Coventry City Council

Public report
Audit and Procurement Committee

Audit and Procurement Committee — 31 January 2022

Name of Cabinet Member:
Cabinet Member of Policy and Leadership – Councillor G Duggins

Director Approving Submission of the report:
Director of Law and Governance

Ward(s) affected:
None

Title:
Information Governance Annual Report 2020/21

Is this a key decision?
No

Executive Summary:

Information is one of the Council's greatest assets and its correct and effective use is a major responsibility and is essential to the successful delivery of the Council's priorities. Ensuring that the Council has effective arrangements in place to manage and protect the information, both personal and business critical, it holds is a priority.

Data protection legislation sets out the requirements on organisations to manage information assets appropriately and how they should respond to requests for information. The Information Commissioner's Office (ICO) is the UK's independent supervisory authority set up to uphold information rights in the public interest, promote openness by public bodies and data privacy for individuals, and monitors compliance with legislation.

This report provides a summary of the Council's performance during 2020/2021 in responding to requests for information received under the above-mentioned legislation. It also reports on the management of data protection security incidents and/or those reported to the ICO and data protection training

Recommendations:

The Audit and Procurement Committee is recommended to:

1) Note the Council's performance on Freedom of Information, Subject Access and other Data Protection Act requests, including the outcomes of internal reviews and the number and outcome of complaints made to the ICO.

2) Note the reporting and management of data security incidents and/or those reported to the ICO.

3) Note data protection training compliance

4) Identify any comments or recommendations

List of Appendices included:

None

Background papers:

None

Other useful documents

None

Has it been, or will it be considered by Scrutiny?

No

Has it been, or will it be considered by any other Council Committee, Advisory Panel or other body?

No

Will this report go to Council?

No

Report Title: Information Governance Annual Report 2020/21

1 Background

1.1 The Information Governance (IG) is the strategy or framework for handling personal information in a confidential and secure manner while ensuring compliance with the relevant statutory and regulatory requirements. IG within the Council is delivered through a distributed model of responsibility rather than through the sole responsibility of the IG Team, with key roles identified and assigned to ensure appropriate oversight and accountability:

- Head of Information Governance
- Information Governance Team
- Senior Information Risk Officer (SIRO)
- Data Protection Officer (DPO)/DPO Team
- Information Asset Owners (IAO)
- Information Asset Managers (IAM) (Heads of Service)
- Information Management Strategy Group

1.2 The function of Information Governance supports the Council's compliance with the General Data Protection Regulations GDPR (UK GDPR), Data Protection Act (DPA) 2018, Freedom of Information Act 2000 (FOIA) and Environmental Information Regulations (EIR). The Council has a statutory obligation to comply with the IG framework by responding appropriately to requests and managing personal data lawfully. The IG Team assist the organisation by monitoring internal compliance, informing and advising on data protection obligations, providing advice and guidance and raising awareness on data protection matters.

1.3 FOIA/EIR impose a statutory obligation on the Council to respond to requests for information within 20 working days, subject to relevant exemptions. The Code of Practice, issued by the Secretary of State for Constitutional Affairs under Section 45 of the FOIA, requires public authorities to have a procedure in place to deal with complaints in regard to how their requests have been handled. This process is handled by the Information Governance Team as an FOI/EIR internal review. After an internal review has been completed an applicant has a right to complain to the Information Commissioner's Office (ICO) for an independent ruling on the outcome. Based on the findings of their investigations, the ICO may issue a Decision Notice. The ICO may also monitor public authorities that do not respond to at least 90% of FOI/EIR requests they receive within 20 working days.

1.4 The DPA 2018 provides individuals with the right to ask for information that the Council holds about them. These are also known as Subject Access Requests (SARs). The Council should be satisfied about the individual's identity and have enough information about the request. The timescale for responding to these requests is one month, starting on the day of receipt. Authorities can extend the time taken to respond by a further two months if the request is complex or a number of requests have been received from the individual, e.g. other types of requests relating to individuals' rights.

