. It is also important that records which no longer have a business function are regularly deleted in accordance with retention and disposal schedules.

Working from home – there is currently a Self Assessment Checklist issued by the HR team for employees working from home, but it does not cover any security or data protection-related issues (see table of risks below).- eg awareness of phishing scams, multi-factor- authentication (MFA), the importance of locking one's screen when away from laptop, etc.

Recommendation: to add the above points to HR Self Assessment Checklist

Summary of Risks (see Risk Register below for full details)

- Lack of staff knowledge/training.
- Internal training is also required – eg workshops – refresher training every 2-3 years to update skills and knowledge
- Customer data on Hubspot – only employees who have a direct business need to access this data should be granted access
- Lack of buy-in or awareness of risks from senior management
- Remove auto-populate (ie predictive text) function from corporate email as this only increases the risk of emails being inadvertently sent to the wrong person who may have a similar name to the intended recipient
- **Cybersecurity** - The Authority should be wary of Hacking/Ransomware/cyber-attacks (see Risk Register below). Local authorities have been targeted before resulting in severe disruption to services and considerable financial loss.

A cyber-attack on Redcar and Cleveland Council's computer systems is estimated to have cost more than £10m and left approximately 135,000 people without access to online services in February 2020.

A report by privacy group Big Brother Watch found that 114 councils had experienced at least one cyber attack between 2013 and 2017.

The NCSC defines a cyber-attack as "'a malicious attempt to damage, disrupt or gain unauthorised access to computer systems, networks or devices, via cyber means".

- The HR department plans to transfer all policies from Sharepoint to Citrus – but there is currently some degree of duplication. It is therefore important that all duplicated HR files in Sharepoint (that were migrated over to Citrus) are reviewed and deleted where necessary.

Development Plan for DPO

The main functions of the Data Protection Officer are as follows:

- Deciding on whether reported incidents constitute a data breach – and if so whether they should be reported to the Information Commissioner's Office (ICO).

- Conducting investigations into any alleged data breaches, writing up relevant reports and deciding on appropriate course of action – see Appendix 3.

- Review existing data-related policies every 2-3 years and update where required.

- Monthly reporting to Corporate Governance Group (or equivalent body) and presence at other meetings of senior management where appropriate.

- Quarterly reporting to Mayor and Board on Key Performance Indicators – reports to be published on CPCA website for public transparency.

- To be present as an advisor to senior management and SIRO where all decisions with data protection/security implications are made – eg the procurement of a new software system or electronic database; or a corporate restructure.

- To serve as main point of contact for the ICO on all data protection issues, including complaints, appeals and data breach reporting.

- To assess risks relating to organisation-wide projects involving the use of personal data – eg procurement of databases, restructuring exercises – this will include the co-ordination of Data Privacy Impact Assessments (DPIAs) prior to implementing any such projects.

- To present monthly DPO report at Information Risk Group meeting (see details below).

- To review and approve a register of processing operations (ie information asset registers maintained by each service area – see above).

- Conducting reviews of contested FOI/EIR/Subject Access requests (this can be done by either the SIRO or the DPO dependent on whether either party was involved in the original decision).

- To oversee renewal of annual registration of CPCA as a data controller with the ICO.

- To advise the authority on privacy notices to data subjects at the point of collection and their personal data, pursuant to articles 12-15 GDPR.

Recommendations for DPO

- Undertake course in DP training – Act Now, Amberhawk and PDP are all recommended reputable providers. (It would also desirable to have an FOI qualification).
- If practically possible the DPO should be issued with a separate email account – eg dpo@cambridgeshirepeterborough-ca.gov.uk - to be published on the Authority's website as the public's main point of contact for matters involving personal data

Recommendations for SIRO

The Senior Information Risk Owner (SIRO) should be a senior officer who provides assurances to the CEO on information risk issues. The Monitoring Officer for example could carry out this role.

Although there will be some degree of overlap with the DPO role, the SIRO role should consist of the following activities:

- Attending monthly IRG meetings (see below for details)
- Ensuring that information risks are followed up and incidents managed
- Overseeing the development of information risk policy – eg reviewing and approving new and existing policies
- Reviewing and agreeing actions in respect of identified information risk issues
- Ensuring senior management is kept up to date on all information risk issues affecting the Authority and its business partners
- Ensuring the Authority's approach to information risk is effective in terms of resources and execution, being appropriately communicated to all staff

All data breaches should immediately be reported to the SIRO.

