Information Governance
Annual Report

2021-22

Peter Knight
Head of Information Governance

June 2022

Contents

1. Background and Context

Information is a vital asset to any organisation, and a large and complex organisation like Suffolk County Council holds and manages a vast amount of information, 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.

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.

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 across 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.

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 (currently £2,900). The Council's Data Protection Registration Number is Z5113825, and the current registration expires on 13 December 2022.

2. Assurance and Accreditation

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

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

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

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

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 (CIGB), 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.

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 two data breach related audits concluded in 2021/22 – one relating to the governance of data breaches, and the other relating to access to personal data within the Council's Liquidlogic adults social care (LAS) IT system. Both of these audits resulted in a 'Reasonable Assurance' Opinion on the controls in place.

In the Annual Internal Audit Report & Opinion 2021/22, the Head of Internal Audit concluded that:

> *"The results of data breach related audits show a good level of compliance across the Authority. Internal Audit is satisfied that the Council's policies clearly remind staff of their responsibilities in respect of handling data, including what to do if a security incident occurs, and the Information Governance Team has assessed and taken the appropriate action where necessary. In addition, staff communications are regularly made, and controls are in place to help prevent data breaches, but ultimately human error cannot be eliminated".*

3. Leadership & Governance

Information governance in the Council is overseen by the Corporate Information Governance Board, which provides oversight and direction on information governance matters to provide assurance in the areas of information governance, information security and information

rights. The terms of reference for the Board are shown in Appendix 1. 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 Corporate Information Governance Board is supported by service-specific information governance boards within the Children & Young People's Services (CYP) and Adult & Community Services (ACS) 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.

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 Clinical Information Assurance Group (CIAG) 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 experience in information governance matters.

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

Senior Information Risk Owner

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, and the SIRO is a member of the Corporate Information Governance Board.

Caldicott Guardians

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 & Community Services (ACS), 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

The Head of Information Governance leads the team 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 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 Governance, Legal & Assurance, and acts as the Chair of the Corporate Information Governance Board on behalf of the SIRO.

Data Protection Officer

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 Suffolk County Council.

IT Security Manager

The IT Security Manager has responsibility for ensuring the Council's Information Technology 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 (CIGB).

4. Information Risk Management

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 three information-related risks on the Corporate Risk Register, namely:

a. The growth in the number of **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. The continued growth in the volume and complexity of **Subject Access Requests (SARs)** from individuals wishing to access their personal data has resulted in a low level of compliance with statutory timescales. Failure to improve the level of compliance could lead to increased level of complaints from requestors to the Information Commissioner's Office (ICO) resulting in intervention by the ICO with potential sanctions, negative media coverage and associated damage to the Council's reputation.

c. 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.

A summary of the three risks, including risk ratings and mitigating actions, is provided in Appendix 2.

5. Information Governance Policy Framework

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.

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 fundamental review of all policies was undertaken during 2021-22, and the revised policies were approved by the Corporate Information Governance Board and the SIRO.

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
- 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

These policies are supported by other documentation and associated guidance where required, all of which is made available to all Council staff via the Council's intranet (mySCC). The range of information, advice and guidance published on mySCC has been significantly expanded during 2021/22.

6. Data Protection Compliance Tools

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

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 every year.
https://www.suffolk.gov.uk/about/privacy-notice/

Registers of Datasets

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 now 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

Data Protection Impact Assessments (DPIAs) are the Council's main way of undertaking information risk assessments of new services, 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 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 development, 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.

All DPIAs are recorded on a central Register for compliance purposes, and it is clear from the graph below that DPIAs are being adopted extensively across the organisation, with 162 DPIAs completed and registered in 2021/22.