1.5 There is no requirement for the Council to have an internal review process for SARs. However, it is considered good practice to do so. Therefore, the Council informs applicants of the Council's internal review process. However, individuals may complain directly to the ICO if they feel their rights have not been upheld.

1.6 The Council also receives one-off requests for personal information from third parties including the police and other government agencies. The IG Team maintains a central log that includes exemptions relied on when personal data is shared with third parties. They

provide advice and assess whether the Council can lawfully disclose the information or not.

1.7 The Council's Management of data protection security incidents is undertaken by the Data Protection Officer Team, they record, investigate and where necessary, recommend actions to be taken based on the impact risk level.

1.8 The Data Protection Officer Team supports the Council in understanding the impact of plans, projects and activities on data protection through a process of impact assessments to support decision-making. The Council also has arrangements in place to support the sharing of data where appropriate and the team provide support in the preparation and sign off of on-going and one-off data sharing agreements.

2 Information Governance Annual Report 2020/21

2.1 The landscape in which public authorities are now operating has seen its third significant change since introduction of the GDPR and the new Data Protection Act 2018 (DPA 2018) in 2018. At the end of the 2019/20 year, the country went into lockdown as part of its response to the Covid 19 pandemic and the impact of Brexit has subsequently led to introduction of the UK GDPR.

2.2 The pandemic has resulted in significant changes to ways of working and priorities. During this period, the Information Governance Team has supported the Council to adapt and keep working effectively. It has facilitated the rapid turnaround of sharing requests and needs whilst ensuring requests have been properly assessed to confirm that the personal data of the people concerned is used in line with relevant legislation and in keeping individuals informed of how their data is handled. This has allowed data to flow compliantly for the purposes of the Council's pandemic response. The IG Team has supported the organisation as new ways of working have been introduced to meet needs while ensuring the continuing protection of information.

2.3 The numbers of requests for information received by the City Council have remained high throughout the pandemic and subsequent lockdowns and the IG function has seen a significant increase in demand for its services.

2.4 Data Security and Protection Toolkit

2.4.1 The Data Security and Protection Toolkit is an online tool that allows relevant organisations that process health and care data to measure their performance against data security and information governance requirements which reflect legal rules and Department of Health policy. This independently audited self-assessment tool enables the Council to demonstrate that it can be trusted to maintain the confidentiality and security of personal information, specifically health and social care personal records.

2.4.2 All organisations that have access to NHS patient data and systems must use this Toolkit to provide assurance that they are practicing good data security and that personal information is handled correctly.

2.4.3 For the 2020/21 reporting period, the submission deadline was 30 June 2021. Ordinarily this is 31 March each year, however due to national, regional and local response requirements to Covid-19, there has been an extended timeframe for both the 2019/20 self-assessment and the 2020/21 self-assessment submission.

2.4.4 The 2020/21 Toolkit was successfully completed, and it was confirmed that the Council has appropriate evidence available for its assessment and the Toolkit standard was met.

2.5 Requests for information

2.5.1 The number of Freedom of Information Requests received by the Council had generally been increasing year on year but reduced from 1474 in 2019/20 to 1267. The Council responded to 71% of FOIA/EIR requests within the target time of 20 working days in 2020/21 compared to 78% for the previous year (see table 2). Performance remains below the target set by the ICO.

2.5.2 In February 2021 a new FOI management system went live and for a short period of time the IG Team needed to run both systems until such time as all the requests on the old system had been completed.

(588 requests were received during the first two quarters of 2021/22 and response rates have improved to 83% following the introduction of the new management system and new arrangements for managing requests.)

2.5.3 The Council received 47 requests for internal reviews in the year 2020/21 (compared to 48 the previous year). The Council responded to these with the following outcomes:

- 19 were not upheld – the exemptions that had been applied were maintained and no further information was provided
- 8 were not upheld – but advice or clarification was provided
- 10 were partially upheld – further was information provided
- 8 were upheld - information was provided
- 1 was withdrawn
- 1 was closed with no further action

(35 requests for internal reviews have been received during the first three quarters of 2021/22).

