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	The GDPR Policy has been updated. This update Policy is shown at Appendix 1. Socitm Advisory are going to provide a baseline set of IT policies as well as IT procedures. These policies will include: • acceptable usage agreement • Device loan agreements • Backup and storage policy • Data policy including portable media etc • IT disaster recovery TDC Autumn 2021

Introduce Staff training programme to cover data protection and information/cyber security	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. Officers have undertaken IT security training run by Barclays Bank. Further IT security training is being finalised for delivery across the organisation.
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

	accidental data breaches where incorrect contacts have been used. 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).
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	Soctim 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 <u>Freedom of Information (FOI) and Environmental Information Regulations (EIR) requests</u>

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.