ENTER NAME OF COMMITTEE	AGENDA ITEM No. 14
	PUBLIC REPORT

Report of:	Neil McArthur, Director of Legal & Governance and Monitoring Officer	
Cabinet Member(s) responsible:	Councillor Amjad Iqbal, Deputy Leader and Cabinet Member for Finance and Corporate Governance	
Contact Officer(s):	Neil McArthur, Director of Legal & Governance and Monitoring Officer Ben Stevenson, Head of Information Governance/Data Protection Officer	Tel. 452387

INFORMATION GOVERNANCE ANNUAL REPORT

RECOMMENDATIONS	
FROM: Neil McArthur, Director of Legal & Governance and Monitoring Officer	**Deadline date:** N/A

It is recommended that Audit Committee:

1. Notes the performance of the council and the Information Governance Service.
2. Considers any areas of compliance to be included in future Information Governance reports.
3. Approves the proposal to receive a six-monthly report on personal data breaches to demonstrate the Council's commitment to protecting personal data.

1. ORIGIN OF REPORT

1.1 This annual report is submitted to Audit Committee in line with their terms of reference.

2. PURPOSE AND REASON FOR REPORT

2.1 The purpose of this report is to provide information on a number of key areas of Information Governance including the council's compliance with statutory timeframes for information rights requests, the approach to managing personal data breaches, compliance and training.

2.2 This report is for Audit Committee to consider under its Terms of Reference:

- 3:25: To have oversight of the Regulation of Investigatory Powers policy and processes.
- 4.6: To review the Council's arrangements for corporate governance against the good governance framework, including the ethical framework and agree necessary actions to ensure compliance with best practice and consider the local code of governance.

3. TIMESCALES

Is this a Major Policy Item/Statutory Plan?	**NO**	If yes, date for Cabinet meeting	

4. BACKGROUND AND KEY ISSUES

4.1 Information Governance is a service that seeks to ensure the council's compliance with legislation through positive engagement and experiences with staff at the right time in the right way to support the right development and use of personal data to the benefit of the council and service users. The service compromises 5.68 full time employees and delivers across a number of key statutory functions such as compliance with the UK General Data Protection Regulation, Data Protection 2018 and FOIA/EIR along with connected legislation. The service exists to provide a central and consistent point for the council for colleagues on all Information Governance matters. This may be advice on how to share information securely, what steps are needed to be compliant, what information should be disclosed or simply checking a thought process before making a decision.

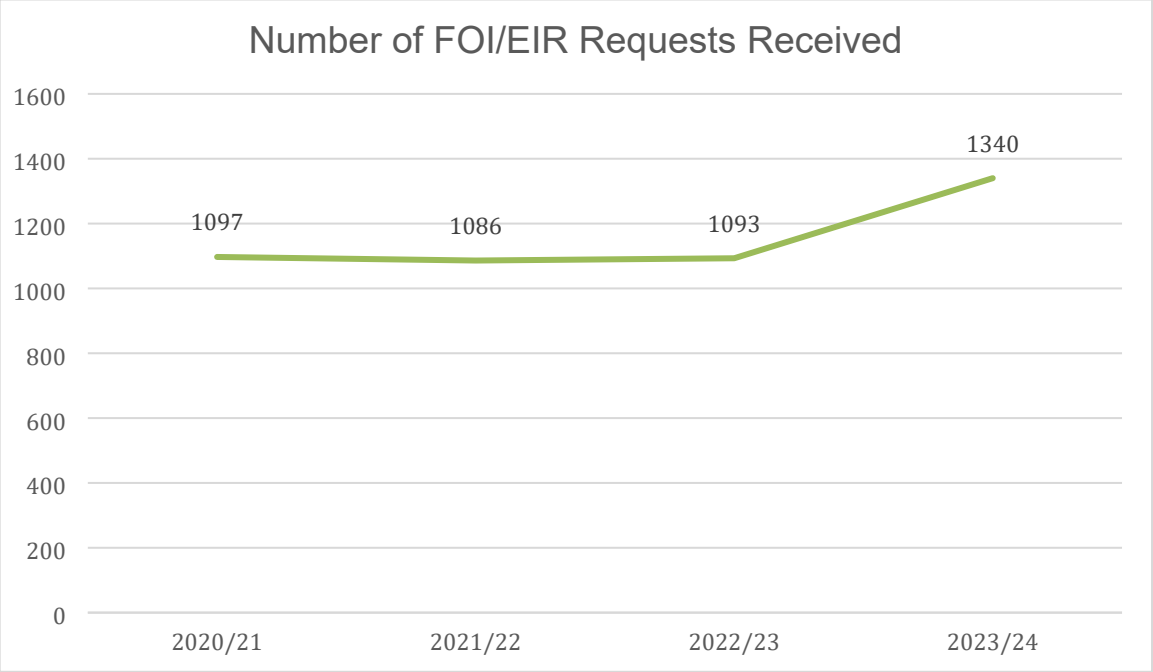
Information Governance also has a critical role in ensuring that the information we as a council hold is considered a valuable asset because it is the foundation of good and informed decision making as well as innovation. Effective information management can improve efficiency, reduce costs, and provide better services. In Information Governance, this translates, embedding good practice, and developing strong understanding of data protection means that the council can manage its data effectively – in terms of knowing what we hold, where we hold it and how we can use it.

