CAMBRIDGESHIRE & PETERBOROUGH COMBINED AUTHORITY

Agenda Item No: 6

# Name of Report: Information Governance Update

| | |
|---|---|
| To: | Audit & Governance Committee |
| Meeting Date: | 24 March 2023 |
| Public report: | Yes |
| From: | Sue Hall<br>Data Protection Officer |
| Recommendations: | The Audit & Governance Committee is recommended to:<br>a) Consider and note the contents of this report |
| Voting arrangements: | N/A |

## 1. Purpose

1.1 To update the Audit and Governance Committee on the current position with regards to Information Governance, and to provide data related to Freedom of Information requests, Environmental Information requests and complaints for the period of 01 January 2022 – 31 December 2022.

1.2 To update the Audit and Governance Committee on data breaches from August 2022 to 31 December 2022.

1.3 This report outlines the key Information Governance activities undertaken by the CA during this period and provides assurance that the CA across all of its work areas and functions remains compliant with its legal obligations and follows good practice.

# 2. Background

2.1 Freedom of Information (FOI) requests from 01 January 2022 to 31 December 2022.

56 x FOIs received from 01/01/22 – 31/12/22
0 x late responses
0 x FOI reviews received from 01/01/22 – 31/12/22
0 x ICO reviews received from 01/01/22 – 31/12/22

1 x FOI from a Councillor
3 x FOIs from Press

Subjects received:

- Transport: e-scooters, bus lanes, Ting, bus stops, bus franchising, public transport – spend on subsidised bus services, plans and drawings for cycleway, zero emission buses

- Business and Skills: market town funding, green home grants, AEB contract information, AEB allocations

- Climate Change: chalk stream projects, planning – climate change, buildings and energy – climate change, governance and funding – climate change

- General: maternity and paternity policy, settlement agreements information, payments to suppliers of the website, branding, researchers/analysts, IT equipment information, mayor hosting events, names of external consultants, trainers and advisors

Environmental Information Regulations (EIR) from 01 January 2022 to 31 December 2022

1 x EIR received from 01/01/22 – 31/12/22
0 x late responses
0 x EIR reviews received from 01/01/22 – 31/12/22
0 x ICO reviews received from 01/01/22 – 31/12/22

Subjects received:

- Highways

Corporate Complaints from 01 January 2022 to 31 December 2022

No complaints were received from 01 January 2022 to 31 December 2022.

2.2 Data Breaches

The following data breaches occurred between August 2022 – December 2022. The only breach which was reportable to the ICO was as follows:

- Growth Co is a company wholly owned by the Cambridgeshire and Peterborough Combined Authority. As part of the ESF StarHub Project, Growth Co are required by Central Government to submit evidence of Invoice (Payslip) and defrayal (BACS Run) for the staff cost element of the project expenditure. This project includes employees from CPCA and employees from Growth Co (5 in total across both organisations). The information for Growth Co employees is obtained from an external payroll provider, and the information for CPCA employees is obtained from the CPCA HR/payroll.

  The CPCA HR/payroll team have been providing Growth Co with a BACS folder for the CPCA payroll so that evidence could be provided to central government for funding that was being cross charged to the salaries of some individuals working in the CPCA. Information regarding 114 employees of CPCA has been sent unredacted to a member of Growth Co.

  This breach was reported to the ICO

  **ICO's Decision -** the ICO considered the information provided and decided that no further action was necessary on this occasion.

- The wrong email address had become attached to the applicant's record and emails meant for the person were sent to a third party.

  This was not reportable to the ICO

- External person was cc'd into an email. The email contained some personal data (name and address).

  This was not reportable to the ICO

2.3 RSM Audit

RSM undertook an audit of Data Protection. Below are the actions from the audit and the work which has been carried out or is still to be carried out giving deadline dates.

**RSM Action 1: Employee Contracts/Code of Conduct forms for Business Board Members, Committee or Sub-Committee Members.** Employee Contracts contain a section on Data Protection. The Code of Conduct forms for Business Board Members, Committee or Sub-Committee Members need to be updated to cover GDPR and Data Protection.