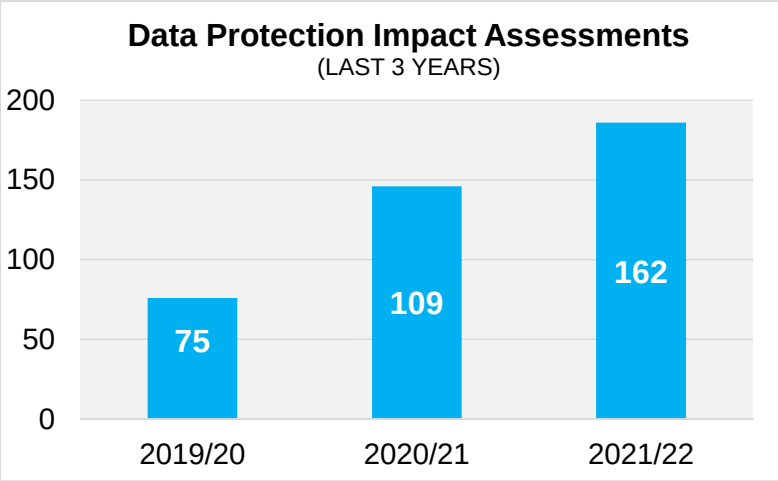

Figure 1 – Data Protection Impact Assessments registered 2019/20 to 2021/22

Register of Information Sharing Agreements

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.

The Council publishes an Information Sharing Assurance Framework, which sets out what senior managers and dataset owners need to consider in terms of negotiation, risk assessment and documentation prior to sharing personal information with an external body for business purposes. Furthermore, 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.

7. Data Ethics

In 2021, the Council developed and published an Ethical Data Stewardship Charter to demonstrate the Council's commitment to a set of principles which govern 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

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

The Council has also committed to establishing an Ethics Panel to provide advice to the organisation on data ethics so it can uphold the principles of the Ethical Data Stewardship Charter, and maintain public trust. The Panel will be set up in 2022/23 under the auspices of the Council's Audit Committee.

8. Performance Reporting

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.

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.

A summary of the KPIs that are included in the Corporate Performance Report, and comparative performance for these for 2020/21 and 2021/22, is shown below:

KPI	2020/21	2021/22
Number of Security Incidents reported (all incidents)	456	577
Number of Security incidents reported (Priority 3+)	148	64
Number of data breach notifications to the ICO	9	5
Number of Subject Access Requests (SARs) received	276	264
Number of open SARs	78	65
Number of overdue SARs	16	19
% of SARs responded to within statutory timescales	63%	55%
Number of Information Requests (FOI/EIR) received	1196	1247
% of Information Requests responded to within statutory timescales	94.5%	94.5%

Figure 2 – Corporate Information Governance KPIs 2020/21 to 2021/22

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

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 data breaches, and an annual FOI/EIR request monitoring report.

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.

9. Training and Awareness-Raising

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.

The ICO requires all staff 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 package, 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.

The latest iteration of the mandatory information training for staff ('Our Information, Our Responsibilities') was launched in April 2022. Prior to this, the Council achieved 96% compliance with the requirement for staff to undertake this type of training; it should be noted that in order to achieve a compliant DSP Toolkit submission (see Section 2), at least 95% uptake is required.

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.

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 (mySCC), 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 articles in the weekly staff newsletter (InsideSCC).

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 appropriate.

10. Information Security Incidents and Personal Data Breaches

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

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). Below is a summary of the categories:

- Level 1 relates to incidents carrying a negligible risk
- Level 2 relates to incidents carrying a minor risk
- Level 3 relates to incidents carrying a moderate risk
- Level 4 relates to an incident carrying a major risk
- Level 5 relates to incidents carrying an extreme risk.

All level 3 or above incidents are considered for notification to the ICO.

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

The UK GDPR states that where a personal data breach incident is likely to result in risk 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.

During 2021/22 there were 577 security incidents reported via IT Self Service. This is a significant increase on the previous year, which in turn was an increase on 2019/20, indicating that staff are becoming more aware of the need to report incidents in a timely manner.