4.2 Freedom of Information/Environmental Information Regulation Requests

The Freedom of Information Act (FOIA) and Environmental Information Regulations (EIR) are two pieces of similar legislation which enable the public access to information held by a public authority such as the council. They both aim to promote transparency and accountability in the public sector by allowing individuals to request and receive information about the operations and decision-making processes of the council. The council will respond to requests under EIR where the information requested is environmental such as land development, pollution levels and waste management. For requests around non-environmental matters then the council will respond under FOIA.

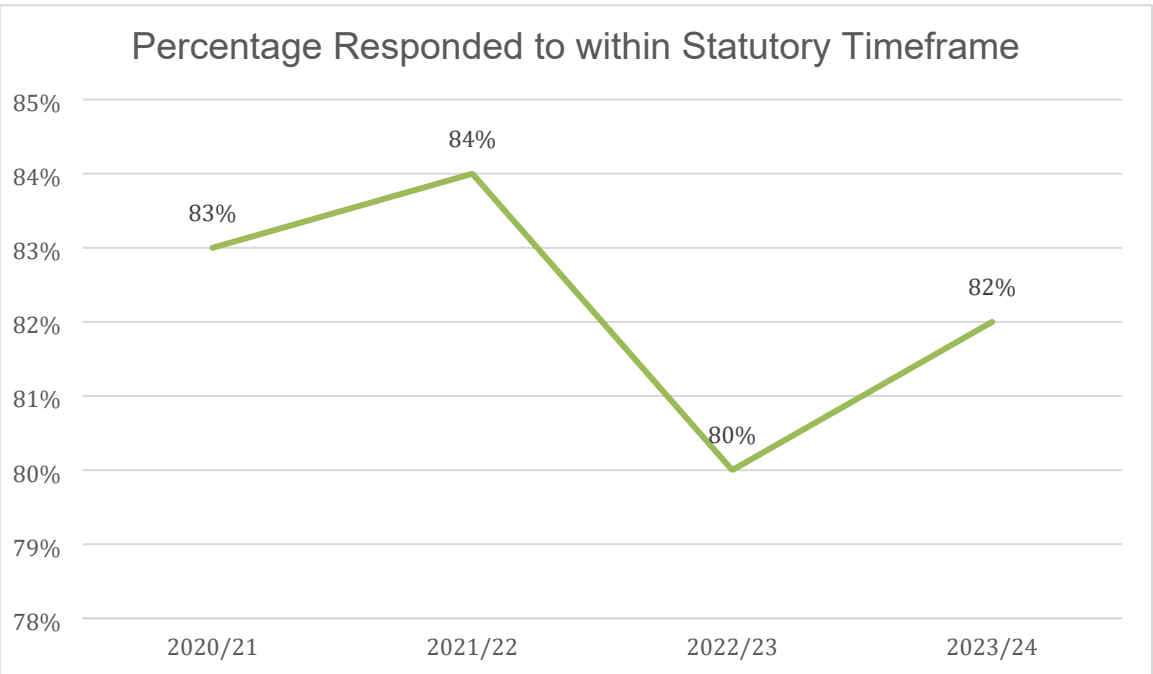
Both FOIA and EIR are applicant and motive blind meaning that the answer we give to one person can be given to any other person making a similar request. The presumption is that we will disclose unless an exemption (FOIA) or exception (EIR) applies. In some cases, an exemption/exception will be absolute such as when the information relates to a person but there will also be cases where we have to consider the public interest test for a qualified exemption/exception such as commercial sensitivity. The council is required to respond to requests within 20 working days, unless it needs to extend that timescale to consider the public interest test.

