Senior Information Risk Officer Report
2023/2024

Contents

Policy owner: Siobhan Martin, Head of Internal Audit and Senior Information Risk Officer
Issue date: June 2024
Review date: June 2025

1. BACKGROUND AND CONTEXT

1.1 Information is a vital asset to any organisation, and a large and complex organisation like East Suffolk Council holds and manages a vast amount of information, some of which can be classified as 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 are three main legislative Acts that determines how the Council manages the information it holds. Which 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 £2,900.00). The Council's Data Protection Registration Number is ZA510093, and the current registration expires on 01 April 2025.

Service Area's within the Council may also have their own Acts in Law which may influence or determine how data is processed.

2. ASSURANCE AND ACCREDIATION

2.1 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:

NHS Data Security & Protection Toolkit

In 2023/2024, the Council completed the NHS Data Security and Protection Toolkit self-assessment demonstrating that we meet the required standards as measured against the National Data Guardian's 10 data security standards, have excellent information governance practices ensuring that personal information is handled correctly. Resulting in the Council obtaining accreditation which qualifies the Council to receive NHS data for various projects aimed to benefit the local community. The next toolkit assessment is due to commence 2025/26.

Annual IT Health Check (National Cyber Security Centre approved)

Our annual IT Health Check includes network penetration testing and is provided by external security experts, who thoroughly test the security of our network from both internal and external perspectives. By conducting regular proactive penetration tests, organisations can identify vulnerabilities and weaknesses in their systems before they can be exploited by attackers. This allows for the timely remediation of any potential risks, reducing the likelihood of service interruptions and associated financial losses.

In addition to the annual health check, the Digital team run their own vulnerability checks and reports throughout the year.

Payment Card Industry Data Security Standard (PCIDSS)

The Digital team undertake PCIDSS compliance on an annual basis, ensuring the Council is up to date with all assessments against each area taking payments and compliant to these strict industry standards which ensure secure levels of transaction and secure storage, including that no payment card information is stored on East Suffolk Council networks.

Cyber Assessment Framework – LGA Cyber360 Review

In November/December 2023, a self-assessment was undertaken using the National Cyber Security Centre's Cyber Assessment Framework (NCSC CAF), which provides a systematic and comprehensive approach to assessing the extent to which cyber risks to essential functions are being managed by the organisation responsible. The framework was developed as part of a pilot project across a handful of Local Government organisations and the Council has been pro-active in adoption of this framework before it becomes mandatory practice.

Following the self-assessment exercise, the LGA Cyber team were invited in to carry out a Cyber360 review, which is also based on the principles within the NCSC CAF and consists of the LGA cyber team themselves with experts from other local government organisations to do a peer-review style assessment of our Cyber Security arrangements, which took place in February 2024.

Head of Internal Audit

In addition to the external assurance mechanisms outlined above, the Head of Internal Audit is responsible for the Data Protection Team and is Strategic Lead for FOI and EIR. Recruitment is planned for a senior member of the Internal Audit Team to provide independent assurance in line with the Audit Charter upon ICT technical matters. The Head of Internal Audit is a member of the Corporate Leadership Team (CLT). Membership of CLT enables the Head of Internal Audit to garner information around governance matters, as well as any breaches of confidentiality or security.

3. LEADERSHIP AND GOVERNANCE

3.1 Information governance in the Council is overseen by the Head of Internal Audit & Strategic Lead for Information Governance and the Chief Executive, which provides oversight and direction on information governance matters to provide assurance in the areas of information governance.

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; 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 East Suffolk Council, the SIRO role is designated to the Head of Internal Audit, and the SIRO is a member of the Corporate Leadership Team.

Data Protection Officer

As a public body, there is a duty on the Council under the UK General Data Protection

Regulation (UK 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 Head of Internal Audit & Strategic Lead for Information Governance, who is supported by the Deputy Data Protection Officer & Internal Audit Manager and the Data Protection Team, all of whom report to the DPO & Strategic Lead for Information Governance. The Head of Internal Audit & Strategic Lead for Information Governance also acts as the SIRO for East Suffolk Council and is the Chair for the Suffolk Information Governance Group (SIGG).