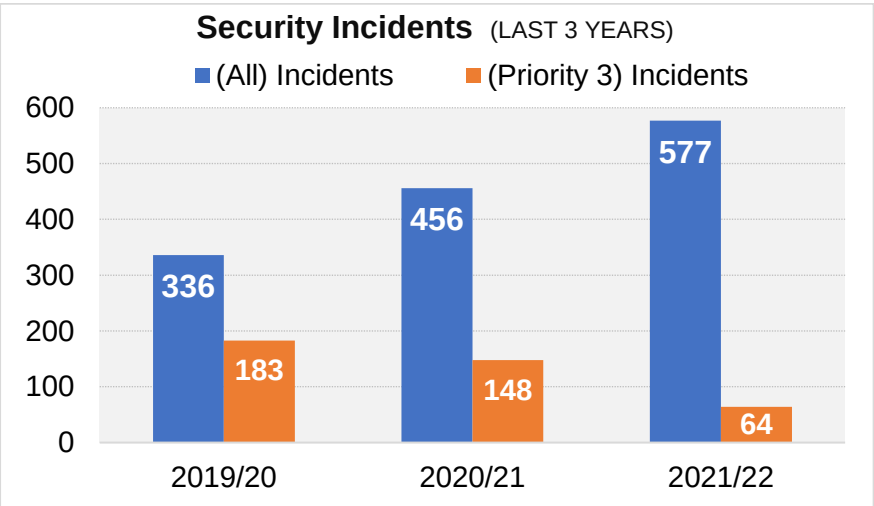

Figure 3 – Security Incidents 2019/20 to 2021/22

Of the security incidents in 2021/22, 64 were in the more serious categories (Priority 3+), which is a significant reduction compared to the previous two years. This reflects both a more systematic and sophisticated approach to assessing security incidents, but also the impact of more timely investigations of incidents by services with mitigating actions being put in place.

In terms of the nature of security incidents, the table below shows a breakdown by type for all incidents as well as for the more serious incidents.

Type of incident	All incidents	Priority 3+ incidents
Information sent to wrong recipient (email/post)	257	14
Unauthorised access (internal)	48	15
Unauthorised sharing	44	8
Fraudulent emails/phishing	36	0
Insecure transfer	35	3
Lost encrypted devices	24	0
Incorrect information recorded	22	2
Verbal disclosure	23	10
Malware/virus	19	1
Data mishandling	18	2
Third party incident (SCC data)	14	2
Unredacted information	11	4
Non-personal information	7	0
Unauthorised access (external)	6	1
Lost paperwork	5	1
Insecure method of disposal	4	0
Theft of information/device	3	1
Third party incident (SCC as data processor)	1	0
Total	**577**	**64**

Figure 4 – Security Incidents by Type 2021/22

The vast majority of security incidents are the result of human error. In terms of all reported incidents, by far the most prevalent type of incident is information being sent to the wrong recipient, either via email or in the post (257 incidents in 2021/22). However, for the more serious (Priority 3+) incidents, the highest number of incidents involved unauthorised access to records by staff (15 incidents), followed by inappropriate verbal disclosure of personal information (10 incidents), and unauthorised sharing of information (8 incidents).