The form will be revised to include information on Data Protection. The revised form will be sent out in May 2023 after the elections when there is a changeover of members.

Deadline 30 May 2023.

**RSM Action 2: Staff Communications and Awareness of Data Protection.** A Communications Plan needs to be established which includes routine reminders through materials such as staff emails/newsletters, team meetings, posters and screen savers to support awareness of data protection.

A Communications Plan is being created to support the awareness of data protection. This will include posters, bulletins, lunch and learn sessions.

Action complete.

**RSM Action 3a: Data Protection Training**. There is no process in place for ensuring that Members are trained on data protection.

Members do not undertake Data Protection training with the CPCA. All Constituent Councils were approached and asked to provide information on what training is provided to their members who sit on CPCA Boards/Committees. Two of the constituent councils do not provide regular mandatory training for members. Data Protection training is to be added to the induction programme for new members which takes place in May 2023 after the elections when there is a changeover of members.

Deadline – 30 May 2023

**RSM Action 3b: Data Protection Training.** A formal process to be implemented for managing overdue Data Protection training. This will include a suitable escalation route for non-compliance.

A section on Data Protection Training/Information Security Training has been included in the draft Learning and Development Policy. It states the following:

- training is mandatory for permanent, temporary, contractors, agency staff, student and trainees
- training is to be undertaken in the first week of employment
- all employees need to complete refresher training every 12 months
- the process is set out
- consequences of non-compliance – this may result in failure of their probationary period.

A section on mandatory training has been added to the appraisal form.

Action complete

**RSM Action 4a – Induction.** A mandatory Training Policy to be documented which covers areas such as the deadlines for completion by new starters, the process for managing non-compliance with training.

A section on Data Protection Training/Information Security Training has been included in the draft Learning and Development Policy. (see Action 3b above).

Action complete.

**RSM Action 4b – Induction.** A process to ensure records are retained for Data Protection training completed by staff who have subsequently left the authority.

The on-line course has been upgraded to include this option.

Action Complete.

**RSM Action 5 – Checking Awareness of Data Protection.** A process to be in place for checking staff awareness/understanding of data protection.

The on-line course has a quiz at the end of the training.

Action complete

**RSM Action 6 – Data Protection Policy.** The Data Protection Policy is to be updated to cover potential fines for non-compliance, the right of individuals to claim compensation for damages caused by a breach, the right to object and the details of the new Data Protection Officer.

The following policies have been updated to reflect the RSM request (highlighted in yellow on the attached documents). A Data Retention Schedule has also been created.

- Data Protection Policy – Appendix 1
- Data Retention Policy – Appendix 2
- Data Retention Schedule – Appendix 3

The changes were approved by the Monitoring Officer who was given delegated authority to approve the policies at the A&G meeting on 24 September 2021 and the CA Board on 27 October 2021.

**RSM Action 7 – Data Protection Roles and Responsibilities.** The roles and responsibilities of the Data Protection Officer are to be recorded in their job description. The following to be included – that they do not determine the purposes and means of the processing of personal data in the organisation or have decision-making responsibilities which may cause a conflict of interest and that the DPO operates independently.

A job description has been created.

Deadline – complete.

**RSM Action 8a – Data Breaches.** The Data Incident Report Policy to be revised to include

- reporting and recording of near misses in addition to actual data breaches;
- how to determine whether a data breach requires reporting to the ICO, for instance, where a risk is likely to affect people's rights and freedoms;
- post-breach review, including lessons learnt;
- what information a data breach notification to the ICO should contain in line with ICO guidance;
- how the data breach is to be notified to the ICO;
- what to do if all information is not available to report to the ICO within 72 hours;
- the requirement to notify an individual affected by the breach under certain circumstances;
- what information to provide to individuals when notifying them about a data breach in line with ICO guidance;
- disciplinary information for breach of the Policy; and
- the new Data Protection Officer details.

