Information Governance
Annual Report

2024-25

Peter Knight
Head of Information Governance

June 2025

Contents

Background and Context

1. Information is a vital asset to any organisation, and a large and complex organisation like Suffolk County Council holds and manages a vast amount, much of it extremely sensitive in nature. It is therefore vital that appropriate structures, policies, guidance and processes are in place to ensure the Council is able to manage this information securely and effectively.

2. Information Governance describes the holistic approach to managing, using and sharing information, and includes coverage around access to information, data quality, information management, information security and information sharing, data privacy and information governance legislative compliance.

3. There is a considerable amount of legislation and regulation that either determines or influences how the Council manages the information it holds. Whilst some of this is service-specific, there are also requirements that impact the whole organisation, including relating to data protection and access to information. Of particular note are the following:

    - **Data Protection Act 2018 and UK General Data Protection Regulation (UK GDPR)** – the UK left the EU on 31 January 2020, and the General Data Protection Regulation (GDPR) was replaced by the UK GDPR. The UK GDPR retains the key principles, rights and obligations of the EU GDPR, and alongside the Data Protection Act 2018, forms the basis of data protection law in the UK. Data protection applies to personal information relating to living individuals, and the legislation governs how the Council uses this information.
    - **Freedom of Information Act (FOI) 2000** – this provides a general right of access to recorded information held by any public authority, including the Council. Anyone can make a request for information under the FOI legislation.
    - **Environmental Information Regulations (EIR) 2004 –** similar in scope to the FOI Act, this legislation covers rights of access to information specifically related to environmental matters.

4. The regulator for information in the UK is the Information Commissioner's Office (ICO), which is *"an independent body established to uphold information rights in the public interest, promoting openness by public bodies and data privacy for individuals".* Part of the ICO's role is thus to hold organisations to account for the way they manage their information. As an organisation that processes personal data, the Council is required to register with the ICO, and pay an annual fee. The Council's Data Protection Registration Number is Z5113825, and the current registration expires on 13 December 2025.

Leadership & Governance

5. Information governance in the Council is overseen by the Corporate Information Governance Board (CIGB), which provides oversight and direction on information governance matters to provide assurance in the areas of information governance, information security and information rights. The Board meets quarterly and includes representatives from each directorate, as well as officers with a specific responsibility for information governance matters (see below). Any significant issues of concern are escalated to the Council's Corporate Leadership Team by exception as required. The Lead Cabinet Member for Information Governance is the Leader of the Council.

6. The CIGB is supported by service-specific information governance boards within the Children & Young People's Services (CYP) and Adult Social Care (ASC) directorates, as they are the directorates that process large quantities of sensitive personal data; other directorates have information governance leads who are members of the CIGB. The Council also has a network of Strategic Information Agents (SIAs) across the organisation who promote and encourage information governance best practice within their service areas.

7. The Council is also represented on relevant partnership bodies and groups, including:
   - the Suffolk Office of Data & Analytics (SODA), a joint initiative across the public sector organisations to make better use of public sector data and intelligence;
   - the Health & Care Information Governance Steering Group (IGSG), which oversees health and care information governance matters; and
   - the Suffolk Information Governance Group (SIGG), which includes representatives from all Suffolk local authorities and exchanges knowledge and intelligence in information governance matters.

8. There are a number of key roles within the Council which have specific information governance responsibilities, and these include:

Senior Information Risk Owner

9. The Senior Information Risk Owner (SIRO) has overall strategic responsibility and accountability for information risk across the organisation. A key responsibility for the SIRO is to provide the Corporate Leadership Team with assurance that information risk is being managed appropriately and effectively across the organisation. In Suffolk County Council, the SIRO role is designated to the Deputy Chief Executive post, and the SIRO is a member of the Corporate Information Governance Board.

Caldicott Guardians

10. Caldicott Guardians are senior officers responsible for protecting the confidentiality of people's health and care information, making sure it is used properly, and enabling appropriate information-sharing with other health and care organisations. The Caldicott Guardian role is mandatory for all health and care bodies, and all Caldicott Guardians are listed on the national Caldicott Guardian Register. There are two Caldicott Guardians in Suffolk County Council – one covering Adult Social Care (ASC), and one for Children & Young People's Services (CYP) – and they are members of their respective directorate-level Information Governance Boards.

Head of Information Governance

11. The Head of Information Governance leads the team of 13 information governance professionals that develops the overall information governance policy and assurance framework, provides advice, guidance and training for staff, and monitors information compliance. The Information Governance Team also has specific responsibilities for a number of areas including data protection, information requests, and records management. The Head of Information Governance reports to the Assistant Director for Govenance, Legal & Assurance, and acts as the Chair of the Corporate Information Governance Board on behalf of the SIRO.

Data Protection Officer

12. As a public body, there is a duty on the Council under the UK General Data Protection Regulation (GDPR) to appoint a Data Protection Officer (DPO). The DPO role has specific defined responsibilities relating to the monitoring of data protection compliance, advising the organisation on its data protection obligations, and acting as a contact point for data subjects and the ICO. The DPO role in the Council is undertaken by the Data Protection Officer & Compliance Manager, who is supported by the Data Protection & Training Manager, both of whom report to the Head of Information Governance. The Data Protection Officer & Compliance Manager also acts as the Data Ethics Advisor for the Council.

IT Security Manager

13. The IT Security Manager has responsibility for ensuring the Council's IT network and systems are secure and that IT security policies are adhered to. The IT Security Manager works closely with the Information Governance Team, including on matters relating to cyber-security and IT-related security incidents. The IT Security Manager is also a member of the Corporate Information Governance Board.

Assurance and Accreditation

14. The Council is subject to a number of external information and Information Technology (IT) assurance and compliance regimes, including mandatory accreditations to facilitate access to various information networks and systems. The following are of particular note, and the Council is compliant with each of these requirements.