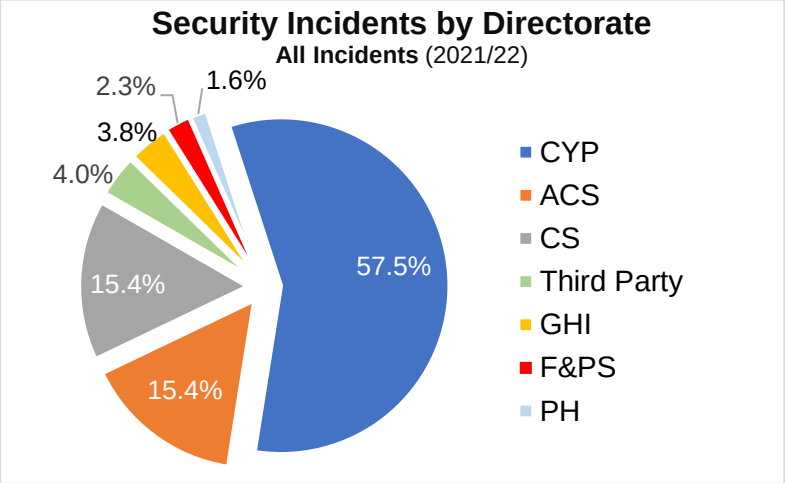

Figure 5 – Security Incidents by Directorate (All Incidents) 2021/22

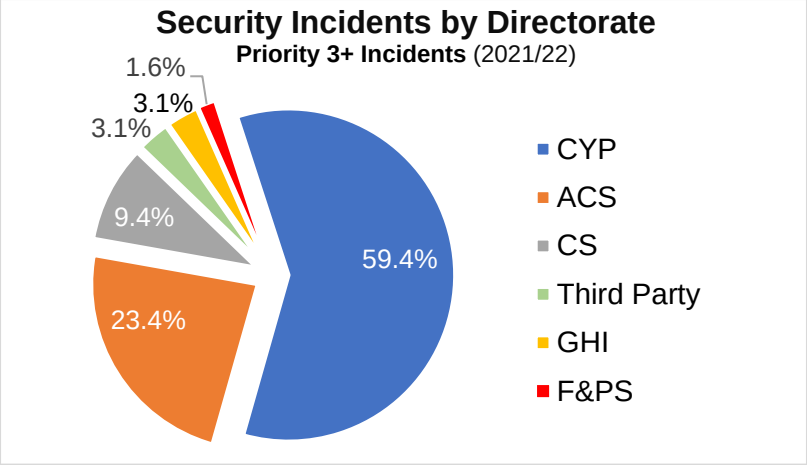

Figure 6 – Security Incidents by Directorate (Priority 3+ Incidents) 2021/22

CYP = Children & Young People's Services
CS = Corporate Services
GHI = Growth, Highways & Infrastructure
ACS = Adult & Community Services
F&PS = Fire & Public Safety
PH = Public Health

As can be seen from the charts above, the majority of security incidents occur within Children & Young People's Services, both in terms of all incidents and the more serious (Priority 3+) incidents.

Five incidents in 2021/22 met the threshold for notification to the Information Commissioner's Office (ICO), but this is a considerable drop compared to the previous two years. All five notifications resulted in 'no further action' by the ICO (thus resulting in no sanctions taken against the Council), although any recommendations that form part of the ICO's decision are always implemented and monitored.

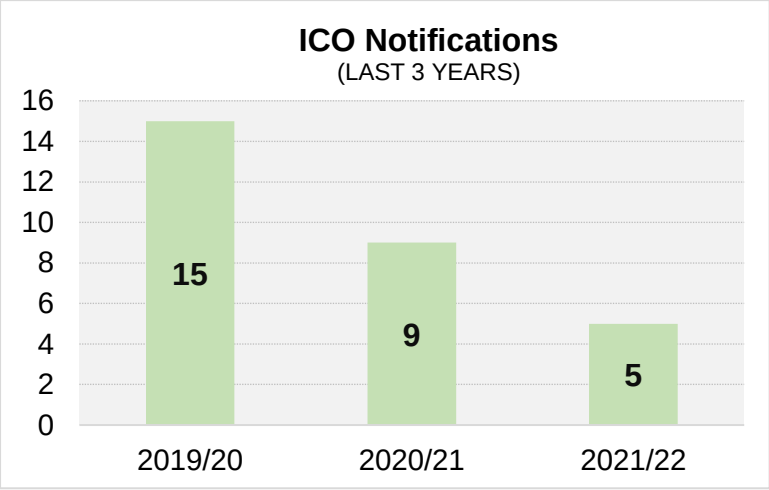

Figure 7 – Data Breach Notifications to the ICO 2019/20 to 2021/22

11. Individuals' Rights

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

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

Subject Access Requests (SARs)

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 personal information about them held by the Council, and to provide them with a copy of that information. The right can also be exercised by an authorised representative on the 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.