The council has a central team that manages the FOIA/EIR process from receipt to response. The ensures that the council has a robust approach to responding to these types of requests by officers with specialist knowledge. A new internally developed and maintained system was introduced last year and there were some initial teething issues that did affect performance initially, but the team was able to overcome these at the same time as the volume of requests sharply increased. The council has continued to receive increasing numbers of requests for information over a number of years.



There has been a distinct increase in the last year with monthly volumes routinely exceeding 110 per month, with a high of 173 received in January 2024 alone.

The below indicates the percentage of responses issued within the statutory timeframe. The Information Commissioner (ICO), as the regulator, has always indicated an expectation of 90% issued within time. The increase in volume has inevitably had an impact on both the Information Governance service and on our colleagues around the council which we will seek to address in the coming year.



Amongst the requests received, we received requests about the below:

- Potholes
- Roadworks
- Swimming pool
- School fencing
- Budgets across the council
- Elections

- Littering/fly tipping
- Cyber security
- Information governance
- Unregulated places
- Special Educational Needs
- Planning matters
- Artificial Intelligence
- Procurement and contracts
- Council tax and business rates

If someone disagrees with the response, then they may request that we undertake an “internal review” and then if they continue to disagree then they may complain to the ICO. The number of internal reviews requested over the period 2020/21 to 2023/24 is 21 or 0.45% of the total responses issued. We had only 3 matters involving the ICO in the same period and none since 2021/22.

The challenge in the coming year is to develop greater use of the available information to reduce the burden of requests on the council by:

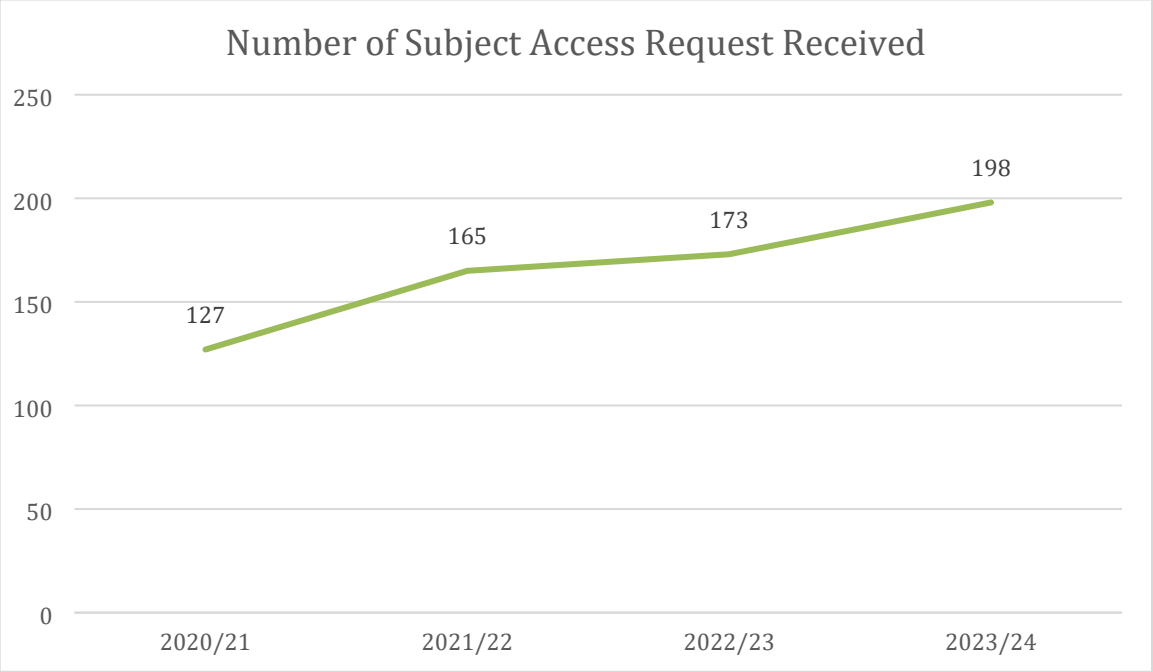
- Increased use of reporting tools to identify repeated themes and develop pre-published data schemes
- Making better use of published data such as the contracts register and monthly spend of over £500
- Increasing visibility of FOI responses through the disclosure log
- Increasing use of AI on both the website and FOI app to encourage self service by customers and by the Information Governance team