Data Security & Protection Toolkit

15. The Data Security and Protection Toolkit (DSPT) is an online self-assessment tool that enables organisations to measure their performance against the National Data Guardian's 10 data security standards. All organisations that have access to health and social care data (which includes the Council), are required to submit an annual DSPT submission, and successful completion demonstrates compliance with the expected data security standards for holding, processing or sharing personal health and care data. This area of activity is of increasing importance as the health and care integration, and the associated sharing of data across organisations, becomes ever more prevalent.

Public Services Network Compliance

16. The Public Services Network (PSN) is the UK government's communications network that allows public sector organisations and their partners to connect and communicate, reduce duplication and share resources. Organisations connecting to PSN have to demonstrate that they have a suitable level of security to minimise the risk to other PSN users. In order to report and demonstrate the level of security a PSN compliance certificate is required, and to achieve compliance an annual application process has to be undertaken involving an external annual IT health check and external audit.

Payment Card Industry Data Security Standard

17. The Payment Card Industry Data Security Standard (PCI DSS) is an information security standard developed to enhance cardholder data security for all organisations that accept, store, process or transmit credit card data, which includes the Council.

There are a number of prescribed requirements that have to be fulfilled for compliance purposes.

Internal Audit

18. In addition to the external assurance mechanisms outlined above, there is a strong relationship between the Council's Information Governance Team and the Internal Audit Team. The Head of Internal Audit is a member of the Corporate Information Governance Board, and membership of the Board enables the Head of Internal Audit to have oversight of information governance matters, as well as any breaches of confidentiality or security.

19. Audits of information governance related matters are undertaken as and when required, as identified by the Head of Internal Audit in consultation with the Head of Information Governance. There were no audits of information governance related matters undertaken in 2024/25.

Information Risk Management

20. Where there are significant information risks identified in the organisation, these are recorded on the Council's Corporate Risk Register, and are actively managed in line with the Council's overall Active Risk Management (ARM) approach. Each risk specifies the nature of the risk and the possible implications, and includes a summary of the mitigating actions that are undertaken in order to reduce the likelihood of the risk occurring. There are currently two information-related risks on the Corporate Risk Register, namely:

    a. The growth in the number of **information security incidents** occurring throughout the Council could lead to the greater loss of sensitive information and a corresponding rise in data breaches involving sensitive personal information, resulting in harm to citizens, damage to the Council's reputation, and the imposition of sanctions from the Information Commissioner's Office (ICO).

    b. There is a risk the Council could be subject to a major **cyber security attack** or information breach resulting in financial loss, significant disruption to services, and reputational damage. To function effectively, the Council relies on robust digital technologies and online capabilities to deliver front line services to residents. The constant threat of viruses, hacking, unauthorised access to information is real and have the potential to disrupt networks, web resources, and public services. Public confidence could be affected if the organisation was not able to adequately protect its systems.

21. A summary of the risks, including risk ratings and mitigating actions, is provided in Annex 1.

Information Governance Policy Framework

22. Ensuring the Council's information governance policies are kept up to date and relevant is a critical element in ensuring the Council is compliant with all relevant legislation and changes in the national policy landscape.

23. The Council has a comprehensive suite of information and IT security policies, all of which are published on the Council's website, and all policies are reviewed every two years as a minimum. A review of all policies will be undertaken during 2025-26, with any significant revisions approved by the Corporate Information Governance Board for approval.

24. The current suite of information governance policies is as follows:
    - Acceptable Use of Information Systems Policy
    - Appropriate Policy Document for Special Category and Law Enforcement Data
    - Data Protection Policy
    - Freedom of Information (FOI) Policy
    - Information Classification and Labelling Policy
    - Information Security Policy
    - Information Security Incident Management Policy
    - IT Network Security Policy
    - Password and Authentication Management Policy
    - Records Management Policy
    - Role Based Access Control Policy
    - Software Policy
    - Surveillance Camera Policy
    - Use of Cloud Services Security Policy
    - Social Media Policy

25. As the Council increasingly looks to embrace the opportunities presented by Artificial Intelligence (AI) and other digital technologies, an AI Policy is currently in development; this will set out the Council's approach to the responsible, lawful and ethical adoption and use of AI across its services and operations.

26. The policy suite is supported by other documentation and associated guidance where required, all of which is made available to all Council staff via the Council's intranet (IRIS).

Data Protection Compliance Tools

27. In addition to the suite of policies, there are a number of internal compliance tools that help to ensure that the Council remains compliant with its data protection responsibilities, in particular:

Privacy Notices

28. The Council has an overall corporate Privacy Notice which sets out how the Council collects and uses personal data to provide and manage services. This is published on the Council's website, alongside a number of directorate- or service-specific Privacy Notices which provide more detail about the specific information collected and used by individual service areas. Privacy Notices are updated as and when required, although a formal review of all Privacy Notices takes place annually.
    https://www.suffolk.gov.uk/about/privacy-notice/

Registers of Datasets

29. A dataset register helps an organisation to keep track of the information it holds. For an organisation as large and complex as the Council, this is especially important. Previously, this information was maintained in a single register, but to aid monitoring and review, there are separate registers for each of the Council's directorates. Information included in the Registers includes what the data is, why it is collected, who the owner of the data is, how it is used, and how long it is retained for. Registers are updated by the relevant service(s) as and when required, with a more comprehensive review undertaken every two years.

Register of Data Protection Impact Assessments

30. Data Protection Impact Assessments (DPIAs) are the Council's primary way of undertaking information risk assessments for new services, information sharing agreements, projects or IT systems. This is especially important where sensitive data (whether this be personal or commercial) is involved. Completing a DPIA is a legal requirement for any data processing activity that is likely to result in a high risk to individuals. Using a standardised process and documentation ensures a consistent approach to assessing the information risks of any data processing developments, and all DPIAs have to be reviewed and approved by the Council's Data Protection Officer (DPO) before the relevant service or project can go live.