2.5.3 Four complaints were referred to the ICO during 2020/21 (compared to five the previous year). The reasons and outcomes for these were:

- Three complaints related to the handling of an FOI and the exemptions engaged by the Council. The ICO issued a decision notice on one and required no further action on the remaining two. The complaints were not upheld.
- One complaint has still to be allocated a Case Worker within the ICO.

(Six complaints have been referred to the ICO during the first three quarters of 2020/21 and five are awaiting the allocation of an ICO case worker.)

Table 1. Number of FOI/EIR requests received

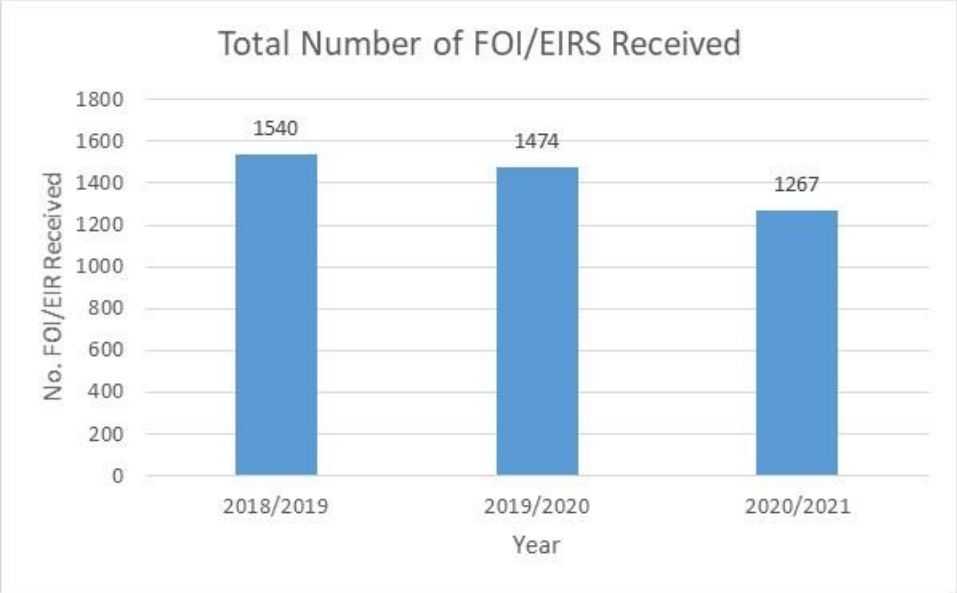
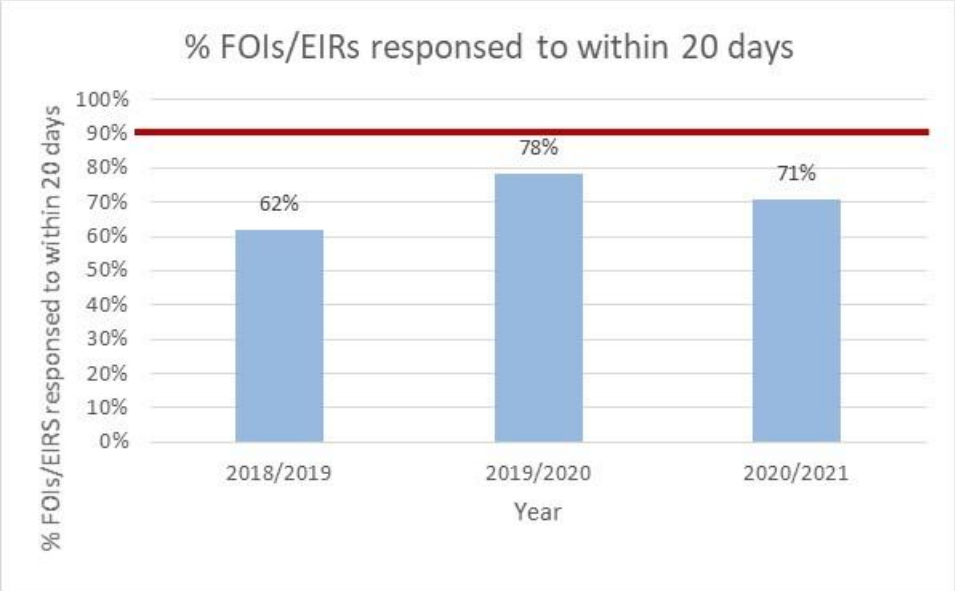