ICT Infrastructure and Operations Manager

The ICT Infrastructure and Operations Manager has responsibility for governance regarding ICT Security. Within the remit of Cyber Security, key responsibilities for the ICT Infrastructure and Operations Manager include monitoring and ensuring compliance with the ICT assurance and accreditation elements listed in section 2 above.

Overarching responsibility lies with the Head of Digital, Programme Management and Customer Services.

4. INFORMATION RISK MANAGEMENT

4.1 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 Risk Management Strategy. 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.

5. INFORMATION GOVERNANCE POLICY FRAMEWORK

5.1 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 intranet for staff access and some available to the public on the Councils website. The current suite of information governance policies/guidance is as follows:

- Data Protection Policy
- Data Quality and Management Policy
- Appropriate Policy Document
- Freedom of Information (FOI) Guidance
- ICT Acceptable Use Policy

- ICT Security Policy
- Information Classification Policy (draft)
- Information Risk & Records Management Policy (draft)

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 (SharePoint).

An in-depth analysis of the Council's existing Data Protection policies and practices is conducted via an annual ICO Self-Assessment. This assessment reviews these policies and practices against current ICO requirements to provide assurance that the necessary measures are in place and identify where additional measures may be required, which are subsequently highlighted as actions to be included in the Data Protection Plan for the following year.

6. DATA PROTECTION COMPLIANCE TOOLS

6.1 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.

Information Asset Registers

Information Asset Registers help an organisation to keep track of the information it holds. For an organisation as large and complex as the Council, this is especially important. A separate Information Asset Register is in place for each Service Area within the Council. 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.

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 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. The Head of Internal Audit & Strategic Lead for Information Governance present figures to CLT quarterly which provides a strategic overview of volume of DPIAs (see section 8).

Register of Data Sharing Agreements

Data Sharing Agreements (DSAs) are one of the Council's ways to prevent data misuse, data abuse, and unregulated data dissemination. DSAs are an agreement between two or more parties that set out the purpose of the data sharing, which data will be shared, standards to be adhered to, roles and responsibilities and, most importantly, how the data can be used.

All DSAs are recorded and logged in a central database held by the Data Protection Team. The Head of Internal Audit & Strategic Lead for Information Governance present figures to CLT quarterly which provides a strategic overview of volume of DSAs (see section 8).

7. DATA ETHICS

7.1 The UK GDPR focus on data ethics is specifically on protecting people's privacy which includes transparency, fairness and accountability.

Transparency

Transparency means that your actions, processes and data are made open to inspection by publishing information about the project in a complete, open, understandable, easily accessible, and free format.

Fairness

It is crucial to eliminate your project's potential to have unintended discriminatory effects on individuals and social groups. You should aim to mitigate biases which may influence your model's outcome and ensure that the project and its outcomes respect the dignity of individuals, are just, non-discriminatory, and consistent with the public interest, including human rights and democratic values.

Accountability

Accountability means that there are effective governance and oversight mechanisms for any project. Public accountability means that the public or its representatives are able to exercise effective oversight and control over the decisions and actions taken by the Council,

in order to guarantee that Council initiatives meet their stated objectives and respond to the needs of the communities they are designed to benefit.

7.2 The Council has an obligation to be open, transparent, and fair in our interactions with the public and internal staff, and this includes our use of data relating to those individuals and groups. Responsibility for the ethical capture, storage and sharing of data relating to individuals and groups sits with the Council, as does the fair and unbiased use of analytics and intelligence tools to inform decision making. The Council shall address any corruption, misuse, or abuse of data, and ensure a level of quality and accuracy of data.

7.3 The Council holds and manages a vast amount of information, some of which can be classified as sensitive in nature. It is therefore vital that at the start of a projects life cycle that a fully thought through process including the consideration of ethics is documented by way of DPIA.

7.4 It is critical that all Council staff understand the importance of handling Council's information in an ethical, transparent, and fair manner.