31. All DPIAs are recorded on a central Register for compliance purposes, and it is clear from the graph below that DPIAs are embedded extensively across the organisation, with 128 DPIAs completed and registered in 2023/24 and 478 completed over the last three years.

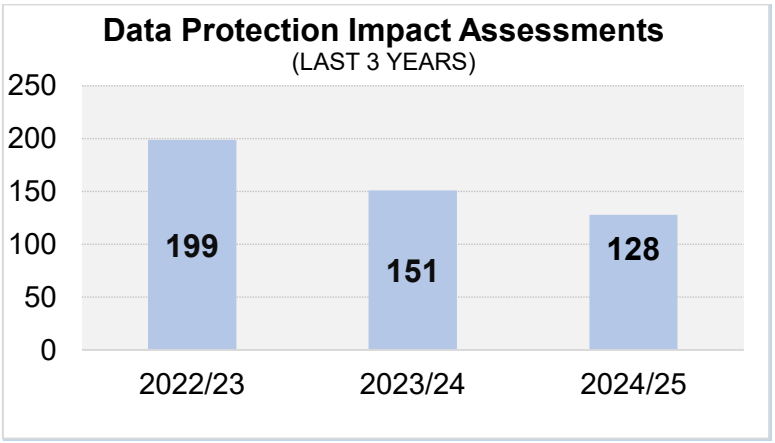

Figure 1 – Data Protection Impact Assessments registered 2022/23 to 2024/25

Register of Information Sharing Agreements

32. Organisations need to share information more than ever to ensure that citizens and service users receive the most effective service interventions. Information Sharing Agreements (ISAs) are a critical tool for ensuring that information is shared appropriately and safely, and in line with the Council's data protection policies.

33. The Council has adopted a standard ISA template to ensure a consistent approach is taken in developing any sharing agreements. A central register of ISAs involving the Council's data is maintained to ensure that the Council has a record of what information is shared with other organisations, and for what purpose.

Data Ethics

34. In 2021, the Council published an Ethical Data Stewardship Charter to demonstrate the Council's commitment to a set of principles which governs the use of data, and outlines the processes to be followed for ethical risk assessment and decision-making. The eight principles of the Charter are:
    a. Accountability
    b. Scrutiny
    c. Transparency
    d. Participation
    e. Design
    f. Oversight
    g. Fairness
    h. Benefit

35. The full Charter is available on the Council's website Ethical-Data-Stewardship-Charter.pdf (suffolk.gov.uk)

36. In 2023/24, the Council established its Data Ethics Advisory Panel, under the auspices of the Audit Committee, to provide advice to the organisation on data ethics so it can uphold the principles of the Ethical Data Stewardship Charter, and help to maintain public trust. The Advisory Panel is convened as and when referrals are required.

Performance Reporting

37. Performance reporting is an important part of helping to ensure that the Council is monitoring the effectiveness of its information governance arrangements, and its compliance with legislation.

38. There are a number of key performance indicators (KPIs) that are measured and regularly reported to internal groups such as the Corporate Leadership Team (as part of the overall Corporate Performance Report) and the Corporate Information Governance Board.

39. A summary of the KPIs that are included in the Corporate Performance Report, and comparative performance for these for the last three years is shown below:

Key Performance Indicator	2022/23	2023/24	2024/25
Number of Security Incidents reported (all incidents)	588	670	724
Number of Personal Data Breaches reported	333	324	338
Number of data breach notifications to the ICO	8	4	5
Number of Subject Access Requests (SARs) received	233	323	382
% of SARs responded to within statutory timescales	44%	77%	91%
Number of Information Requests (FOI/EIR) received	1258	1384	1356
% of FOI/EIR Requests responded to within statutory timescales	93.0%	97.0%	99.3%

Figure 2 – Corporate Information Governance KPIs 2022/23 to 2024/25

40. Directorate-level Information Governance Boards and/or Leadership Teams also consider specific performance measures relevant to their service areas.

41. The Corporate Information Governance Board also receives more detailed performance reports on specific matters on a cyclical basis – for example, a six-monthly monitoring report of security incidents and personal data breaches, and an annual FOI/EIR requests monitoring report.

42. There is a lack of benchmarking information available regarding information governance matters. The Council is not required to submit any annual returns to the Information Commissioner's Office (ICO) or any other body, and there is therefore no published data that can help the Council assess how it compares to other similar authorities. The ICO has stated its intention to publish statistical information at some point, but there are no timescales associated with this at the current time.

Training and Awareness-Raising

43. It is critical that all Council staff understand the importance of dealing with the Council's information appropriately, safely and securely. Getting it right means the personal information the Council holds about customers and citizens, and the Council's own information, is protected.

44. The ICO requires all staff to undertake mandatory data protection training at least every two years. Since this requirement has been in place, the County Council has developed and used its own bespoke e-learning training, which is tailored to the specific needs and context of the organisation, rather than procuring a generic, 'off the shelf' package that many organisations rely on. This has the advantage of ensuring that the content is directly relevant to Council staff and can also be adapted to changing circumstances whenever the training is updated. All staff in Suffolk County Council undertake this mandatory training every year, and the latest iteration ('Our Information, Our Responsibilities') was launched in April 2025.

45. Information governance training is also provided through bespoke sessions to individual services and teams, prioritising those teams where there is an identified need or where there are concerns about information management understanding or practice. Furthermore, specific training is required for staff in some services where access to sensitive personal data is required for case management systems – for example, all users of the LiquidLogic social care IT system are required to undertake additional training which includes data protection and information security elements.