Table 2. Proportion of FOI/EIR requests completed within target time



ICO Adequate Response Rate 90%

2.6.4 The City Council already publishes a significant amount of information and identifying opportunities to increase the volume and type of information published (subject to legal compliance) will increase transparency and help to reduce the number of FOI's the Council receives because the information will already be available.

2.6.5 The Council received 268 valid Subject Access Requests (SARs) during 2020/21. The number of SARs has been rising year on year with a significant increase seen following the introduction of the GDPR. While the Council receives fewer SARs than other information requests, many of these are complex and can involve managing significant amounts of sensitive information. The introduction of the GDPR also reduced the required response time for responding to SARs from 40 days to one calendar month. The completion rate within the target time has seen a slight increase to 76% (see table 4).

Table 3. Number of SAR's received

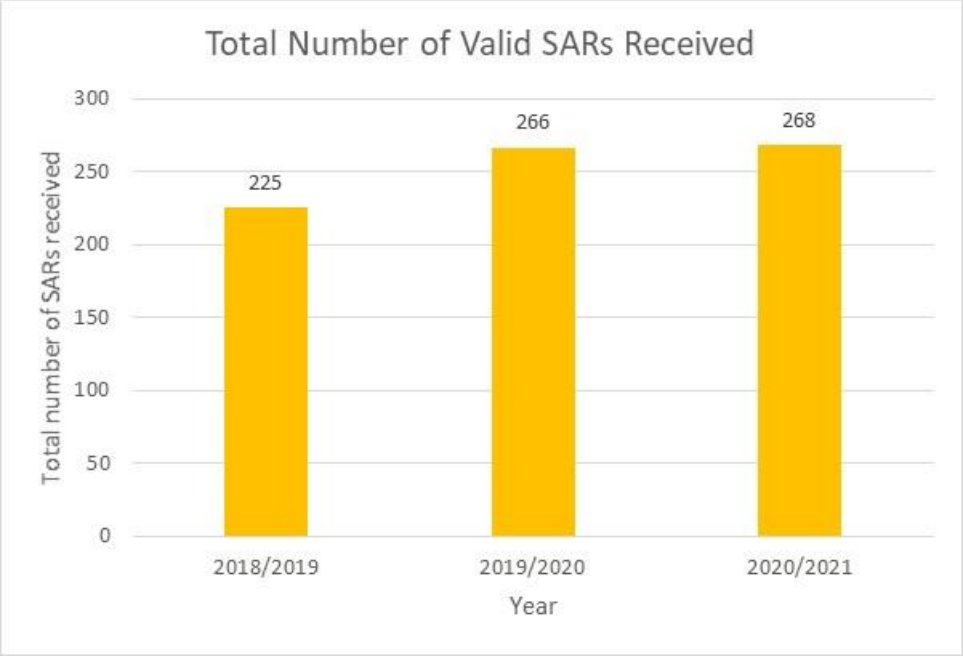
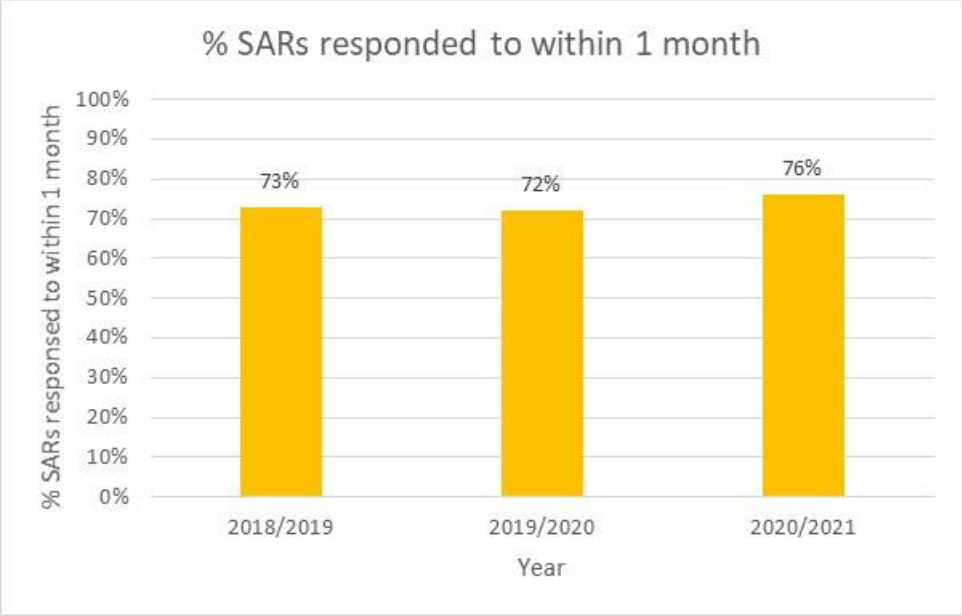