7.5 There are a number of projects/ initiatives that incorporate all the Suffolk Local Authority's encouraging cross working including the ability to draw on the expertise of the Suffolk County Council Ethics Panel.

8. PERFORMANCE REPORTING

8.1 The Head of Internal Audit & Strategic Lead for Information Governance presents an Information Governance Statistic report to CLT quarterly which provides a strategic overview of Data Protection activity as follows:

Data Protection and Corporate Fraud processed 665 requests made under data protection legislation.

	Request Type	Q1	Q2	Q3	Q4	23/24 Total	22/23 Total
Data Protection	Proof of Life	0	0	0	2	**2**	2
	Right to Erasure	0	0	0	5	**5**	2
	Right to Rectification	0	0	0	0	**0**	0
	Subject Access Request	10	8	9	11	**38**	39
	Third Party Request	82	81	99	77	**339**	352
Corp. Fraud	Third Party Request	78	73	75	55	**281**	347
	Total	**170**	**162**	**183**	**150**	**665**	**742**

Data Protection team investigated 117 data protection cases, of which 2 case required reporting to the ICO.

The ICO concluded their investigations into these breaches, no fines issued, and no further action was needed by ESC.

Outcome	Q1	Q2	Q3	Q4	23/24 Total	22/23 Total
Confirmed Breach	10	13	17	22	**62**	62
Non-Compliance with Legislation	1	3	8	3	**15**	9
Compliance with Legislation	0	0	0	0	**0**	0
Not a Breach	10	11	10	9	**40**	37
Under Investigation	0	0	0	0	**0**	1
Total	**21**	**27**	**35**	**34**	**117**	**109**
Reported to the ICO	**1**	**1**	**0**	**0**	**2**	2

Data Protection team have received 316 internal requests for advice. The team provides independent strategic and operational level advice, support and guidance on data protection, risk and control processes.

Advice Type	Q1	Q2	Q3	Q4	23/24 Total	22/23 Total
Data Protection Impact Assessment	13	12	9	14	**48**	54
Data Sharing Agreements	23	29	30	32	**114**	62
FOI / EIR	0	0	0	0	**0**	2
GDPR	24	25	25	33	**107**	74
Information Asset Register	1	1	0	0	**2**	0
Privacy Notices and Consent	4	4	6	5	**19**	13
Releasing Information	3	2	12	2	**19**	33
Retention and Deletion	0	1	4	2	**7**	8
Training and Guidance	0	0	0	0	**0**	0
Total	**68**	**74**	**86**	**88**	**316**	**246**

FOI and EIR requests are processed by the Customer Services team.

	Q1	Q2	Q3	Q4	23/24 Total	22/23 Total
Requests Received FOI	218	223	211	234	**886**	521
Requests Received EIR	30	46	48	67	**191**	N/A
Land Charge Search Requests Received	625	692	587	587	**2491**	2258
Total Requests Received	873	961	846	888	**3568**	2779
Requests Closed	847	968	870	899	**3584**	2819
Requests Completed within Target	99.5%	99.5%	99.7%	99.3%	**99.47%**	99.41%
Internal Reviews	1	4	2	2	**9**	19
Tribunal Reviews	0	0	0	0	**0**	0
Requests Referred to the ICO	0	1	1	1	**3**	3

*Figures are for financial year 2023/24.

8.2 The Head of Digital, Programme Management and Customer Services presents reports to the Corporate Leadership Team quarterly which provides a strategic overview of cyber incidents and cyber security and IT incidents resolution. The Portfolio Holder is also briefed separately on a regular basis by Head of Digital, Programme Management and Customer Services or Strategic Director.

Cyber Attacks including failure of ICT due to robustness of network (Cyber Security/ Resilience) also features on the Council's Corporate Risk Register which is shared and reviewed at Corporate Leadership Team and Audit & Governance Committee.

9. TRAINING AND AWARENESS RAISING

9.1 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 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 was launched in this financial year and 98% of staff have completed the training.

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.

Information governance training, covering data protection, records management and Freedom of Information, is also provided to all County Councillors by the Head of Internal Audit following an election. All Councillors received this training following the Council elections in May 2023 as part of their induction programme.