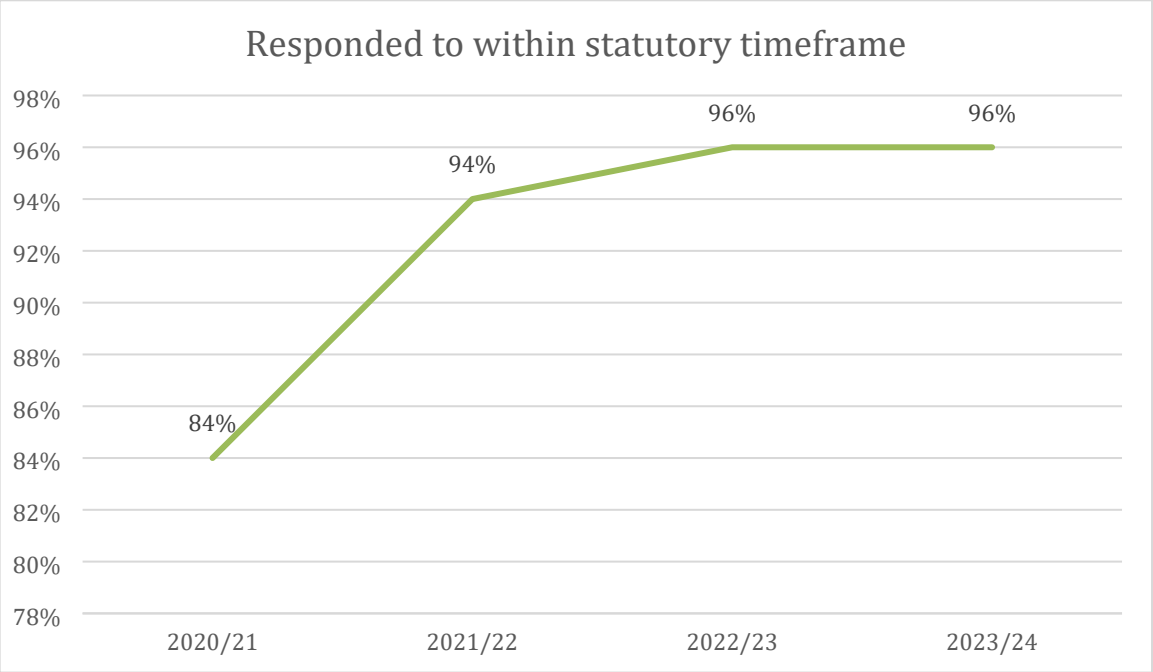
4.2 Data Subject Rights

Under data protection legislation, individuals have specific rights around their personal information which include the rights of access, erasure and rectification. The IG service is a central service which manages rights requests for the council as this ensures consistent application of legislation with specialist advice and guidance.

The most common request is that of access to information with the majority relating to children’s social care. The right of access gives a person the right to their own information but not automatically to the information of others such as parents or siblings. A subject access request can often be very large and complex with an IG officer needing to review files and undertake redaction where appropriate. Individuals who were in care for much of their childhood will have had huge amounts of sensitive information recorded about them and their family. This means the review of files to ensure that only the appropriate information is disclosed requires high levels of concentration and attention to detail. Requests must be responded to within a calendar month unless they are deemed complex, and the Council can then extend by a further two calendar months.

The number of subject access requests received has continued to rise over the last four years. It should be noted that not all requests received progress to a response being issued. This is because sometimes individuals do not respond to requests for proof of identity or clarification on what information they are seeking. The tables below provide information on the number received, responded to and number within the appropriate timescale.





Given the intensive nature of the work, and the fact that one officer undertakes the vast majority of the work, then to achieve these high levels of performance is an exceptional achievement.

In 2023/24, the council received an additional four requests from individuals to exercise their rights in relation to their personal data. One related to the right to erasure which the council could not comply with as it would have required the deletion of a council tax account. Three related to the right to rectification; we corrected the data held in relation to a waste management issue and in two social care matters, we updated the information held to reflect the person's views.