Information Risk Group

The Information Risk Group (IRG) should meet monthly and consist of the Senior Information Risk Owner (SIRO), DPO and (if applicable) a senior IT officer and information governance officer (or nearest equivalent role).

The group should be used a forum for decision-making on important matter – eg new protocols, action on breaches, development plans, etc. The Group should maintain a register of ongoing issues which should be updated after every meeting.

Recommended format of IRG meeting:

- Minutes from previous meeting (including actions) – it is recommended that a spreadsheet of ongoing and completed actions is maintained and reviewed/amended at every meeting
- DPO update (covering breaches, complaints, new projects, initiatives, new data legislation, latest ICO news)
- SIRO update
- Information Security update (to be presented by equivalent member responsible for information assurance/security) - eg this could be a member of the outsourced ICT team
- FOI/SAR update – to include latest monthly performance stats, any particularly difficult or complex requests, escalation of cases, application of exemptions, ICO appeals, overdue cases, etc
- Review of Register of Ongoing Issues

Appendix 1 - Key risks

Risk	Description	Potential consequences	Solution
Lack of staff training/knowledge	Most employees have not had formal training or experience in information governance	Breach of GDPR due to data being mishandled or avoidable error being made	Implement training programme across CPCA; make GDPR/DP and cybersecurity training compulsory for all staff New staff should be automatically enrolled on training which must they must complete in order to pass probation Refresher training for staff every 2-3 years
Auto-populate function in Outlook email system	Email system has predictive text function which automatically suggest email address after the first 3-4 letters are typed into the "To" field	Data breach caused by message being sent to the wrong person who may have a similar name to the intended recipient	Disable auto-populate function across the organisation There may be opposition to this idea due to apparent inconvenience – if the proposal is overruled by senior management, this decision should be officially documented (see Appendix 4)
Use of Survey Monkey by Comms Team	Collects IP addresses of respondents	Service is based in USA, therefore personal data (IP addresses) collected will leave the EEA, creating a risk of lost or compromised data	Conduct Surveys via existing Hubspot CRM platform or switch to an EU-based tool such as SmartSurvey (If Authority wishes to remain with SurveyMonkey this risk should be officially documented in Corporate Risk Register - and privacy statement should advise that data is being held outside EEA)
Use of Mailchimp by Energy Hub team for electronic newsletter mailouts	Collects email addresses of individuals who have signed up	Service is based in USA – see above	Switch to an EU-based mailing tool such as Sendinblue, GetResponse or Moosend ((If Authority wishes to remain with Mailchimp this risk should be officially documented and privacy statement should advise that data is being held outside EEA)
Accidental retention of data beyond statutory date	Files kept on system which if not regularly cleansed	Risk of GDPR breach	Regular data cleansing exercises

	can easily be forgotten		
Lack of cybersecurity accreditation	Level of cyber threats not fully realised	Attack on authority networks	Apply for CyberEssentials certification https://www.ncsc.gov.uk/cyberessentials/overview
Duplication of records	Inefficiency	Risk of GDPR breach if sensitive/personal data is duplicated unnecessarily	Implement Records Management Policy
Lack of policy on leavers	Employees who leave taking confidential or sensitive data with them; failing to return electronic equipment	Leaking of sensitive information potentially leading to financial (eg fine from ICO) and reputational damage	Incorporate section on leavers in Data Security Policy – to include provision that all leavers should have their IT accounts disabled automatically after leaving and the IT security officer (or equivalent postholder) should always be notified
Cyber-attacks	Ransomware or hacking attacks directed at CPCA's ICT infrastructure	Financial (eg fine from ICO) and reputational damage	Use a suitable tool like F-Secure, McAfee or Bitdefender – liaise with 3C ICT
Lack of standardisation within staff information management practices	Inconsistency which could lead to breach	Financial (eg fine from ICO) and reputational damage	Standardisation of policies and procedures across the combined authority
Collecting personal data without adequate DPIA in place	Personal info being collected without consideration of the risks and impact on personal privacy involved	Financial (eg fine from ICO) and reputational damage (eg insufficient security controls can in some cases lead to users accessing the personal data of others)	Existing DPIA in place for Agresso (financial system) is incomplete DPIAs to be completed for Citrus and Hubspot
Impact of staff WFH due to Covid lockdown	Lack of staff awareness concerning security of laptops/mobile devices	Data breaches	Complete DPIAs; arrange appropriate staff training; introduce clearer protocols on use of mobile devices (see above)