46. In addition to formal training, awareness-raising is also a valuable way of keeping staff appraised of information governance matters. There are various mechanisms available to facilitate this, including: publishing information governance advice and guidance on the Council's intranet (IRIS), which is updated and expanded regularly; delivering sessions to relevant fora (such as webinars for webinars for managers and senior leaders in the organisation); and publishing relevant articles in the weekly staff newsletter (InsideSCC).

47. Information governance training, covering data protection, records management and Freedom of Information, is also provided to all County Councillors by the Information Governance Team following an election. All 75 County Councillors received this training

following the Council elections in May 2021 as part of their induction programme, and individual sessions for any new Councillors (e.g. following a by-election), are also provided as required.

Information Security Incidents and Personal Data Breaches

48. Confidentiality and security of information about service users and citizens is extremely important, and the Council has robust policies and processes in place to seek to minimise the risks associated with collecting, storing and managing vast amounts of information.

49. When an incident that affects the security of any information does occur, it has to be reported (via IT Self-Service) as soon as it discovered, in line with the Council's information security incident management process. All incidents are then investigated to ascertain the nature of the incident, and are categorised by type and severity of risk by the Information Governance Team using a 'decision and risk record', (which also influences the actions taken in response to the incident).

50. Some information security incidents result in a personal data breach, which occurs when "personal or 'special category' data is lost, damaged or destroyed, either accidentally or on purpose; and/or shared with, or accessed by, someone who is not entitled to access it, either accidentally or on purpose" (ICO definition).

51. The UK GDPR states that where a personal data breach incident is likely to result in risk of harm to the rights and freedoms of individuals, the Council must inform the ICO within 72 hours of becoming aware of the breach. This requires the use of the ICO's standard notification form. The Council also has a lawful duty to inform the individuals affected without undue delay if a breach is likely to result in high risk to their rights and freedoms.

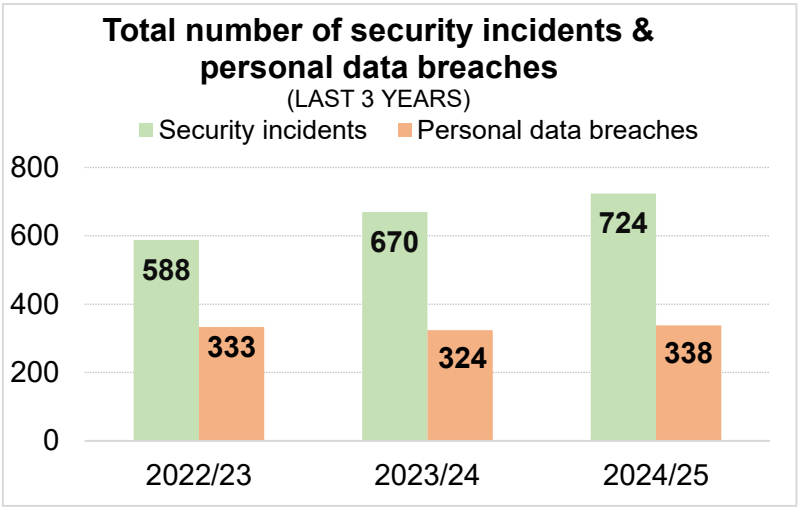

Figure 3 – Security Incidents and Personal Data Breaches 2022/23 to 2024/25

52. During 2024/25 there were 724 information security incidents reported via IT Self Service, which is an 8% increase on the previous year (670). Whilst this increase is of concern, it does however indicate that staff are aware of the need to report incidents when they do occur, and the process for doing so. Of the 724 information security incidents in 2024/25, 338 (46%) resulted in a personal data breach, which is a slight percentage reduction compared to the previous year (48%).

53. In terms of the nature of information security incidents, Figure 4 below shows a breakdown by type for all incidents, as well as for personal data breaches. The vast majority of these are the result of human error. In terms of all reported incidents, by far the most prevalent type is information being sent to the wrong recipient, either via email or in the post (312 incidents in 2024/25, which equates to 43% of the total). This category was also the most prevalent for personal data breaches (219 breaches), followed by unauthorised sharing of information (45 breaches).

Type of incident	2023/24		2024/25	
	All incidents	Personal Data Breaches	All incidents	Personal Data Breaches
Information sent to wrong recipient (email/post)	263	200	312	219
Unauthorised sharing	77	59	74	45
Data mishandling	42	12	58	17
Incorrect information recorded	81	9	84	13
Unauthorised access (internal)	21	9	25	12
Third party incident (SCC data)	19	6	20	11
Insecure transfer of information	11	2	30	6
Lost paperwork	14	12	11	5
Unauthorised access (external)	2	0	7	4
Unredacted information	11	7	4	3
Verbal disclosure	15	5	7	2
Malware/virus	6	0	11	1
Lost encrypted devices	63	0	46	0
Fraudulent emails/phishing	36	0	25	0
Non-personal information	3	0	6	0
Building security	4	1	2	0
Theft of information/device	1	1	2	0

Figure 4 – Security Incidents by Type 2023/24 to 2024/25

54. As can be seen from Figures 5 and 6 below, the majority of information security incidents occur within Children & Young People's Services (CYP), both in terms of all incidents (53%) and personal data breaches (58%). Adult Social Care (ASC) recorded the second highest level of security incidents (26%) and personal data breaches (25%). The service areas in Corporate Services in which the most incidents and breaches occurred in 2024/25 were Legal (14 incidents of which 9 were personal data breaches), and Coroners/Registrars (10 incidents of which 4 were personal data breaches).