4.3 Personal Data Breaches

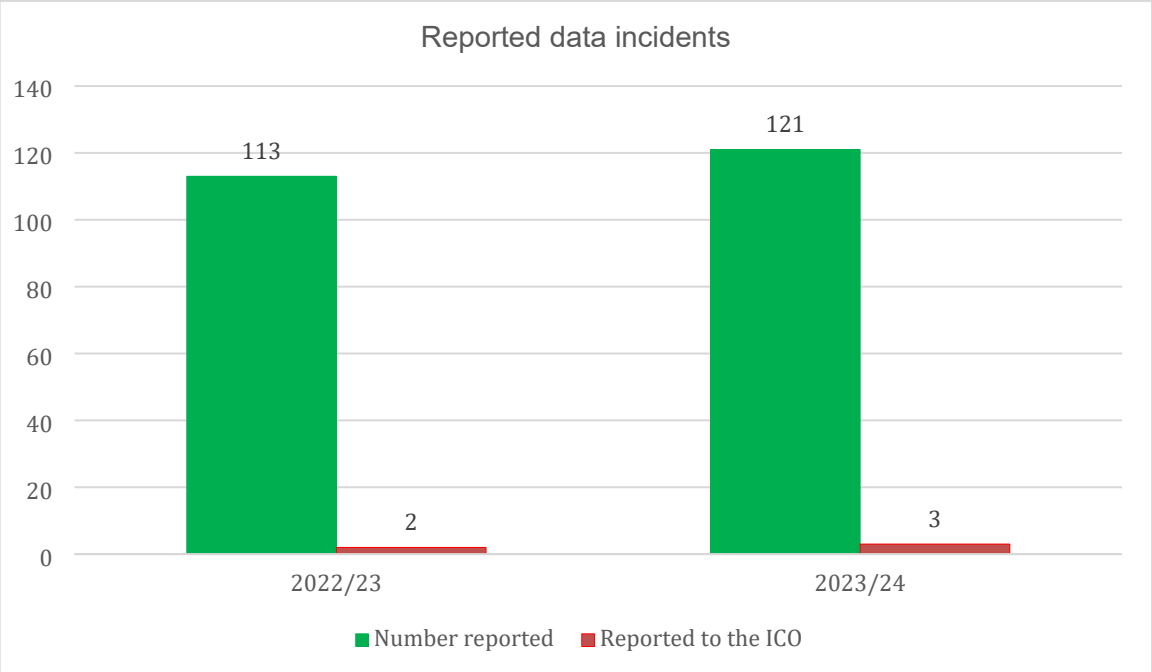
A personal data has a very clear definition within the legislation:

A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

This means that it is not just deliberate actions or losing information but also those caused by human error and incorrect disclosures. When an alleged or actual breach is reported then we must assess what kind of risk or detriment it may cause to the person whose data it is. The UK GDPR advises that this risk or detriment means that if we are not able to address a breach in an appropriately and timely manner then it could cause some damage to a person such as a loss of control over their personal information, identify theft, financial loss, damage to reputation or a loss of confidentiality. This means that we need to understand from the service concerned what type of information has been breached, how, what impact it could have on someone and if we have been able to contain or mitigate the breach. We are required to report any breach where there is such a risk to the ICO and if there is a high risk to the person then we must inform them of the breach.

Our approach has always been to repair and remedy the breach – i.e. fix what has happened and ensure we do not see a recurrence. This may mean we inform the person affected even if there is not a high risk because this shows a greater level of transparency in how we handle personal information.

The below shows the number of breaches reported across the council in the last two financial years. The levels have remained very similar and shows that the majority of reported matters can be mitigated or contained without a risk to the person concerned. The volumes should also be seen in the context for instance of how many emails and letters a council will issue a year and the number of issues caused. The level of breaches which need to be reported to the ICO is low in comparison which demonstrates that the council is able to mitigate to avoid any damage to a person.