Appendix 2 - Sample Information Asset Register (IAR)

Name of system, process or information asset	Types of information held	Purpose	Format	Location	Security controls in place	Responsible officer	Protective marking	GDPR Article 6 Legal basis for processing (if the data is personal)	Retention period
Staff training	Dates, course details, employees who attended	Health & safety, statistical reporting	Electronic	Sharepoint	Access restricted to HR team only	***[insert name of asset owner]***	Protect	Public task	40 years for health & safety training, 6 years for other training
Payroll, salary, allowance, expenses	Contract hours, mileage, timesheets, etc	Audit purposes, statistical reporting, HMRC	Electronic	Citrus	Password protected	***[insert name of asset owner]***	Protect	Public task; performance of a contract	6 years
Pensions information	Pensions paid into scheme	Future pension attainment	Electronic	Citrus	Password protected	***[insert name of asset owner]***	Protect	Public task; performance of a contract	100 years
Sickness absence	Dates of sick leave, reasons, triggers and stages, occupational health	For monitoring sickness; statistical reporting	Electronic	Citrus	Password protected	***[insert name of asset owner]***	Protect	Public task; performance of a contract	6 years
Contractual information	Changes to contract letters, DBS, Probation	Audit purposes, response to queries	Electronic/ paper	Citrus	Password protected	***[insert name of asset owner]***	Protect	Public task; performance of a contract	6 years

Appendix 3 - Template form for recording data breaches

(To be used in conjunction with PERSONAL DATA BREACH NOTIFICATION POLICY)

Personal Information Risk Incidents Report Form

Serious Information Risk Incident (SIRI) Category* (DPO to complete)	(eg Near miss)			
Service Area				
Summary & Chronology of incident				
Date and time reported to the Council				
Is this is a s170 offence?*				
Total number of individuals affected				
Is financial or special category personal data involved?**				
If YES, please describe in more detail				
Format of the information	**PAPER**	**DIGITAL (Unencrypted)**	**DIGITAL (Encrypted)**	**OTHER**
Have the affected individuals been informed?				
What was the cause of the incident?				
What can be done to prevent reoccurrence?				
Has the incident been reported to the ICO?				
Is there potential for media interest?				
DPO COMMENTS OR RECOMMENDATIONS				

SIRI Category

0 = near miss
1 = Confirmed security risk, but no need to report to ICO (can be dealt with internally)
2 = Confirmed security risk which must be reported to ICO within 72 hours

*Section 170 Offence – the criminal offence of knowingly or recklessly and without authorisation obtaining, disclosing or selling personal data under s170, DPA 2018

Special category personal data – Racial or ethnic origin, political opinions, religious beliefs, trade union membership, physical or mental health, sexual life, legal or court proceedings, biometric data

Appendix 4 – Official Record of a Decision (SAMPLE)

CAMBRIDGESHIRE & PETERBOROUGH
COMBINED AUTHORITY

Proposal to remove Auto-populate function in Outlook email system

Following a monthly meeting of the Information Risk Group on [**dd/mm/yy**] it was recommended to the Board that the auto-populate function (predictive text tool) be disabled from the CPCA's email system for all users. This action would prevent data breaches in that emails would not be sent erroneously to recipients with similar names to the intended recipient.

It was noted that ***[X]*** breaches occurred during the past ***[Y]*** years as a result of auto-populate.