Directorate	2023/24	2024/25
	All incidents	All incidents
Children & Young People's Services (CYP)	335 (50%)	381 (53%)
Adult Social Care (ASC)	197 (29%)	190 (26%)
Corporate Services (CS)	81 (12%)	64 (8%)
Growth, Highways & Infrastructure (GHI)	17 (3%)	25 (3%)
Fire & Public Safety (FPS)	6 (1%)	14 (2%)
Public Health (PH)	11 (2%)	18 (2%)
Third Party (TP)	23 (4%)	32 (4%)
Total	**670**	**724**

Figure 5 – Information Security Incidents by Directorate 2023/24 to 2024/25

Directorate	2023/24	2024/25
	Personal Data Breaches	Personal Data Breaches
Children & Young People's Services (CYP)	190 (59%)	197 (58%)
Adult Social Care (ASC)	76 (24%)	86 (25%)
Corporate Services (CS)	37 (12%)	29 (9%)
Growth, Highways & Infrastructure (GHI)	4 (1%)	5 (1.5%)
Fire & Public Safety (FPS)	0 (0%)	5 (1.5%)
Public Health (PH)	3 (1%)	2 (1%)
Third Party (TP)	14 (5%)	14 (4%)
Total	**324**	**338**

Figure 6 – Personal Data Breaches by Directorate 2023/24 to 2024/25

55. Five personal data breaches met the threshold for notification to the Information Commissioner's Office (ICO) in 2024/25, compared to four in the previous year. All of the notifications resulted in 'no further action' by the ICO (resulting in no sanctions taken against the Council), although any recommendations that form part of the ICO's decision are implemented and monitored.

56. The Council continues to implement additional measures to seek to reduce the number of information security incidents and personal data breaches occurring. A summary of the key activities undertaken both at a corporate level and within the two directorates which experience the highest levels of incidents and breaches (Children & Young People's Services and Adult Social Care), is provided in Annex 2.

Individuals' Rights

57. UK Data Protection law provides a number of rights for individuals in relation to the personal data that an organisation holds about them, namely:

- The right to be informed
- The right of access
- The right to rectification
- The right to erasure
- The right to restrict processing
- The right to data portability
- The right to object
- Rights in relation to automated decision-making and profiling

58. The Council's Information Governance Team coordinates the process for dealing with individuals' rights requests, with the responsibility for actioning or responding to the requests sitting with the relevant service(s).

Subject Access Requests (SARs)

59. Under data protection legislation, the Council must give individuals the right of access to their personal information under the 'right of access'. An individual can submit a Subject Access Request (SAR) requiring the Council to provide them with a copy of any personal information which it holds about the individual. The right of access to records can also be exercised by an authorised representative on an individual's behalf (for example, a solicitor). The Council has one month to respond to a valid SAR, although

this can be extended by two months for requests where the records are deemed to be voluminous and/or complex.

60. Some requests include thousands of pages of records; in 2024/25, 37 SARs responded to comprised over 2,500 pages of records. All of these records (which can exist in multiple formats, such as hard copy documents or electronic records, and be located across different services), have to be identified, collated, and converted into a form that allows them to be processed; every piece of information has to be read and where necessary redacted, to ensure that only the appropriate information is released to the requester.

61. Increased awareness of the rights of individuals to access information about themselves has resulted in a significant increase in the number of SARs submitted to the Council in recent years. There has been a significant increase in SARs received in 2024/25 compared to the previous two years as shown below.

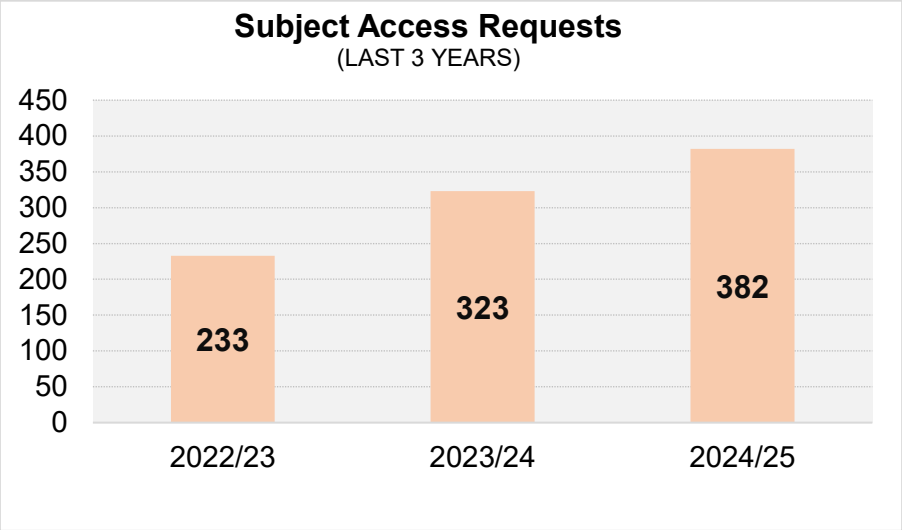

Figure 7 – Subject Access Requests (SARs) 2022/23 to 2024/25

62. The vast majority of SARs submitted to the Council relate to people wishing to see records relating to Children & Young People's Services, such as children's social care records, and records pertaining to children and young people with special educational needs and disabilities (SEND). Far fewer requests are received relating to other directorates, although there has been an increase in the number of ASC-related SARs in 2024/25.

	2023/24	2024/25
Directorate	**No.**	**No.**
Children & Young People's Services (CYP)	243	292
Adult Social Care (ASC)	33	39
Joint CYP/ACS	23	25
Growth, Highways & Infrastructure (GHI)	4	3
Corporate Services (CS)	18	16
Fire & Public Safety (FPS)	1	3
Public Health (PH)	1	0
Total	**323**	**382**

Figure 8 – SARS by Directorate 2023/24 and 2024/25

63. The high volume of SARs, combined with the fact that a significant number of these involve voluminous or complex records, has meant that achieving statutory compliance rates in recent years has proved a challenge. However, of the 382 SARs submitted to the Council in 2024/25, 91% were responded to within the statutory timescale, which is a welcome significant improvement in the Council's compliance rate compared to previous years.

