Coventry City Council

Public report

Audit and Procurement Committee

Audit and Procurement Committee 16th July 2018

Name of Cabinet Member:
Cabinet Member for Policy and Leadership - Councillor G Duggins

Director Approving Submission of the report:
Director of Finance and Corporate Resources

Ward(s) affected:
None

Title:
2017/2018 Information Governance Annual Report

Is this a key decision?
No

Executive Summary:

The City Council adopted its Information Management Strategy in March 2016. The Strategy recognises that information is one of the Council's greatest assets and its correct and effective usage is a major responsibility and essential to the successful delivery of the Council's priorities. Since the introduction of the Strategy, the Council has put a range of measures in place to embed effective information governance throughout the organisation.

The implementation of the Information Management Strategy was a key step in helping the City Council to prepare for the implementation of the General Data Protection Regulation which came into force in May 2018 and introduced the most significant change in data protection legislation in 20 years. The GDPR strengthens the rights of individuals and reflects the significant technological changes that have taken place over the last 20 years since the Data Protection Act legislation was introduced in 1998. The GDPR has been written into UK law and the new Data Protection Act 2018 also came into force in May 2018.

Data protection legislation sets out the requirements on public 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 sets out how the Council performed during 2017/18 in responding to requests for information received under the Freedom of Information Act, Environmental Information Regulations and Data Protection Act, the completion rate, outcome of internal reviews and complaints made to the ICO. It also reports on the management of data protection security incidents reported, data protection training, preparations for the introduction of the General Data Protection Regulations and the follow up to the ICO Audit of the Council's data protection arrangements which took place during the year.

Recommendations:

1. The Audit and Procurement Committee is recommended to review:

   a) 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.

   b) Reporting and management of data security incidents.

   c) Data Protection training compliance for employees.

   d) Data protection training arrangements for Members, including any requirements

2. The Audit and Procurement Committee is recommended to identify any comments or recommendations to the Cabinet Member for Policy and Leadership

List of Appendices included:

Appendix A – Number of FOI/EIR requests received and completion rates in the last 3 years
Appendix B – Number of Subject Access Requests received and completion rates in the last 3 years
Appendix C – Nature and severity of data protection security incidents reported in 2017/2018

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: 2017/18 Information Governance Annual Report

1. Context (or background)

1.1 The Information Management Strategy Group oversees the Council's performance in relation to handling requests under the Freedom of Information Act (FOIA), Environmental Information Regulations (EIR) and Data Protection Act (DPA) 1998. This is part of monitoring compliance with relevant legislation as stated in the Council's Information Management Strategy. The Information Governance Team (IGT) coordinates requests received. The team also manages data protection security incidents reported to them by recording, investigating where necessary and recommending actions to be taken based on the risk level.

1.2 The Council is obliged to respond to information requests under FOIA/EIR 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 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 IGT as an FOI/EIR internal review.

1.3 After an internal review has been completed an applicant has a right to complain to the 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 sufficient information about the request. For the period of this report the Council had to receive the statutory £10 fee before it could respond and had to complete the response within 40 calendar days.

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, like with FOIA/EIR requests, 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 IGT maintains a central log that includes exemptions relied on when personal data is shared with third parties. The IGT gives advice and assesses whether the Council is allowed to disclose the information or not.

1.7 Data security incidents reported to the IGT vary in severity based on the nature of the data compromised and the impact of the breach on the data subjects or the people whom the information is about.

1.8 The introduction, in May 2018, of the General Data Protection Regulation (GDPR) and passing of the Data Protection Act 2018 represented the most significant change in data protection legislation in 20 years. It strengthened the rights of individuals and reflects the significant technological changes that have taken place over the last 20 years since the Data Protection Act of 1998. This report covers the 2017/18 financial year, so reports against the Council's obligations under previous legislation, but also includes an update

on preparation for the implementation of the GDPR. It covers how the Council handles requests received under FOIA, EIR and DPA. It outlines the number of requests received, proportion of responses completed within the set timescales and outcomes of internal reviews and complaints made to the ICO during 2017/18. Details on the number of data protection security incident reported and data protection training completed by Council employees are also included.