Table 4. Proportion of SARs responded to within target time



% Complete within either 1 month, or 3 months where complex extension applied in 2020/2021 is 86%

2.6.6 The Council received 8 requests to carry out an internal review into a SAR application during 2020/21 (compared to four the previous year). In 5 cases, further information was provided which was located through further searches based on information provided by the requester. Where information was not provided, this was due to a) the original exemptions were upheld regarding grievance/disciplinary process and b) information was not held by the council.

2.6.7 No complaints were referred to the ICO related to Subject Access Requests in 2020/2021.

2.7 Data Security Incidents

2.7.1 Protecting information from theft, loss, unauthorised access, abuse and misuse is crucial in order to reduce the risk of data breaches or financial loss incurred through non-compliance with key legislation.

2.7.2 The IG data protection security incident reporting process supports the Council's objective that breaches are managed promptly, and outcomes of investigations are used to inform reviews of the control measures in place to keep personal information secure.

2.7.3 In addition, the Council encourages the reporting of near misses and potential breaches as this promotes awareness, avoids complacency therefore reducing the likelihood of a serious breach to information. Increased data protection awareness within the organisation has resulted in an increase in reports and investigations although not all reported incidents will have resulted in a breach. Even where there is no breach, incidents can provide valuable insight into training requirements and processes and procedures which may need to be strengthened as a preventative measure. When investigating data protection security incidents, the Data Protection Team routinely consider resultant training needs and bespoke training and/or advice is provided as required. Messages continue to be provided to staff alerting them to the need to protect personal data and use it appropriately.

2.7.4 In 2020/21, 295 reports of information security incidents were sent to the Data Protection Team, an increase from 219 in the previous year. Of these, 165 did not involve a breach of personal data. These included for example near misses, loss or theft of equipment, cases where technical measures prevented access to data and incidents where a breach was contained. Of the incidents where a breach of personal data was identified, 112 were identified as low risk, 6 low/medium, 7 medium and 1 high. The majority of reports were classified as information being disclosed in error with 25 reports relating to loss or theft of hardware, 18 to technical/procedural errors and 13 unauthorised access.

2.7.5 The GDPR introduced requirements for personal data breaches that meet certain thresholds to be reported to the ICO. No self-reports were made to the ICO during 2020/2021.One complaint was made by a data subject directly to the ICO who assessed that the council failed to ensure security of personal data when it disclosed third party information and asked the council to ensure that staff who handle personal data are aware of the importance of keeping data secure. In addition, a third-party organisation working with the council had an incident which resulted in the breach of City Council data. They self-reported to ICO.