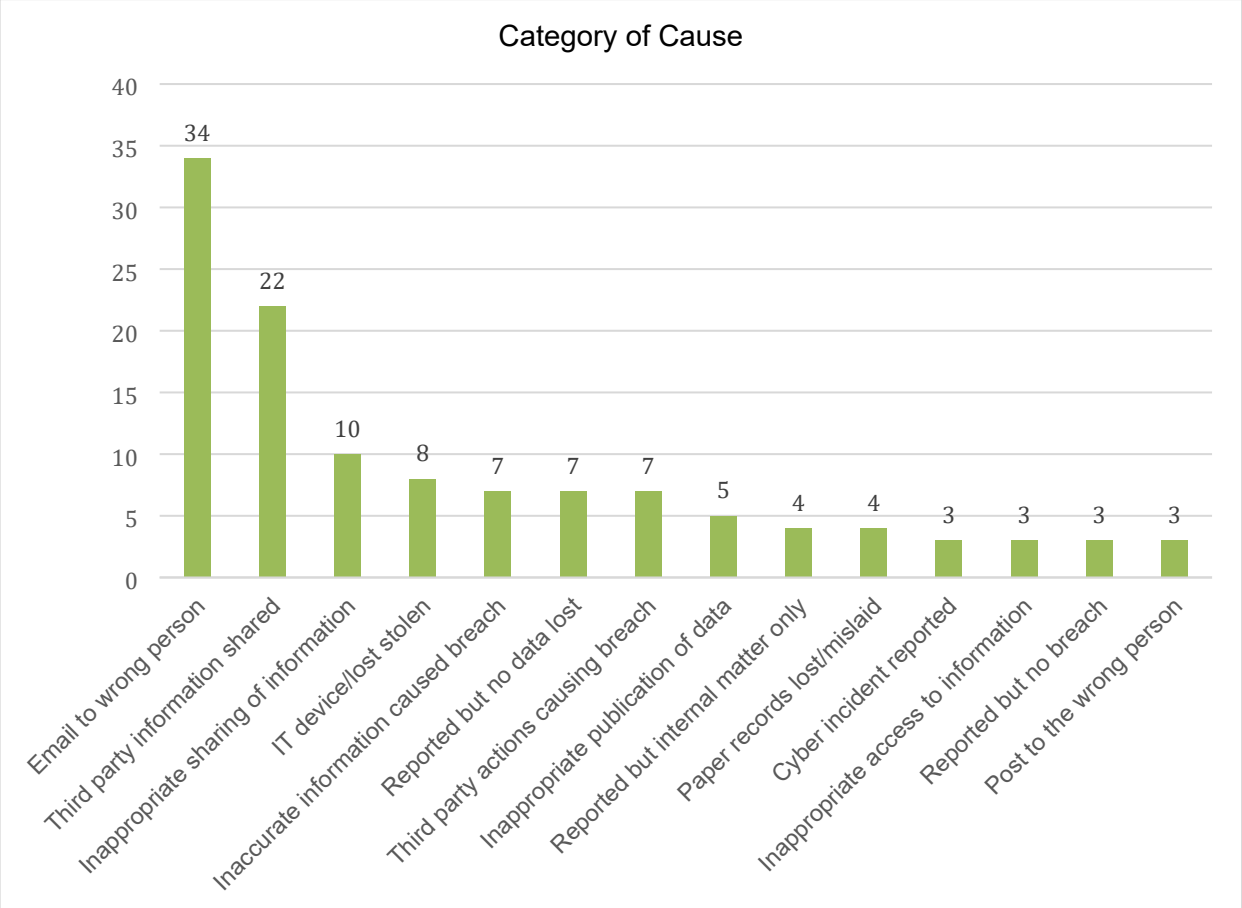


The three matters reported to the ICO last year were as follows:

Description of incident	Actions taken to address	Outcome from ICO
Incorrect address held onto a social care assessment led to the assessment being posted to the wrong address	Council officer visited the address and the individual confirmed that they had returned the assessment to the council. This was confirmed. The affected person was informed and was satisfied	No further action taken however recommendations provided around training

	with how we had contained and dealt with the matter.	
Email address mistyped when entered and caused email to be sent to incorrect email address	Council officer missed a single letter from the email address and caused an education report to be issued to the wrong recipient. Attempts to ask the incorrect recipient to delete were made but no response received. The situation and impact were then monitored. The family were informed and were kept updated on	No further action taken however recommendations given around checking email addresses and use of passwords where necessary
Address not updated correctly which causes a social care assessment to be delivered to the next door property	The letter had been delivered 5 months earlier and it was not clear why it was not handed to the correct property. The matter was reviewed and the error identified but it remained unclear as to whether the assessment had been read.	No further action taken however recommendations provided around updating address and sharing documents by email if possible.

The following below shows the cause of all incidents reported in the last financial year. From this, it can be seen that the Council have recorded those caused by a contracted provider for instance and those where no data has actually been lost. It can also be seen that the overriding cause is human error through emails to the wrong person and sharing information with a third party in error or providing information to another party when it may not have been appropriate to.



The following table provides information on the above and explains the types of category:

Email to the wrong person	An officer has emailed information to the wrong email address
Third party information shared	Information about one person has been shared with the wrong person
Inappropriate sharing of information	Information has been shared with a person which, upon review, may not have been appropriate to share
IT Device/Lost Stolen	All council devices are encrypted and have device management software. Personal devices used to access council information e.g. phone to access email must have device management software installed
Inaccurate information caused breach	Out of date or mistyped information leading to a breach
Reported but no data lost	A matter may be reported however upon review no data has been lost
Third party actions causing breach	A contracted provider or partner caused the breach
Inappropriate publication of data	Information has been published on the website when it should not have been
Reported but internal matter only	An incident where the information has been shared incorrectly with another council officer but has not left the organisation
Paper records lost/mislaid	Records may have been mislaid and found or lost
Cyber incident reported	A cyber incident such as a phishing attack has been reported
Inappropriate access to information	Access to information on a system should not have been granted or has not been restricted
Reported but no breach	Reported but no actual breach occurred
Post to the wrong person	Post is sent to the wrong person

This kind of understanding helps to understand where a weakness in a process or system may exist for instance and help inform how we can address these going forward. It also helps to develop training or communications for staff because we can make it relevant to a role or a team and help it be understood that a personal data breach has an impact on a person, and it is that person we should be focussing on. It is proposed to bring a six monthly report to Audit Committee on personal data breaches reported, consequences, lessons learned and improvements made to demonstrate the council's commitment to protecting the personal data of our residents.