1.9 **Freedom of Information and Environmental information Regulations**

1.9.1 The number of FOI requests received by the City Council increased again on the previous year. 1471 FOI/EIR requests were received in period 2017/18, compared to 1374 requests received in the 2016/17. The Council responded to 73% of FOIA/EIR requests within the target time of 20 working days in 2017/18 compared to 68% for the previous year. Despite the number of requests increasing, the proportion of requests dealt with within the target time has improved again, although performance remains below the 90%, the level required by the ICO. See Appendix A.

1.9.2 There were 39 requests for internal reviews in the year 2017/18 compared to 15 in the previous year. The Council responded to these with the following outcomes:

- 14 were not upheld – the original response and any exemptions applied were maintained and no further information was provided
- 12 were partially upheld - further information was provided
- 8 were upheld and the requested information provided
- 3 remain under consideration and have not yet been closed.
- 1 requester submitted a new request
- 1 sought clarification from the requester as questions had been answered but no response was received

1.9.3 Six complaints were referred to the ICO. The reasons and outcomes for these were:

- 1 – Time taken to respond and failure to respond to request to review – response provided
- 2 - Initial response to request not received; response provided
- 2 – Handling of request under Section 50 – no further action required
- 1 – requester is now appealing the ICO's decision and has applied to the First Tier Tribunal. Still awaiting outcome.

1.10 **Data Protection Act Requests**

1.10.1 The Council received 136 valid Subject Access Requests (SARs) during the course of 2017/18, compared to 144 in the previous year. There was an improvement in the response rate to SARs 112 (82%) were completed within 40 calendar days compared to 68% in 2016/17. The Council still receives requests relating to social care that are complex to deal with and take a long time to complete. Summary of the number of requests received performance in the last 3 years is shown in Appendix B.

1.10.2 The Council received one application to carry out an internal review into a SAR application in the course of the year, which was not upheld. Two SAR complaints were referred to the ICO. In one, the ICO upheld the Council's decision not to provide the information after applying an appropriate exemption. In the other complaint, the requester had complained he had not received a full response within the 40 calendar days. However it had previously been agreed with the requester to receive the information by way of a staged disclosure, which had been completed. No further action was required on both complaints.

1.10.3 The new General Data Protection Regulation that came into effect in May 2018 requires the Council to respond to SARs within one calendar month (and 2 calendar months for complex requests). Under the GDPR, the Council is no longer able to charge a £10 fee for SARs. The Council can be fined for not meeting the deadlines or providing insufficient information to the requester. By their nature, SARs can be complex and the preparation of comprehensive responses time consuming. The IG Team has reviewed its processes for dealing with SARs in line with GDPR and is working with services to ensure that the Council meets its obligations.

1.10.4 Under Section 29 of the DPA the police and other agencies can request for personal information for the purposes of prevention and detection of crime. Other DPA exemptions exist where the organisations can disclose personal data in exceptional situations. 350 'one-off' requests were logged on the central register managed by the IGT. 326 (93%) of these requests have been completed or closed on the central register. IGT responded to a majority of these and others were allocated directly to specific service areas to respond.

1.11 **Data Protection Security Incidents**

1.11.1 The Council's Information Management Strategy sets out the need to protect information from theft, loss, unauthorised access, abuse and misuse. This is important in order to reduce the risk of data breaches or financial loss incurred through non-compliance with key legislation such as the DPA. It is good practice to report on information incidents and breaches.

1.11.2 An effective data protection security incident reporting process ensures that any breaches are contained and managed promptly and the outcomes of the investigation are used to inform reviews of the controls that are in place to keep personal information secure. The reporting of near misses is also actively encouraged. The process allows the organisation to learn from mistakes and prevent serious breaches that may cause harm to individuals and the Council.

1.11.3 Continuous improvements are being made to the data security breach management process that is being aligned to the new Information Risk Management Policy, approved in March 2017. The new Information Asset Register identifies designated Information Asset Owners who have responsibility for investigating any breach of their information assets.

1.11.4 The management of data security incidents or breaches reported involves containing and recovering any compromised information, assessing the harm or risk posed by the breach, considering whether to notify the affected individuals or relevant authorities where necessary and determining mitigation needed to prevent further occurrence of similar incidents. The risk assessment is based on the likely or actual harm to individuals, number of individuals affected and the level of sensitivity of the personal information compromised. The risk assessment score used is based on guidance issued by the Health and Social Care Information Centre (HSCIC) which takes into account the impact and likelihood the breach would have on the individuals. In most of the incidents reported the risk level was low as the data compromised was either contained, not sensitive, encrypted or only a few individuals were affected. See Appendix C.