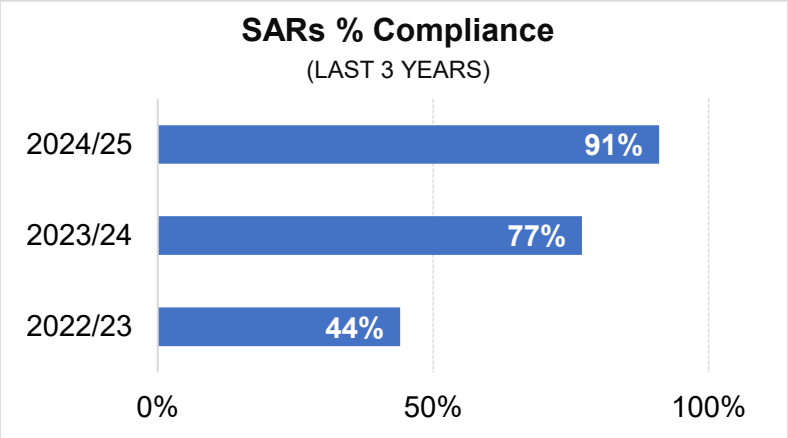

Figure 9 – Subject Access Requests (SARs) Compliance 2022/23 to 2024/25

Other Individuals' Rights requests

64. Since GDPR has been in force, the Council has received requests from individuals exercising rights (other than the right of access referred to above), relating to their personal data, notably 'the right to erasure' (also known as the 'right to be forgotten'), and 'the right to rectification' (of inaccurate or incomplete information). The Council has one month to respond to such requests, and these are actioned by services where it is appropriate to do so.

	No. of requests	
Type of request	**2023/24**	**2024/25**
Request for erasure	6	5
Request for rectification	6	9
Request to restrict processing	0	0
Other	0	0
Total	**12**	**14**

Figure 10 – Number of Individuals Rights Requests (non-SAR) 2023/24 to 2024/25

Information Requests (Freedom of Information and Environmental Information Regulations)

65. The Freedom of Information (FOI) Act 2000 provides a general right of access to recorded information held by any public authority. The Environmental Information Regulations (EIR) 2004 provide a similar right of access to environmental information held by public authorities. Requests received by the Council under FOI or EIR regimes have similar obligations and are handled in a similar way. Anyone can make a request, and the Council receives requests from a wide variety of sources, including individual citizens, organisations, media organisations, political organisations and legal bodies.

66. The process for handling FOI and EIR requests is co-ordinated by the Council's Information Governance Team, with relevant services providing the information for the

response to the request. The Information Governance Team also provides specialist advice, guidance and support to staff who are involved in responding to a request.

67. The number of FOI and EIR requests in the last three years is shown in the chart below. There has been a slight decrease in the number of FOI/EIR requests received in 2024/25 compared to the previous year. The 1,356 requests received in 2024/25 equates to approximately 113 requests received per month.

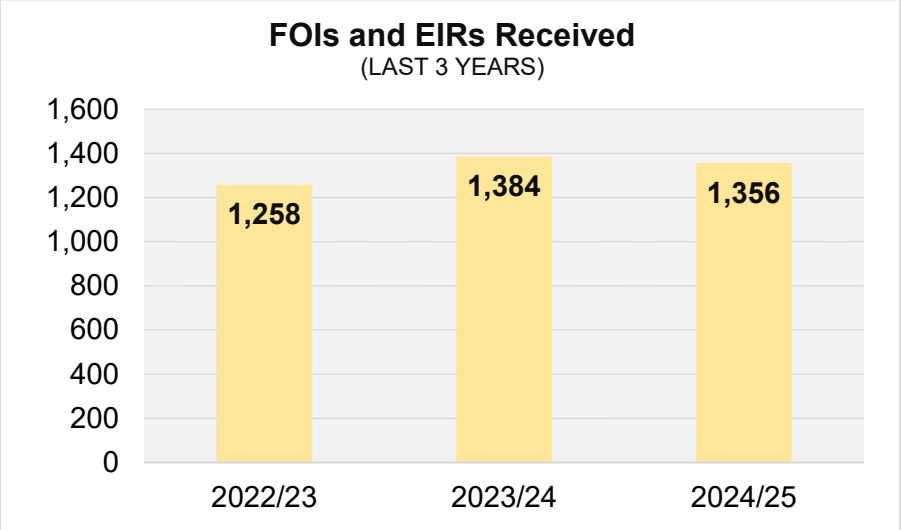

Figure 11 – Number of Information Requests (FOI/EIR) received 2022/23 to 2024/25

68. Under the legislation, the Council must respond to all FOI/EIR requests for information within 20 working days. Failure to comply with this deadline could lead to a complaint by a specific requestor to the Information Commissioners Office (ICO). The ICO has the power to serve a Decision Notice on a public authority for failing to comply with the 20-working day deadline.

69. The ICO's expected minimum level of compliance with responding to FOI and EIR requests is 90%. As the table below shows, the Council has exceeded this target in each of the last three years, and there has been a further improvement in the compliance rate in 2024/25 to 99.3%.

