Agenda Item No:8

Report title: Information Governance Update

To:	Audit and Governance Committee
Meeting Date:	5 March 2021
Public report:	Public Report
From:	Rochelle Tapping Deputy Monitoring Officer

Recommendations:

The Audit and Governance Committee is recommended to:

1) To note the findings and recommendations of the report on Information Governance, which will be implemented at the Combined Authority.

2)Agree 6 monthly reporting into the Committee on information governance matters

Voting arrangements: A simple majority of all Members

1. Purpose

1.2 To advise the Audit and Governance Committee of the Information Governance report including findings and recommendations for implementation.

2. Background

2.1 Information Governance includes compliance with freedom of information, data protection laws and information security. To establish the efficiency of information governance at the Combined Authority, including improvements required, a review of the same was necessary. Between August and October of 2020, the CPCA instructed an external data protection specialist to conduct that review and produce a report.

2.2 The technical scope of the review included reviewing current data protection and Information Governance arrangements; to establish compliance and adequacy of information security, develop an action plan, create systems and policies etc, create a development plan for the Data Protection Officer, advise in relation to creating an Information Risk Group, create processes for handling and logging FOI/EIR/Subject access requests, develop a staff training plan, advise on the annual work plan and review the information security arrangements. The review findings and recommendation are detailed within the report, which is provided in the Appendix.

2.3 The report includes a clear action plan to improve information governance and to also ensure staff awareness of GDPR obligations. Since the report was drafted, the UK left the EU and so the matters outlined within the report, relevant to the EU should be disregarded. This point is considered further in the legal implications outlined below.

2.4 There is an intention to implement all the relevant report recommendations over the course of the next year. There are more complexities around implementing the recommendations that relate to information security as this involves work that needs to be conducted by 3C ICT, who provide IT support to the Combined Authority. Discussions have commenced with 3C ICT, to ascertain a plan of action. In terms of the more immediate priorities arising from the report, these include staff training, to avoid non-compliance and updating all policies.

Quarterly Report

2.5 The report recommended that quarterly reporting on information governance matters and key performance indicators be presented to the Audit & Governance Committee. That report would cover the number of data breaches and how they were handled, number of complaints received, timing of FOIs, cases referred to the ICO. However, the size of the CPCA and amount of FOIs, and information governance matters suggests that quarterly reports are too frequent given that the construct of Combined Authority means that information governance is not a vast work area. Instead, the Committee may determine that 6 monthly reporting is more appropriate.

2.6 The table below details the main recommendations of the report, progress to date and the target completion date.

Recommendation	Progress and target completion date (TCD)
Update policies where necessary	All policies are being updated. TCD Spring 2021.
Introduce Staff training programme to cover data protection and information/cyber security	A UK GDPR training course has been identified. TCD Summer 2021. This will be mandatory for all staff with newly appointed staff also completing the course on induction. Search for Information security course is ongoing- TCD Summer 2021
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*	Planned implementation date Spring 2021 This will be an ongoing task therefore no applicable TCD
Create a new data protection section on CPCA website	The CPCA is launching a new website in March 2021. There will be a dedicated section on that website for data protection. TCD date is the website launch date.
Merge all Records Retention policies into a single policy	Yet to be undertaken TCD Summer 2021
Quarterly report on information governance matters and key performance indicators to be presented to Audit & Governance Committee (or equivalent body)	To be confirmed by the Committee
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*	Liaison with 3C ICT has commenced in relation to implementation of encryption of emails and removal of auto-populate function TCD Summer 2021

investigate your environment for vulnerabilities i.e., attempting to hack the system.	External organisations will be approached regarding penetration tests. Target completion date Winter 2021.
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.*	This is planned as a long-term objective, should the CPCA decide to pursue PSN compliance. No TCD
Draw up data sharing agreements with any third-party organisations where information is shared	A number of DSAs have been draw up. This will be an ongoing action as the need for individual DSAs become apparent. No TCD
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*	Yet to be implemented but more beneficial if this commences after staff UK GDPR training Target date Summer 2021
Review duplicated files	Liaison with 3C ICT has commenced in relation to implementation -TCD Summer /autumn 2021
Appoint Data Protection Officer (DPO) and Senior Information Risk Owner (SIRO) Development plan for DPO and recommendations for SIRO-*The final approaches will be determined by the Combined Authority but will align with UK law*	The Deputy Monitoring Officer is the Data Protection Officer. The following email is now live: dpo@cambridgeshirepeterborough-ca.gov.uk The Monitoring Officer is the SIRO No TCD as ongoing roles
Convene monthly Information Risk Group meetings	Yet to be implemented TCD Summer 2021

3. Financial Implications

3.1 None

4. Legal Implications

4.1 The Data Protection Act 2018 (DPA 2018) sets out the framework for data protection law in the UK. It updates and replaces the Data Protection Act 1998, and came into effect on 25 May 2018, but was subsequently amended on 01 January 2021 by regulations under the European Union (Withdrawal) Act 2018, to reflect the UK's status outside the EU.

4.2 DPA 2018 sits alongside and supplements the UK General Data Protection Regulation (UK GDPR). The UK GDPR is the retained EU law version of the General Data Protection Regulation ((EU) 2016/679) (EU GDPR) as it forms part of the law of England and Wales, Scotland and Northern Ireland by virtue of section 3 of the European Union (Withdrawal) Act 2018.

4.3 The ICO regulates data protection in the UK. Non-compliance with data protection law amounts to breach, with penalties for breach including the imposition of fines.

4.4 Data protection policies, privacy notices etc, adopted by the CPCA will be updated to reflect UK data protection laws.

5. Other Significant Implications

5.1 None

6. Appendices

6.1 Appendix – Information Governance Report

7. Background Papers

7.1 None