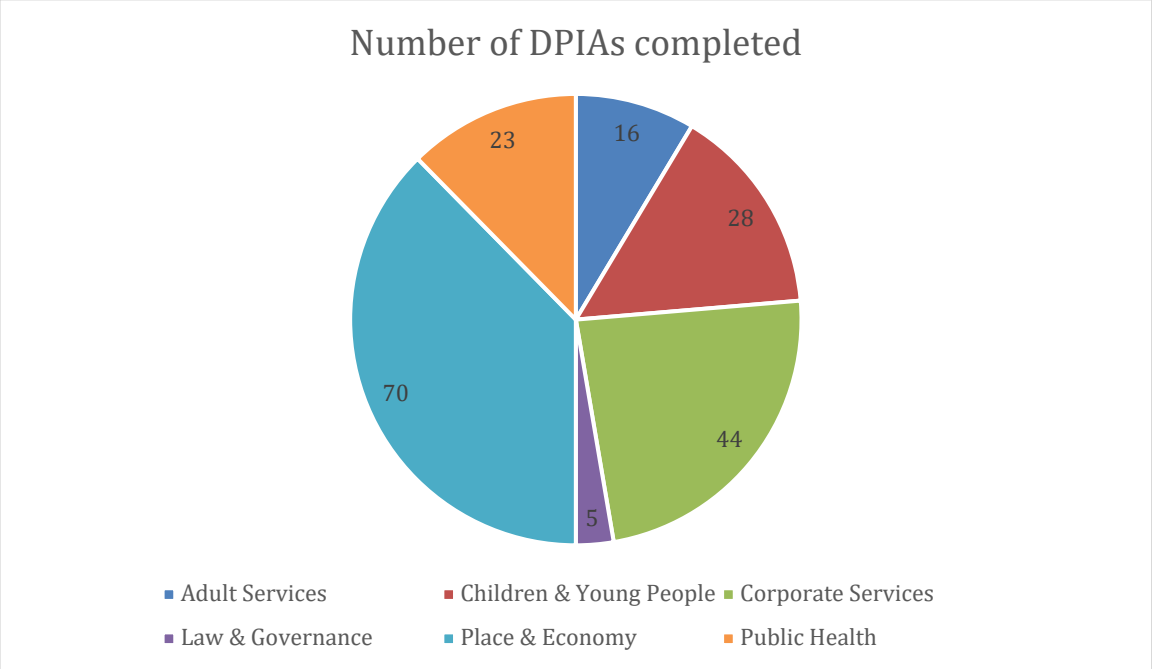
4.4 Data Protection Impact Assessments

The IG service can support and guide colleagues through compliance with legislation but sometimes IG is seen as something that prevents projects from progressing and is bureaucratic. However, our approach is to have a positive impact on projects, new systems and procurements through identifying ways to make a positive impact for services and their customers.

This may be through by suggesting ways to explain to service users what the council is doing or who we are working with and why in a privacy notice. It may be by supporting sharing between the council and partners with sharing agreements that enable better and more joined up working. We can advise on retention of information and ensure that the council's retention schedule and information asset registers can be updated.

The way in which we can understand a project and ensure that the above is incorporated is through data protection impact assessments (DPIA) which are in effect risk assessments of a project or new system.

Under the UK GDPR, the council is always required consider an assessment of the impact on privacy when personal information is being used and mandatory to complete one in cases where large amounts of sensitive information are being used for example. We see these a key way to understand a project, to see where there may be risks involving personal data but most importantly to see where we can assist. Since the start of 2023, we have completed over 180 screening and full impact assessments. The below shows the range across the council in the last 18 months.



These have covered key council initiatives or procurements such as

- The use of artificial intelligence in social care
- New education systems
- Housing Support Grants
- Apps to support public health initiatives
- Planning IT systems
- Complaints database
- Car parking such as Automatic Number Plate Recognition
- Overt enforcement cameras
- Customer facing systems for issue reporting
- Blue Badges
- Homelessness system
- Violence at work registers
- Single Person Council Tax Reviews
- Shared Health and Social Care Record

The outcome of these assessments can be updates needed to privacy or information notices shared with service users, the need for a contract or sharing agreements or informing a procurement to focus on key aspects such as data security.