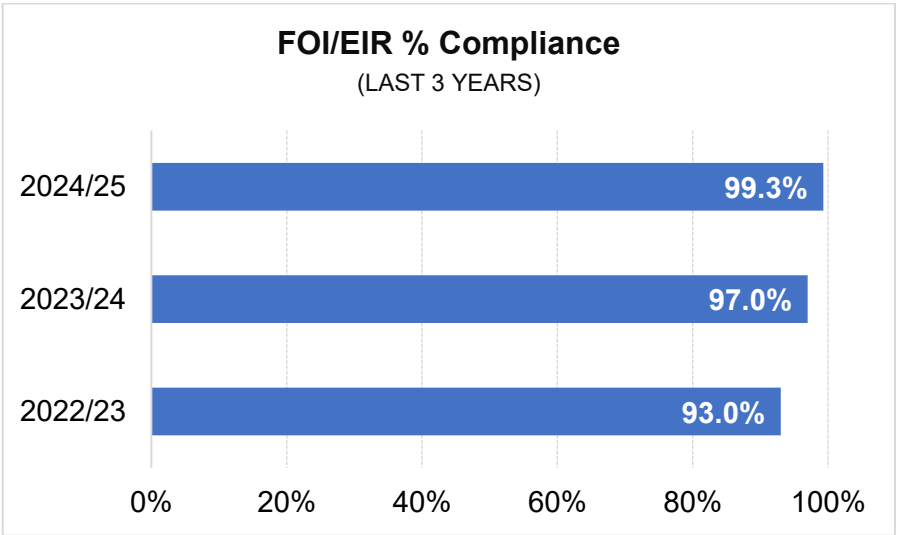

Figure 12 – Information Requests (FOI/EIR) compliance 2022/23 to 2024/25

70. Requests are received relating to a wide variety of issues or services, as the chart below illustrates. The most requests received in 2023/24 related to Growth, Highways & Infrastructure (GHI), Corporate Services (CS), and Children & Young People's Services (CYP). Far fewer requests are received for Fire & Public Safety (F&PS), Adult Social Care (ASC) and Public Health (PH). The service areas within the Corporate Services Directorate which receive the most requests are Finance, HR, Property and IT.

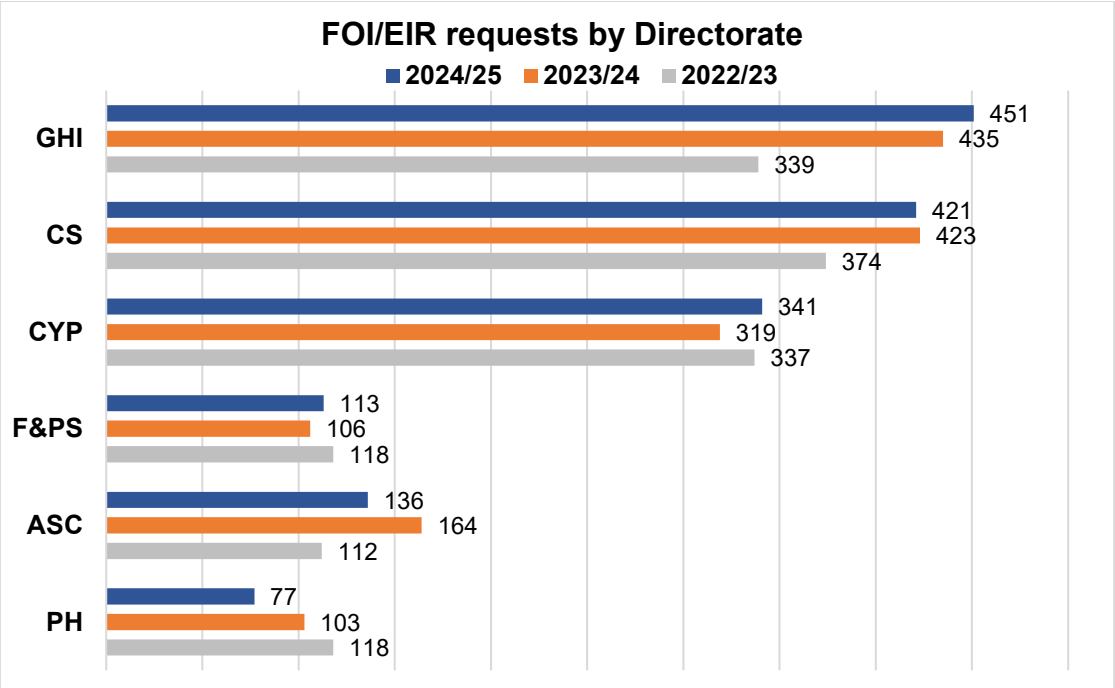

Figure 13 – Information Requests (FOI/EIR) by Directorate 2022/23 to 2024/25

71. Five FOI/EIR-related complaints were lodged with the ICO in 2024/25 compared to two in 2023/24. Of the five complaints, the ICO upheld our original response decision in three instances; for the remaining two complaints, additional information was provided to the requesters as required by the ICO.

Records Management

72. Good records management is a critical element of ensuring the Council manages the information it holds securely and efficiently throughout its lifecycle, whether this be in digital form or paper records. The Council's overall approach to records management is set out in its Records Management Policy, and good practice is reinforced in the Council's mandatory information governance training for staff. To supplement this, a Records Management Handbook will be developed in 2025/26 to provide guidance and tips for services and individual staff members to help them improve their records management practices.

73. The Council has a Records Management Centre (RMC), where paper records are held in storage on behalf of Council services. The RMC is based at Council premises in Ipswich, previously occupied by Suffolk Archives. Documents held at RMC are stored securely, and can be retrieved and accessed by the relevant Council service as necessary. Examples of when records might be needed is when a SAR or FOI/EIR request is received and the information is required for the response.

74. Approximately 34,000 boxes of Council records are currently stored at the RMC. All records held there have a review date, and what happens to these records at the review point is determined by the defined retention periods associated with the record type, which is detailed in the Council's Registers of Datasets (see Section 6).

75. Once records have reached their end of life, a decision is made as to whether the records should be safely destroyed, or placed with Suffolk Archives if they are public or historical interest. Over 5,000 boxes of records were securely destroyed during 2024/25 following reviews of holdings by Council services.