1.11.5 In 2017/18, there were 114 information security incidents reported, compared to 138 in the previous financial year. The majority of reported incidents were as a result of information being disclosed in error. A breakdown of the nature of incidents reported is illustrated in Appendix C.

1.11.6 Whilst it was not a requirement under the relevant legislation to report breaches to the ICO, this was recommended where there was a likelihood of significant harm to the individuals or a large number of individuals were affected.

1.11.7 Two incidents were reported to the ICO in 2017/18, resulting from children's social care paperwork being left in a property and the theft of documents from the car of a commissioned service provider. Both were concluded with no enforcement action due to sufficient remedial measures being taken by the Council. This compares to two incidents reported to the ICO in 2016/17. The Council has considered all recommendations following these investigations and carry out regular process reviews in order to minimise the risk of further breaches occurring.

1.11.8 The ICO reviewed the 2016/17 Information Governance annual report to look at the variance between the number of reported security incidents and those that the Council had reported to the ICO. It concluded that that "Coventry City Council are risk assessing information security incidents and conducting trend analysis in an appropriate manner and reporting to the ICO in a considered manner".

1.11.9 During their investigations, the ICO considers controls that organisations have in place to minimise occurrence of similar incidents and if similar incidents by the same organisation have been reported to them. Recent fines issued by the ICO for data protection security breaches by public sector organisations include:

- Nottinghamshire County Council; £70,000 – for leaving vulnerable people's personal information exposed online for five years
- Gloucester City Council; £100,000 – after a cyber attacker accessed council employees' sensitive personal information
- Gloucestershire Police: £80,000 – after sending a bulk email that identified victims of non-recent child abuse.

1.11.11 The GDPR introduces the requirement that a personal data breach must be reported to the Information Commissioner within 72 hours of becoming aware of the breach if it's likely to result in a risk to people's rights and freedoms. The Council has been working to update and strengthen its arrangements for reporting, managing and reviewing data security incidents and raising awareness of the need to report all incidents and near misses promptly so that relevant actions can be taken and lessons learned.

1.12 **Data Protection Training**

1.12.1 An Information Management and Data Protection Training Strategy was prepared in March 2018 to support the implementation of the Council's Information Management objectives. The Strategy incorporated recommendations made by the Information Commissioner's office following their recent audit. It sets out approach to training for Data Protection Legislation, including the General Data Protection Regulation, Information Security, Records Management, Freedom of Information Act and Subject Access Requests. It sets out how the Council will ensure that the entire workforce has the skills and competence required to carry out the activities in which information is collected, stored and processed, and that they are aware of the legislative environment and their roles and responsibilities. It includes how compliance will be monitored and reported and how the Council will evaluate the effectiveness of training.

1.12.2 In line with the new Training Strategy and to support the implementation of the General Data Protection Regulation, the Council updated its online training which all networked employees are required to complete. The first module is an introduction to data protection and is aimed at everyone who handles personal data. It covers what is meant

by personal data, the responsibilities of those handling it and the principles of data protection. It also explains the changes to Data Protection laws that came into force with the implementation of the General Data Protection Regulations and the stronger rights for individuals. The addition of a second module addressing information security, meets a further recommendation from the ICO. This deals with how other people's information, such as a person's name and address or details about their health or financial situation, should be handled. It covers the importance of keeping data secure, what needs to be protected and who it should or shouldn't be disclosed to; the main threats to data and data systems; the basics of cyber security; some key steps to keeping data secure; and how to protect information whilst working on the move.

1.12.3 The deadline for completion of the new online training extended into the 2018/19 year and by the implementation of GDPR on 25 May only six of the almost 4000 employees required to complete the course had not done so. These employees have had their network access restricted until the course has been completed.

1.12.4 The Training Strategy also includes the roll out of basic training for employees who do not have access to the Council's network and introduces new requirements for specialist data protection training for groups of staff who carry out specific roles. Progress in these areas will be monitored by the Information Management Strategy Group.