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 (264 in 2021/22), although this is a slight reduction on the previous year (276).

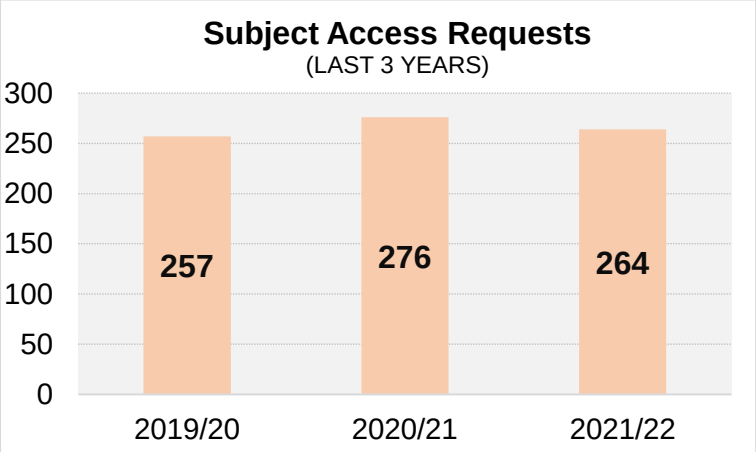

Figure 8 – Subject Access Requests (SARs) 2019/20 to 2021/22

Over three-quarters of SARs received 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.

The high volume of SARs, combined with the fact that a significant number of these involve voluminous or complex records, has placed considerable pressure on the organisation and achieving statutory compliance rates has proved a challenge. Of the 264 SARs made to the Council in 2021/22, 55% were responded to within the statutory timescale. In 2021/22, over 10% of the requests involved the processing of over 5000 pages of records. All of the 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. However, the Council liaises with requesters where there are

likely to be delays to agree a batch release plan or an alternative acceptable deadline. Furthermore, resources for dealing with SARs has been increased in 2021/22, and this should impact positively on the Council's ability to meet prescribed timescales going forward.

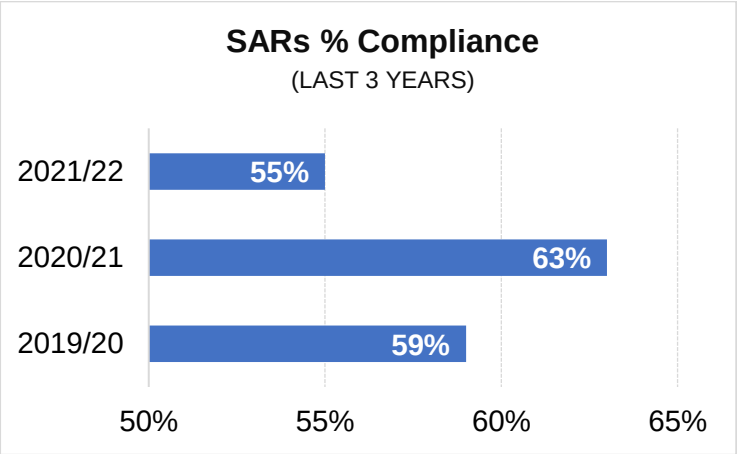

Figure 9 – Subject Access Requests (SARs) Compliance 2019/20 to 2021/22

Other Individuals' Rights requests

Since GDPR has been in force, there have been number of requests from individuals exercising rights (other than the right of access referred to above), relating to their personal data. Particularly, there has been an increase in terms of requests for 'the right to rectification' and 'the right to erasure', whereby individuals have disputed information in their records. The Council has one month to respond to such requests, and these are actioned by services where it is appropriate to do so. The figures below relate to the number of requests received in 2021/22.