A copy of the following documents are attached:

- Data Incident Reporting Policy – Appendix 4
- Data Incident Reporting Form – Appendix 5

The changes were approved by the Monitoring Officer who was given delegated authority to approve at the A&G meeting on 24 September 2021 and the CA Board on 27 October 2021.

Deadline - complete

**RSM Action 8a – Data Breaches.** The log for GDPR breaches to be updated to include details of near miss (in addition to actual breaches); date of when the breach occurred; content of data lost/impacted; format of data lost/impacted; source of data lost/impacted; categories of those affected by the breach, root cause of the breach; consequences, whether the breach was notifiable to the ICO.

The log has been updated.

Deadline – complete

**RSM Action 9 – Password Protected Communications.** The Password and Authentication Policy to be updated to provide specific guidance in relation to utilising password protected communications where personal data is involved.

The policy has been updated to reference training. The Access Control Policy contains information on confidential data.

Action – complete.

2.4 Information Risk Group Meeting

An Information Risk Group meeting is held monthly. Attendees at present are Data Protection Officer, Senior Information Risk Officer, Head of Digital Services at SOCITM, PMO Manager, Programme Co-ordinator, Finance rep

Standard agenda items are Data Protection update report, FOI/ EIR/SAR/Complaints update, SIRO update, Information Security update. Action notes are taken at each meeting.

2.5 Other work

- Data Protection Training/Information Security Training – a programme has been compiled to ensure that the CPCA is compliant with GDPR. All new starters are required to complete the two mandatory training courses. This training needs to be completed each year.

**Table showing Data Protection/Information Security course compliance**

| Date | Course | Staff completed training | Staff started training but not completed | Staff not started training | Staff on system |
|---|---|---|---|---|---|
| 01/03/2023 | Data Protection | 98 | 4 | 11 | 113 |
| 01/03/2002 | Information Security | 100 | 5 | 8 | 113 |

- Data Protection Impact Assessment Screening Checklist/Data Protection Impact Assessment (DPIA) – a DPIA describes a process designed to identify risks arising out of the processing of personal data and to minimise these risks as far and as early as possible. DPIAs are important tools for negating risk, and for demonstrating compliance with the GDPR. The forms for the CPCA can be found at Appendix 6 and 7. These are added for reference.

- Sharepoint Redesign Project - storage of digital documents being moved to a team share site to make data more secure.

- Storage of physical documents to an off-site storage location – legal documents are being stored at an off-site storage unit as the CPCA does not have access to a fire-proof cabinet at Pathfinder House.

## Significant Implications

## 3. Financial Implications

3.1 There are no financial implications
.

## 4. Legal Implications

4.1 The Combined authority is under a duty to ensure that it processes, holds and releases any information in line with a range of legislative provisions including General Data Protection Regulation, Data Protection Act 2018, Freedom of Information Act, Privacy and Electronic Communications Regulations and the Human Rights Act.

4.2 The CA also has a duty to publish information wherever possible, and in accordance with its own publication scheme. However, regard should be had to not publishing any information of a confidential or sensitive nature, in accordance with the relevant legislation and public interest tests.

4.3 Ineffective information governance arrangements have a number of inherent risks in the context of organisational management, the use of resources and service delivery. Addressing any issues raised in this report is a means of mitigating such potential risks and maximising opportunities for effective information management and use to support decision making and service delivery.

## 5. Public Health Implications

5.1 There are no Public Health implications

## 6. Environmental and Climate Change Implications

6.1 There are no environmental and climate change implications.

## 7. Appendices

7.1 Appendix 1 - Data Protection Policy
Appendix 2 - Data Retention Policy
Appendix 3 - Data Retention Schedule
Appendix 4 - Data Incident Reporting Policy
Appendix 5 - Data Incident Reporting Form
Appendix 6 - Data Protection Impact Assessment Screening Checklist
Appendix 7 - Data Protection Impact Assessment