1.12.5 The online training course has been made available to all elected Members and to date 18 councillors have successfully completed the course. Information on the changes in data protection law has been provided to all Members and a workshop is being planned to highlight case studies that are particularly relevant to Elected Members and discuss any questions or concerns. The Audit Committee are asked to consider any further data protection support that should be offered to Members, including how take up of the training should be encouraged.

1.13 Other Issues

1.13.1 In February the outcomes of a data protection audit carried out by the ICO in November 2017 were reported to the Audit and Procurement Committee. This repeated an audit carried out in 2015 looking at governance arrangements, training and awareness and data sharing arrangements corporately and in Children's Social Care and the Revenues and Benefits service. The Council continues to work on delivering the actions arising from the ICO audit (which includes for example the implementation of the training strategy referred to earlier in this report). A detailed report on progress towards completion of the actions is scheduled for the Audit and Procurement Committee later in the year.

1.13.2 In addition to the measures taken in preparation for the introduction of GDPR identified earlier in this report, the Council has designated a Data Protection Officer as public authorities are required to do. It has been carrying out a programme to put in place records of processing activities to record what data the Council handles and the lawful basis for doing so. This has informed updates to the Council's privacy notices. This work has identified further actions to strengthen the Council's data protection arrangements and the Information Management Strategy Group is monitoring progress.

2. Options considered and recommended proposal

2.1 It is important that the Council continues to monitor and report on its performance in relation to access to information requests, information security incidents and training completed. This, together with the oversight of elected Members helps to promote high standards of information governance and continuous improvement. The ICO reviewed

the Council's 2016/17 Information Governance Report in the context of the number of information security incidents and commented that *"In all, it appears that the Public Report demonstrates a desire by CCC to be open and transparent in both its FOI and DPA obligations, performance and commitments."*

3. Results of consultation undertaken

3.1 None

4. Timetable for implementing this decision

4.1 None

5. Comments from Director of Finance and Corporate Resources

5.1 Financial implications
There are no financial implications in relation to the recommendations in this report.

5.2 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. The monitoring and reporting on the outcomes of ICO complaints represents good practice and promotes good governance and service improvement.

6. Other implications

6.1 How will this contribute to achievement of the Council's Plan?

The monitoring and reporting of the Council's performance for responding and handling access to information requests under FOIA and DPA together with all ICO complaints will promote high standards of information governance and contribute to the openness and transparency of the Council's decision making and commitment to continuous service improvement and equality.

6.2 How is risk being managed?

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

6.3 What is the impact on the organisation?

As set out in 6.1

6.4 Equalities / EIA

As set out in 6.1

6.5 Implications for (or impact on) the environment

None

6.6 Implications for partner organisations?

None

Report author(s):

Name and job title:
Adrian West
Members and Elections Team Manager

Directorate:
Place

Tel and email contact:
Tel: 024 7683 2286
Email: adrian.west@coventry.gov.uk

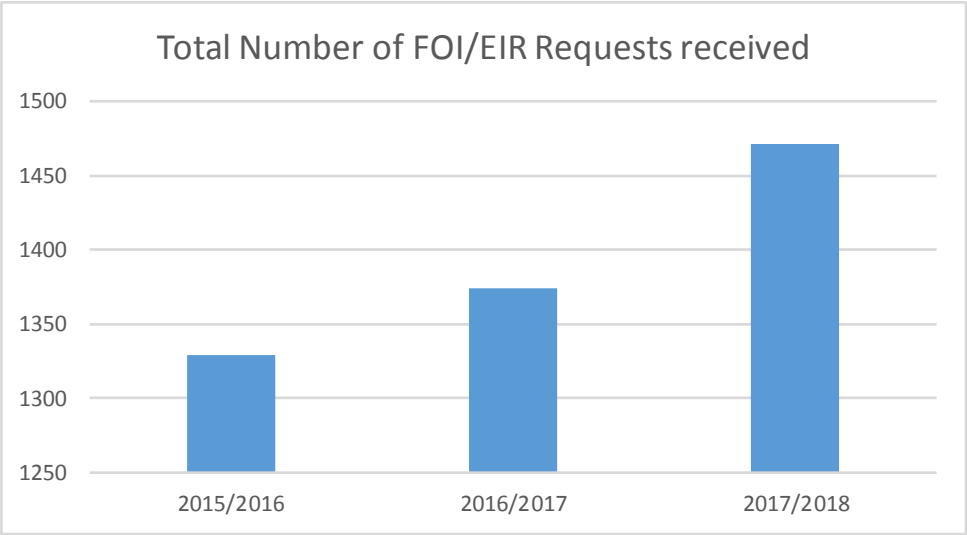
Enquiries should be directed to the above person.