Type of request	No. of requests
Request for erasure	6
Request for rectification	4
Request to restrict processing	1
Total	**11**

Figure 10 – Number of Individuals Rights Requests (non-SAR) 2021/22

12. Information Requests (Freedom of Information and Environmental Information Regulations)

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.

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.

The number of FOI and EIR requests in the last three years is shown in the chart below. As can be seen, the Covid-19 pandemic did not have a significant impact on the number of requests the Council received. The 1,247 requests in 2021/22 equates to 104 requests per month.

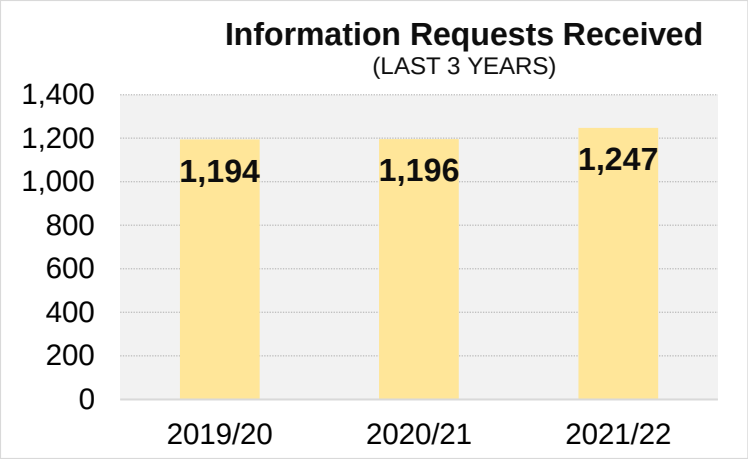

Figure 11 – Number of Information Requests (FOI/EIR) received 2019/20 to 2021/22

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. The ICO's expected 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 two years, even during the Covid-19 pandemic.

	2020/21	2021/22
% of Information (FOI/EIR) Requests responded to within 20 working days	94.5%	94.5%

Figure 12 – Information Requests (FOI/EIR) compliance 2020/21 to 2021/22

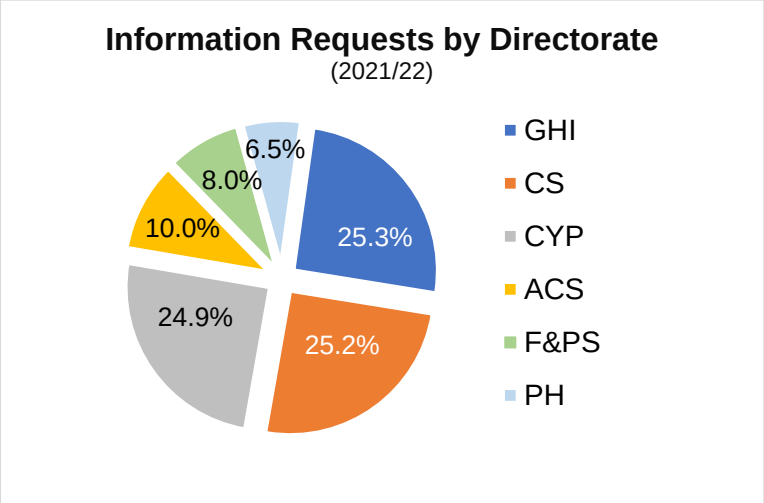

Figure 13 – Percentage of Information Requests (FOI/EIR) by Directorate 2021/22

CYP = Children & Young People's Services
CS = Corporate Services
GHI = Growth, Highways & Infrastructure
ACS = Adult & Community Services
F&PS = Fire & Public Safety
PH = Public Health

Requests are received relating to a wide variety of issues or services, as the chart above illustrates. The most requests received in 2021/22 relate to Growth, Highways & Infrastructure (GHI), Corporate Service (CS), and Children & Young People's Services (CYP). Far fewer requests are received for Adult & Community Services (ACS), Fire & Public Safety (F&PS) and Public Health.