A report was presented to the Board by the DPO outlining the current risks and assessing the impact of removing the function

Decision: The proposal was approved/overruled by the Board **(delete as appropriate)**

If proposal was overruled, provide details of reasoning below:

Appendix 5 - Sample Data Privacy Impact Assessment (DPIA)

(NB - The company referred to below is fictional, but the DPIA is based on a real life example)

Data Privacy Impact Assessment for NovaRap

General Information

1	**NAME OF PROJECT/PROCESS**	Purchase of NovaRap (software package for producing e-newsletters)
2	**OBJECTIVE** **Describe the established and proper legal basis for the scheme**	To save money on print and postage (approximately £40k per year) we are replacing this channel of communication with a digital e-newsletter/new emailing platform to communicate effectively with residents, businesses and visitors
3	**BACKGROUND** **Why is the use of personal information required?**	Names and email addresses required so we can communicate with local residents to keep them up to date with our services and promote events. We will also ask for further information such as areas of interest so we can tailor our communications to specific topics
4	**Benefits to the Authority and other parties or stakeholders**	The new emailing platform will enable us to become more cost-effective and develop a new targeted marketing strategy
5	**Constraints**	GDPR and data protection compliance when collecting data – see below
6	**QUALITY EXPECTATIONS – ie how will the system improve existing practices?**	The new software will allow us to engage with audiences directly and improve the quality of interaction. With the new system we will be able to send more frequent updates in a cost-effective way. There is potential to use the platform for effective communications
8	**Cross reference to other projects**	Service saving costs – for the Authority to go paperless
9	**Project Manager**	Strategy & Communications manager
10	**Information Asset Administrator (normally the head of the relevant service or team manager within the department concerned)**	Head of Communications
11	**CUSTOMERS & STAKEHOLDERS**	Local residents, businesses, councillors, senior management, local media

	Screening Questions	
1	**Does this project involve the use of special category (sensitive) information?**	No
2	**Does this relate to (1) a new ongoing process or (2) a**	(2) we will be acting as data

	permanent change in the way the Authority will handle personal information?	controller
3	**Will you be using the information about individuals for a purpose or in a way in which it is not currently used?**	It will be the first time the Authority has used an email information platform
4	**Will information about individuals be disclosed to organisations or people who have not previously had access to this information?**	No
5	**Does the project involve the matching or other aggregation of personal information from different sources which could have an impact on privacy?**	No

Consultation **Describe what prior consultation carried out?**	The decision was made by senior management with support of the Executive following lobbying by the Communications team
Privacy and related risks **1. What are the indentified risks?** **2. What safeguards will be employed?**	1. Data breaches in the event of a cyber-attack or misuse of the personal data either maliciously or inadvertently 2. NovaRap are GDPR, ISO 27001 and CyberEssentials compliant. The system includes safety lockout, a session-based security tool
Which conditions for processing personal data as per GDPR/Data Protection Act 2018 does this use of information meet?	We will be using an opt-in system to obtain consent from people signing up to the newsletter which includes our privacy policies
You must ensure that data subjects are informed of: **The identity of the data controller** **The identity of the data processor** **The purpose for which the information will be used** **Any further details required to ensure fair and lawful processing**	Data controller = CPCA Data processor = NovaRap Purpose – to inform residents and businesses about the Authority NovaRap complies with the Privacy & Electronic Communications Regulations 2011, which sets out more specific privacy rights around electronic communications
What process is in place to ensure disposal of personal information which is no longer required?	After identifying those who have opted out their data can be deleted
If relying on consent for the processing of the personal information, how will withdrawal of consent be handled?	Those who wish to unsubscribe will be manually removed from the database. The system also allows us to suppress a contact from receiving emails from us.
What measures are required to keep the information safe, available and reliable? How will unauthorised access or use be identified?	Unauthorised internal access and weak passwords will be prevented through data security assurances, including staff training. NovaRap reduces threats through highly secure industrial standard encryption to protect all data in transit between their servers and the user. All tracked and identifiable data between sender and recipient is also encrypted

What training is required to ensure staff know how to handle the information securely in accordance with procedures?	Training will be provided to staff about to send, share and store the data securely
Will the process include the transfer or storage of personal information outside of the European Economic Area either directly or by the internet (cloud) or website? **If the answer is yes, how will you ensure that the personal data is adequately protected or otherwise meets the requirements of the sixth GDPR principle (integrity and confidentiality)?**	No Not applicable

Information Asset Owner's declaration and signature

I confirm that I have considered the processes outlined above and can confirm they will be compliant with the Data Protection Act 2018 and the General Data Protection Regulations (GDPR). I hereby authorise acceptance of this Privacy Impact Assessment:

Name: F. McNally
Job title: Strategy & Communications Manager
Signed:

(SEE ATTACHED NOVARAP'S PRIVACY STATEMENT AND DATA SECURITY GUARANTEE)