Key Developmental Activities undertaken in 2024/25

76. Whilst a number of activities undertaken during 2024/25 have been referred to above, below is a summary of the key governance related developmental activities undertaken during that year:

    a. Produced updated mandatory e-learning training on information management and data security for all Council staff, with an added focus on information security incidents and data breaches.
    b. Implemented measures to improve the Council's compliance rate for responding to Subject Access Requests (SARs).
    c. Implemented an online system for registering and managing Data Protection Impact Assessments (DPIAs).
    d. Revised the Council's information risk assessment processes to accommodate requests for Artificial Intelligence (AI) systems and software.
    e. Further improved internal processes for responding to FOI and EIR requests (resulting in an improvement in compliance).
    f. Completed the review of the Council's legacy records held at the Records Management Centre.

Priority Activities for 2025/26

77. Listed below is a summary of some of the main developmental activities that are planned for 2025/26. Progress against these actions will be reported in the next iteration of the Information Governance Annual Report:

    a. Implement additional measures to seek to minimise the number of information security incidents and data breaches occurring, including:
        - targeting additional training for those services where incidents are most prevalent, and
        - implementing further technical preventative measures.
    b. Review the Council's data protection compliance tools, including its suite of Privacy Notices, and Register of Data Protection Impact Assessments (DPIAs).
    c. Review and update the Council's suite of information governance policies to reflect organisational changes and wider national developments.
    d. Engage proactively with the Council's overall strategy for the use of Artificial Intelligence (AI) to ensure AI products are adopted appropriately and safely.

e. Develop a Records Management Handbook to enable staff to improve their records management practices.

f. Ensure the Council responds appropriately to the new UK Data (Use and Access) Act and implements any associated changes to policies and procedures.

Annex 1 - Summary of Information Risks on the Corporate Risk Register

Risk Ref & Service Area	Risk Description	Risk Score	Mitigation Score	Mitigation Actions/Themes
RMICTC0005 **Information Governance** **[Head of Information Governance]**	The growth in the number of information security incidents occurring throughout the Council could lead to the greater loss of sensitive information and a corresponding rise in data breaches involving sensitive personal information, resulting in harm to citizens, damage to the Council's reputation and the imposition of sanctions from the Information Commissioner's Office (ICO).	High	High	▪ Comprehensive policies, procedures and guidance updated regularly in the light of new legislation, guidance, and best practice. ▪ Processes in place to learn from security incidents and data breaches. ▪ Security incident monitoring reports reviewed every six months by Corporate Information Governance Board. ▪ Security incident element of mandatory staff training strengthened. ▪ Training targeted at service areas where incidents are especially prevalent. ▪ Firewall security strengthened.
CS0003 **IT Cyber Security** **[IT Security Manager]**	There is a risk the Council could be subject to a major cyber security attack or information breach resulting in financial loss, significant disruption to services, and reputational damage. To function effectively, the Council relies on robust digital technologies and online capabilities to deliver front line services to residents. The constant threat of viruses, hacking, unauthorised access to information is real and have the potential to disrupt networks, web resources, and public services. Public confidence could be affected if the organisation was not able to adequately protect its systems.	Very High	Medium	▪ Raising awareness of cyber threats and impact. ▪ Cyber Threat, Information Governance, and other corporate policies kept updated. ▪ Software & other technology to protect Council infrastructure. ▪ Council runs ad-hoc phishing exercises and testing. ▪ Reviewed latest Cyber advice from the National Cyber Security Centre (NCSC).

Annex 2 – Summary of Actions Undertaken or Planned Regarding Information Security Incidents and Personal Data Breaches

Corporate:

- In-depth six-monthly monitoring of incident and breach levels by Corporate Information Governance Board.
- Strengthened the security incident element of the statutory learning module undertaken by all staff.
- Updated and expanded the security incident guidance and support pages on the SCC intranet
- Regular Phishing exercises undertaken amongst Council staff by the IT Security Team.
- All specific recommendations from the Information Commissioner's Office (ICO) with regard to notified data breaches implemented and monitored.
- Liaison with IT providers regarding additional technical measures that can be implemented to reduce the number of security incidents occurring (e.g. through emails).
- Assessment of the potential for AI products to reduce the prevalence of security incidents and data breaches.
- Assessment of the potential for increased use of customer portals to access personal information rather than being sent by email, post etc.
- Development of bite-size e-learning modules for any staff member who has instigated an information security incident.

Children & Young People's Services (CYP):

- Recruitment of a dedicated Information Governance Lead in 2025 to improve capacity and leadership and drive forward improvements in practice and compliance.
- Re-launch of the CYP Information Governance Board with action plan and risk register reviewed and updated at bi-monthly meetings.
- Development of an information governance Business Intelligence Dashboard to facilitate improved data analysis and insight.
- Any serious data breach automatically escalated to the relevant senior leader(s) within CYP.
- Survey of CYP staff to better understand breadth of knowledge and understanding of security incidents and data breaches to target interventions.
- Monthly information governance newsletter for all CYP staff, the latest of which focused on security incidents and data breaches.
- Re-launch of staff webinars on pertinent information governance topics, including security incidents and data breaches.

Adult Social Care (ASC):

- Regular monitoring and analysis of information security incident and personal data breach levels (including lessons learned discussions) by the well-established and mature ASC Information Governance Board.

- Deep-dive analysis of incidents and breaches in targeted service areas to identify why incidents are occurring and how they can be reduced.
- Targeted training for those service areas where prevalence is high, or where teams have requested training.
- Communications to all staff with key messages regarding security incidents and data breaches.
- Re-launch of improved information governance support offer from the ASC Business Management Team – e.g. ASC-specific guidance on Intranet pages, and a 30-minute recorded session on security incidents.
- Internal process agreement between ASC Information Governance Team and ASC Liquid Logic Team in place to reduce unnecessary security incident reporting.
- Audit of ASC Liquid Logic system undertaken monthly to monitor and highlight any concerns with unauthorised access to customer records.