If a requester is not satisfied with the response to their FOI/EIR request, they can request an Internal Review of the response. In 2021/22, 58 such reviews were requested, which equates to 4% of the total requests received. In 39 cases, the review upheld the original response, 8 cases were partially upheld, 9 were overturned, and 2 were withdrawn. Three complaints were lodged with the ICO, but no Decision Notices were served on the Council as a result of the complaints (the outcome of one of these complaints is still awaited).

13. Records Management

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.

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.

Approximately 45,000 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). 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. Approximately 4,000 boxes of records were securely destroyed during 2021/22 following reviews of holdings by Council services.

14. Key Developmental Activities in 2021-22

Whilst a number of activities undertaken during 2021/22 have been referred to above, below is a summary of the key governance related developmental activities undertaken during that year:

a. Reviewed and updated the Council's suite of information governance policies.
b. Strengthened security incident reporting and management arrangements in response to the increase in data breaches.
c. Published revised information risk assessment (DPIA) processes, guidance and documentation.
d. Published additional information, advice and guidance relating to information governance on the Council's intranet (mySCC).

e. Developed and published the Council's Ethical Data Stewardship Charter.

f. Relocated the Records Management Centre from leased premises to Suffolk County Council premises previously occupied by Suffolk Records Office, thereby improving security of the records held there whilst saving the Council money.

g. Launched updated mandatory e-learning training on information management and security for all staff.

h. Provided bespoke training sessions for services and teams on security incidents, information risk assessment, Subject Access Requests, FOI/EIR requests, and records management.

i. Provided information security training for all 75 County Councillors following the Council elections in May 2021.

15. Priority Activities for 2022-23

Listed below is a summary of some of the main developmental activities that are planned for 2022/23. Progress against these actions will be reported in the Annual Report for 2022/23:

a. Develop and publish an Information Governance Annual Report

b. Further develop the 'self-service' approach to information management advice and guidance via the Council's intranet (mySCC)

c. Work collaboratively across services to improve the Council's compliance rate for Subject Access Requests (SARs)

d. Develop a new web-based approach to the Council's Freedom of Information (FOI) Publication Scheme

e. Complete a programme of data protection compliance reviews, including Privacy Notices, Registers of Datasets, Data Protection Impact Assessments (DPIAs) and Information Sharing Agreements (ISAs)

f. Convene a Data Ethics Panel in support of the Ethical Data Stewardship Charter.

g. Implement further measures to seek to minimise security incidents, including developing training programmes for instigators of security incidents

h. Continue the programme of reviews of records held by Council services at the Records Management Centre (RMC)

i. Publish enhanced records management guidance for staff.

Appendix 1 - Corporate Information Governance Board Terms of Reference

Corporate Information Governance Board Terms of Reference

PURPOSE OF THE BOARD

The primary purpose of the Corporate Information Governance Board (CIGB) is to drive and oversee the ongoing development of corporate strategies to ensure Suffolk County Council has effective information governance and assurance arrangements in place.

ROLE OF THE BOARD

1. To champion corporate information governance and assurance across all areas of the Council
2. To foster a culture across the Council that values, protects, uses and shares information
3. To promote co-operation and learning across the Directorates on all matters relating to information governance and assurance at work.
4. To monitor the information risk management arrangements that the Council has in place
5. To monitor the Council's compliance with relevant legislative requirements, assurance frameworks and regulations
6. To review and approve new information governance policies and changes to existing policies
7. To oversee the ongoing development and efficacy of the Council's Information Asset Register (Registers of Datasets)
8. To receive and review relevant information governance performance information, seeking assurances that robust arrangements are in place to clearly communicate and incorporate any lessons learnt into corporate policies, procedures and guidance
9. To receive and consider reports into breaches of information security, availability or confidentiality and, where appropriate, undertake or recommend remedial action
10. To ensure adequate information training and awareness-raising arrangements and resources are in place for Council staff and Councillors
11. To consider any information governance issues brought to its attention by individual Board members that have wider corporate implications
12. To report to, and advise, the Council's Corporate Leadership Team and Joint Leadership Team on any matters relating to information governance that should be brought to their attention
13. To consider reports, information and new legislation from central government and the Information Commissioner's Office (ICO) and make appropriate recommendations where necessary to the Corporate Leadership Team
14. To act as a key reference and approval body for the development of wider information governance arrangements across the public sector in Suffolk
15. Individual members of the Board have a responsibility to ensure that they engage proactively with the Board and disseminate relevant information arising from the activities of the Board to their management teams and/or other fora