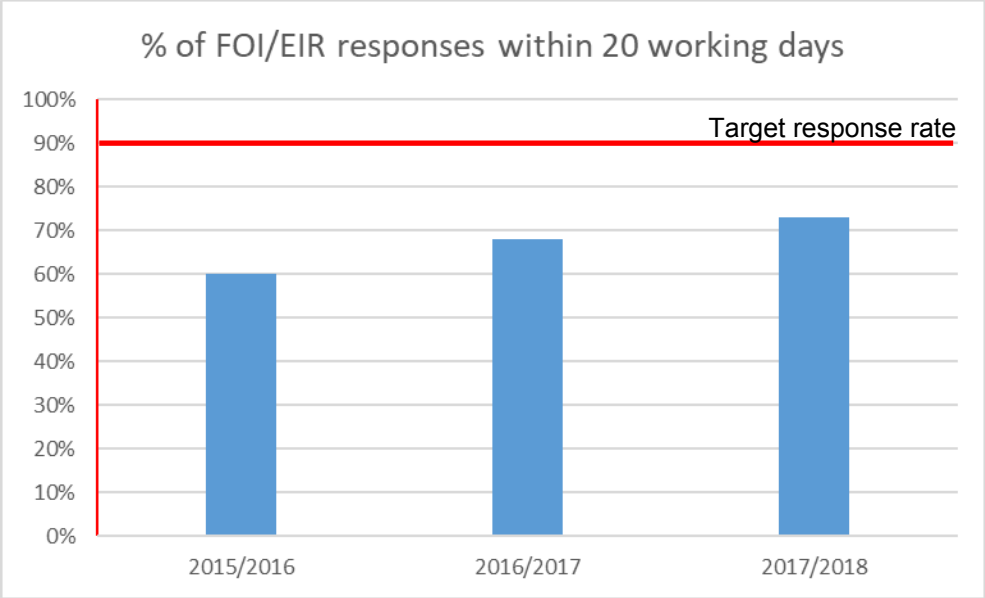
Contributor/approver name	Title	Directorate or organisation	Date doc sent out	Date response received or approved
Contributors:				
Michelle Salmon	Governance Services Officer	Place	28.06.18	28.06.18
Sharon Lock	Head of Information Governance	Place	28.06.18	02.07.18
Joe Sansom	Programme Manager – Transformation Project Team	People	28.06.18	02.07.18
Names of approvers for submission: (Officers and Members)				
Paul Jennings	Finance Manager (Corporate Finance)	Place	28.06.18	28.06.18
Sarah Harriott	Corporate Governance Lawyer, Legal Services	Place	28.06.18	28.06.18
Barry Hastie	Director of Finance and Corporate Resources	Place	28.06.18	06.07.18
Councillor G Duggins	Leader and Cabinet Member for Policy and Leadership	-	28.06.18	05.07.18