10. PERSONAL DATA BREACHES AND INFORMATION SECURITY INCIDENTS

10.1 Personal Data Breaches

Confidentiality and security of personal data of service users and residents is extremely important, and the Council has robust policies and processes in place to minimise the risks associated with collecting, storage, and management of vast amounts of information.

Some incidents involving this information may 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. Officers are instructed that all such incidents should be reported to the Data Protection Team for consideration and risk assessment in line with the Data Protection Policy.

The Council 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. Additionally, the Council may also notify individuals for transparency, where it is deemed appropriate and will not cause further harm or distress to the individual.

The UK GDPR states that, where a personal data breach 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. Additionally, the Council has the option to notify the ICO where a breach may not meet the threshold to report but is deemed serious enough to be made aware. This requires the use of the ICO's standard notification form and, of the breaches reported to the Data Protection Team in 2023/2024, 2 breaches have been reported to the ICO to date. The ICO concluded their investigations into these breaches, no fines were issued, and no further action was needed by the Council.

The vast majority of data breaches are the result of human error. In terms of all reported breaches, by far the most prevalent type of breach is information being sent to

the wrong recipient, either via email or in the post.

A report is produced for CLT quarterly which details, volume, nature, and outcome of all potential data breaches, see section 8.

10.2 **Information Security Breaches (ICT incidents)**

When an incident that affects the security of any ICT systems does occur, it has to be reported to the Head of Digital, Programme Management and Customer Services, and/or where appropriate to Internal Audit as soon as it discovered, in line with the Council's ICT Security Policy.

During 2023/24 there were zero security incidents reported to ICT. Further information can be found on the Our Foundations dashboard.

11. INDIVIDUALS' RIGHTS

11.1 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 Data Protection Team coordinates the process for dealing with individuals' rights requests. The most prominent right we see used by individuals in the right to access also known as a Subject Access Request.

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.

12. INFORMATION REQUESTS (FOI/EIR)

12.1 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 Freedom of Information Team, with relevant services providing the information for the response to the request. The Head of Internal Audit is the Strategic Lead for FOI and EIR and the Internal Audit Service also provides specialist advice, guidance and support to staff who are involved in responding to a request.

The Head of Internal Audit & Strategic Lead for Information Governance present figures to CLT quarterly which provides a strategic overview of volume of FOIs (see section 8).

13. RECORDS MANAGEMENT

13.1 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 Information Risk and Records Management Policy (in draft) and Data Quality and Management Policy (under refresh). Good practice is reinforced in the Council's mandatory information governance training for staff and the routine use of Information Asset Registers.

14. PRIORITY ACTIVITIES FOR 2024/25

14.1 SIRO to ensure all statutory responsibilities are effectively fulfilled.

14.2 The Data Protection Officer produces a plan of work for the Data Protection Team on an annual basis which includes an action plan of activities that will take place. Progress against this action plan is presented to Audit & Governance Committee. Some examples of what was included within the 23/24 plan are:

- Implementation of the new Data Protection and Data Security e-learning.
- ICO Self-Assessment

14.3 FOI/EIR plan to be created for 2024/25.

14.4 Creation of the Cyber Security Action Plan, which brings together all outputs and recommendations from the Annual IT Health check/Penetration Testing, the NCSC CAF Self-Assessment and the LGA Cyber360 review into a single action plan. The nature of cyber security means that it is an ever-changing landscape as new technology is developed and new vulnerabilities are identified. The Cyber Security Action Plan will formalise all actions from all checks into a single action plan and will become an ongoing action plan to address all cyber security needs going forward.

APPENDIX 1 – CORPORATE LEADERSHIP CHARTER

CLT Charter

APPENDIX 2 – SUMMARY OF INFORMATION GOVERNANCE RISKS ON THE CORPORATE RISK REGISTER

Risk Level (corporate or service level)	**Risk Name**	**Service Area**	**Risk Score**
Corporate (June 2024)	Cyber Attacks including failure of ICT due to robustness of network (Cyber Security/ Resilience)	Digital, Programme Management & Customer Services	C2 (Amber)