ACCOUNTABILITY

The Board is accountable to the Council's Corporate Leadership Team (CLT), and will report and make recommendations to CLT where necessary.

The Senior Information Risk Owner (SIRO) and the CIGB, in conjunction with the Council's Information Governance team, is responsible for maintaining the currency of all aspects of information policy, including related sub-policies, procedures and guidance. This oversight will take into account legal compliance, government directives, and corporate strategies and resources.

BOARD MEMBERSHIP

The Chair of the Board is the Council's Senior Information Risk Owner (SIRO), currently, the Director of Corporate Services. The Chair may delegate responsibility for chairing the Board to another member of the Board.

Members of the Board include:

- Head of Information Governance
- Caldicott Guardian (Adult Services)
- Caldicott Guardian (Children's Services)
- Head of Knowledge & Intelligence
- Data Protection Officer & Compliance Manager
- Data Protection & Training Manager
- IT Security Manager
- At least one representative(s) from each Directorate and/or key service area – ideally an Information Governance lead
- Others by invitation

FREQUENCY OF MEETINGS

- The CIGB should normally meet quarterly; however, it may meet more frequently as required
- Dataset Owners are expected to set up their own working arrangements to manage their areas of responsibility
- The Board may also establish task and finish groups to undertake particular projects or investigations, which will then report back to the Board
- Minutes of meetings will be produced and circulated within two weeks of the meeting

REVIEW OF TERMS OF REFERENCE

- These Terms of Reference should be reviewed every 2 years and any changes agreed by the Board.

Appendix 2 - 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 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 (12)	Medium (9)	▪ Comprehensive policies, procedures and guidance updated regularly in the light of new legislation, guidance, and best practice. ▪ Processes in place to learn from potential security incidents and data breaches. ▪ Security incident monitoring reports reviewed by Corporate Information Governance Board & Corporate Leadership Team. ▪ Security incident element of mandatory staff training strengthened. ▪ Firewall security strengthened.
RMICTC0006 **Information Governance** **[Head of Information Governance]**	The continued growth in the volume and complexity of Subject Access Requests (SARs) from individuals wishing to access their personal data has resulted in a low level of compliance with statutory timescales. Failure to improve the level of compliance could lead to increased level of complaints from requestors to the Information Commissioner's Office (ICO) resulting in intervention by the ICO with potential sanctions, negative media coverage and associated damage to the Council's reputation.	High (12)	Medium (9)	▪ Active management of 'open' and 'overdue' SARs by Information Governance Team. ▪ Staff resources specialising in this area of work have been strengthened. ▪ Extensive guidance, support and training to directorates in dealing with SARs. ▪ Regular communication with requesters where delays are likely, and agreement of batch release plans for complex and/or voluminous SARs ▪ Regular performance reporting to Directorate Management Teams and Corporate Leadership Team.
CS0003 **IT Cyber Security**	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	High (12)	Medium (9)	▪ Raising awareness of cyber threats and impact. ▪ Cyber Threat, Information Governance, and other corporate policies kept updated.

Risk Ref & Service Area	Risk Description	Risk Score	Mitigation Score	Mitigation Actions/Themes
[IT Security Manager]	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.			▪ 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) - based on Ukraine - Russia escalations