2.8 Training and Awareness

2.8.1 Data Protection training is key to ensuring staff are aware of their responsibilities. Training is currently delivered through the Council's e-learning platform and annual completion of the data protection course is mandatory for all staff with access to personal data. Staff who do not have access to a computer in their role (not office based) and those with minimal personal data involved in their role are provided with appropriate level training. This ensures that an appropriate level of understanding and awareness is reached that is relevant to their role/responsibilities.

2.8.2 For the 2020/21 year, the Council reported a completion rate of the Council's mandatory data protection training of 95% when completing NHS Data Security and Protection Toolkit.

2.8.3 In addition to the above, ICT have delivered awareness sessions specifically relating to cyber security and regular cyber security messages are issued by ICT to staff.

3 Options considered and recommended proposal

3.1 It is essential that the Council continues to monitor and report on its performance in relation to access to information requests, information security incidents and training completed in order to promote best practice information governance and drive continuous improvement in the Councils ability to comply with the laws relating to information.

4 Results of consultation undertaken

4.1 None

5 Timetable for implementing this decision

5.1 None

6 Comments from Chief Operating Officer (Section 151 Officer) and the Director of Law and Governance

6.1 Financial implications

There are no specific financial implications resulting from the issues within this report although it is worth noting that the Information Commissioner's Office is able to levy significant fines for serious non-compliance with the legislation surrounding the management of information.

6.2 Legal implications

There are no specific legal implications arising out of the recommendations. However, the Council's performance is subject to external scrutiny by the ICO, who have the authority to impose sanctions upon the Council for non-compliance. The monitoring and reporting on the outcomes of ICO complaints represents good practice and promotes good governance and service improvement.

7 Other implications

7.1 How will this contribute to the Council Plan (www.coventry.gov.uk/councilplan/)?

The monitoring and reporting of the Council's performance regarding responding to, and handling access to information requests under FOIA and DPA 2018, including any complaints made to the ICO will enable continuous improvement, raise awareness and promote high standards of information governance, fostering a culture of openness and transparency within the Council and demonstrating our commitment to best practice information governance, security, and protection.

7.2 How is risk being managed?

The reporting and monitoring on the Council's performance to information laws and outcomes of ICO complaints will help reduce the risk of the ICO upholding complaints and taking enforcement action against the Council.

7.3 **What is the impact on the organisation?**

Operating best practice Information Governance and Security will support public confidence in the Council, offering assurance to service users of the council's commitment to Data Protection and Transparency. Partner and client organisations will have the assurance they required in order to engage with the Council and share data. the risks of serious breaches of personal Data/Information Assets should be reduced thus reducing the likelihood of action by the ICO.

7.4 **Equality Impact Assessment (EIA)**

The Council's responsibilities under Section 149 of the Equality Act 2010 are supported by UK GDPR/DPA2018, requiring that Special Category Data is afforded extra measures of security to protect that data.

7.5 **Implications for (or impact on) climate change and the environment**

None

7.6 **Implications for partner organisations?**

As set out in paragraph 7.3 above.

Report author's Name and job title:
Sharon Lock
Head of Information Governance

Service:
Information Governance

Tel and email contact:
Sharon Lock: 024 7697 0982
sharon.lock@coventry.gov.uk

Enquiries should be directed to the above personnel.

Contributor/approver name	Title	Service	Date doc sent out	Date response received or approved
Contributors:				
Adrian West (DPO)	Members and Elections Team Manager	Law and Governance	14/01/22	18/01/22
Michelle Salmon	Governance Services Officer	Law and Governance	14/01/22	18/01/22
Names of approvers for submission: (officers and members)				
Paul Jennings	Finance Manager (Corporate Finance)	Finance	20/01/22	20/01/22
Julie Newman (SIRO)	Director of Law and Governance	Law and Governance	14/01/22	19/01/22
Councillor G Duggins	Leader and Cabinet Member for Policy and Leadership	-	14/01/22	20/01/22

This report is published on the council's website: www.coventry.gov.uk/councilmeetings