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

Appendix A

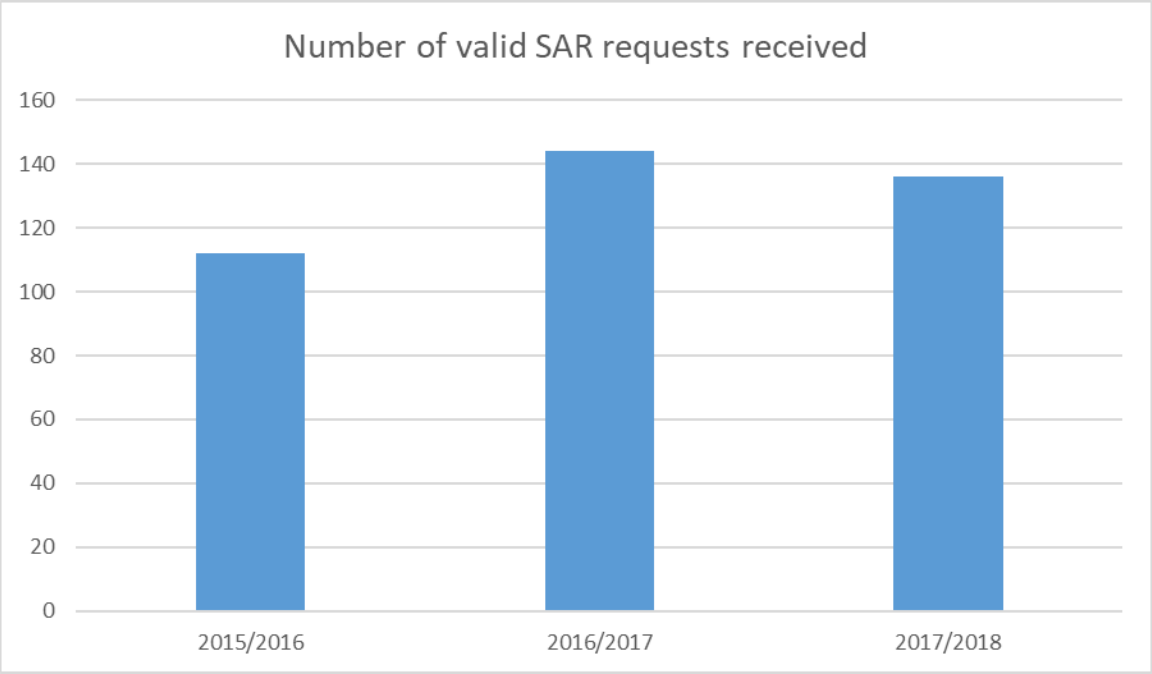
Number of FOI/EIR requests received and completion rates in the last 3 years

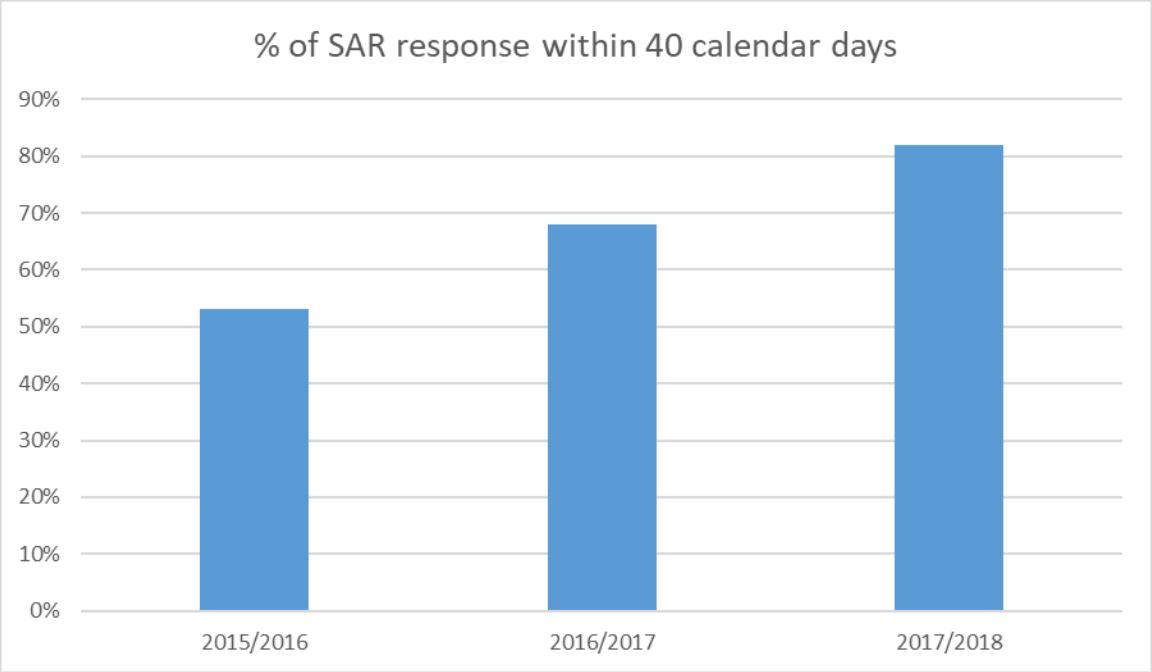




Appendix B

Number of Subject Access Requests (SAR) received and completion rates in the last 3 years.





Appendix C

Nature and severity of data protection security breaches reported and severity in 2017/18