The key takeaway we want services to have is a better project because it is compliant and secure, but also delivers value for service users. The key outcome for the council is to have a better understanding of what data it collects, uses, shares and receives because it is that data which will help inform council decision making and make for better, more efficient services.

4.5 Training

Training is a key way of raising awareness and embedding good practice within the council. It is also a way of officers taking the time to remind themselves of why data protection is important.

Officers are required to undertake mandatory learning on an annual basis, and we also offer bespoke training and attendance at team meetings to help services with their specific issues. In the last year, mandatory data protection training was completed by 98% of staff. We also offer data protection and FOIA/EIR training to all Members on an annual basis.

We would also note that 99% of staff completed the mandatory cyber security training. This training is critical to the safety of the organisation and individuals. The council spends a lot of money and resource on protecting itself, and most attacks are blocked without anyone noticing.

- In the last 12 months the council's IT service have automatically blocked 17.5m emails, 56% of these were blocked as they came from an address that has a poor reputation and is likely to be a bad actor.
- Of the emails that got through they then blocked another 809,799 of which 69,494 were phishing emails, 54 ransomware emails, 26,832 Business Email Compromise - which aim to impersonate senior officers and Members within the Council
- The next stage of the process is manual within IT where they may have to take action on a further 4,000+ email per month

Attackers are constantly changing their tactics and occasionally phishing emails get through and as a council we rely on staff to be able to recognise these attacks and report them. Unfortunately, we are often attacked via an email address that is known to us, another council or a supplier that we trust that itself has been compromised. Since training has been made mandatory, we have seen a decrease in the number of users clicking on bad links but in the last week a user clicked on a link and didn't notify IT. This emphasises that training and the reapplication of training is essential.

4.6 Oversight and governance

The Information Board, previously shared with Cambridgeshire County Council, will be relaunched this year and chaired the council's Senior Information Risk Owner, the Director of Law & Governance and Monitoring Officer. Its remit will continue to be the below and it will be responsible for shaping and enabling the delivery of information management strategies in line with the council's corporate priorities.

- Records retention and destruction management
- Information asset management
- Information published under Freedom of Information Act/ Environmental Information Regulation requests
- Publishing and management of open data
- Data Protection including the council's approach to subject rights, breaches, impact assessments
- Information and cyber security matters
- The use of the council's data within research/project use of council data
- Mandatory Data Protection, Information Governance and Security Training
- Audits of processes and controls
- Policies affecting the management and security of information.

This board will meet four times year and an annual report will be provided to this committee and the Council's corporate leadership team.

5. CORPORATE PRIORITIES

5.1 The use of information in developing how we work and how we could work is directly linked to the corporate priority of a Sustainable Future City Council. This is because having good information governance means that information becomes a valuable asset that we manage the council's data in a way that make it fit for purpose, enables it to be linked across and we can reuse it where possible to deliver more efficient and targeted services.

6. CONSULTATION

6.1 Director of Legal and Governance and Monitoring Officer
Service Director IT & Digital Services
Chief Internal Auditor

7. ANTICIPATED OUTCOMES OR IMPACT

7.1 The outcome of this report is to establish an annual reporting process in relation to Information Governance

8. REASON FOR THE RECOMMENDATION

8.1 There should be oversight and understanding of how the Council complies with its statutory duties around information governance as well as understanding its performance in line with established indicators.

It is also considered that better oversight of how the Council responds and prevents personal data breaches would aid continuous improvement and compliance.

9. ALTERNATIVE OPTIONS CONSIDERED

9.1 There is an option to not present a report which would not provide any oversight or to be provide a more limited report which may deliver less assurance on compliance.

10. IMPLICATIONS

Financial Implications

10.1 There are no financial implications from this report.

Legal Implications

10.2 It should be noted that personal data breaches can attract potentially serious legal and regulatory action such as audits, undertakings, fines and, in some cases criminal liability. A personal data breach can also lead to damages claims by those affected as well as reputational damage and loss of trust.

Equalities Implications

10.3 There are no equalities implications from this report.

11. BACKGROUND DOCUMENTS

Used to prepare this report, in accordance with the Local Government (Access to Information) Act 1985

11.1 UK General Data Protection Regulations and Data Protection Act 2018
Freedom of Information Act 2000
Environmental Information Regulations 2004

12. APPENDICES

12.1 There are none.