INFORMATION SECURITY INCIDENT MANAGEMENT POLICY

We will on request produce this Policy, or particular parts of it, in other languages and formats, in order that everyone can use and comment upon its content.

Document ID: ICT-PL-0109
Version: 1.5
Date: December 2025
Review date: December 2027

DOCUMENT MANAGEMENT

Version	Date	Summary of Changes
1.1	July 2017	First version
1.2	November 2018	Review and updates
1.3	March 2021	Review and updates
1.4	June 2023	Review and updates
1.5	November 2025	Review and updates

Accountable Owner		Approval date
Head of Information Governance	Peter Knight	04/12/2025
Head of Information Governance	Peter Knight	05/02/2024

Responsible Owner		Approval date
DP & Training Manager	Joanne Withey	05/11/2025

Reviewers [	Role	Approval date
Policies Review Group: Peter Knight John Thurkettle Anna Stephenson Joanne Withey Nigel Inniss Corporate Information Governance Board - ratification	 Head of Information Governance IT Security Manager DPO & Compliance Manager DP & Training Manager SIRO	See above

Publication information

	Published (if YES, enter document location)?	**Location**
All staff	Yes	IRIS
Public	Yes	SCC website

1. **Introduction**

The purpose of this policy is to ensure:

a) That all information security incidents within scope of the policy are reported and handled consistently, and that resources are applied with due regard to relative impact and severity.

b) That all staff understand the difference between information security incidents and personal data breaches.

c) That reports and investigations are carried out when necessary, and that statistical and other analysis is presented to senior managers, governance bodies and the Corporate Leadership Team in a meaningful way so that security issues can be prioritised and addressed.

d) Finally, that SCC discharges its obligation to report, in a timely way, information security incidents which come within the compass of data protection and other legislation. Security incident data will be made available to the public.

e) This policy should be read in conjunction with the following policies and guidance:

- Artificial Intelligence (AI)
- Data Protection
- Acceptable Use of Information and Systems
- Information Security
- Records Management
- SCC Information Classification Guidance (see Appendix A below)

2. Scope

a) This policy applies to SCC employees, elected Members (Councillors), any partners, voluntary groups, third parties and agents who SCC employees have authorised to access ICT, including contractors and vendors with access to ICT systems. For the purposes of this policy all these individuals are referred to as ‘user’ or ‘users’.

b) The policy covers all types of information - written, spoken and computer information - and where something has occurred which has created an impact on the confidentiality, integrity and availability of that information.

c) All suppliers and contracted third parties who provide services to SCC shall undertake to follow the policy particularly reporting of incidents within the agreed timescale.

3. Roles and responsibilities

a) **Implementation and Monitoring of Policy:** the Information Governance Team has been tasked to implement this policy and monitor its effectiveness.

b) **Managers:** are responsible for ensuring that adequate induction and training is undertaken by staff and that support is provided to them in relation to implementing this policy. Managers are also responsible for conducting investigations, reporting outcomes when requested to by SIAs, and ensuring that staff read and understand any updated guidance and/or communications, see paragraph (e) below. It is the responsibility of managers to inform senior managers and, if appropriate, relevant members (Councillors), of any significant security incidents.

c) **Strategic Information Agents (SIAs):** are responsible for liaising with the Information Governance team and coordinating service investigations into information security incidents.

d) **Monitoring Officer**: is responsible for ensuring that adequate induction and training is undertaken by Councillors and that support is provided to them in relation to implementing this policy.

e) **Corporate Information Governance Board (CIGB):** receives a monitoring report on information security incidents every six months. Members of the CIGB are expected to share this information with senior managers in their respective directorates or service areas.

f) **Users**: SCC delivers modular training to all users who have access to the Council's data and network. These training modules inform users of the requirements of the IT Security Policies. All users must engage with this training and complete all mandatory modules. Line managers have a responsibility to support this training and must raise with HR if any staff member does not or cannot complete the training.

   All users who may be involved in an information security incident must cooperate with any investigation requirements into that incident.

   All users are responsible for keeping up to date with any guidance and/or communications which may be circulated via internal newsletters (e.g. InsideSCC), the intranet (e.g. the Information Governance pages), or other bulletins.

g) **Non-compliance with this policy** could warrant further action and investigation under the Council's Disciplinary Procedures. In certain circumstances, breach of this policy may be considered gross misconduct resulting in dismissal.

   Councillors found to be in breach of this policy may be deemed to be non-compliant with the Members' Code of Conduct which may lead to a referral to the Council's Monitoring Officer.

h) **Security incidents** - users must report all suspected security incidents via IT Self Service *'Report an Incident'* as soon as they become aware that one may have occurred. Incidents can be reported by any user who has discovered an information security incident.

4. **Incident reporting**

a) All incidents must be reported via IT Self Service *'Report an* Incident'.

b) Information security incident defines an incident that affects the security of any SCC data, including personal and non-personal.

c) Personal data breach is as defined under the UK GDPR as being any information security incident which result in:

i. Accidental or deliberate loss or destruction of personal data; or
ii. Sharing with or access by any unauthorised party to personal data

d) If any user becomes aware of an incident that has not been reported, they must report it via IT Self Service without delay.

e) The incidents will be graded by the Information Governance team using the grading below so that the right level of resource can be applied.

5. **Grading by impact**

1. NEGLIGIBLE

Any type of incident formally recorded (e.g. on the IT reporting system), or something worthy of investigation but turns out to be a 'false positive', 'near miss' or loss of equipment where there is a remote chance of the data being readable, which has negligible impact on privacy or services.

Reporting of such incidents is still valuable and should be used as part of ongoing information security risk assessment.

2. MINOR

Confirmed or likely loss of personal data or other privacy breach relating to up to 10 individuals that poses low risk to privacy and no health or safety impacts (e.g. just name, address, customer number at AMBER level[1]).

Confirmed or likely issues relating to integrity of information on <10 staff or customers such as confused identities, out of date information or records misplaced which causes localised

[1] See Appendix A for description of information classification.

inconvenience or delays.

Some localised and short-lived loss of availability, such as through a temporary systems failure, which leads to the disruption of non-critical services.

3. MODERATE

Confirmed or likely loss of personal data or privacy breach relating to more than 10 individuals OR any breach of OFFICIAL- SENSITVE information at 'red' level*. Likely local media interest and adverse publicity.

Issues relating to integrity of information to the extent that the data can no longer be understood or is out of date and could have health, social care and safety or other service implications.

Some disruption to critical services that means information is unavailable causing unacceptable impact and invocation of localised business continuity plans. This may be either a short disruption to a very critical service or a longer disruption
to a group of less critical services.

4. MAJOR

Confirmed or likely loss of personal data or privacy breach relating to more than 100 individuals OR loss of any sensitive personal data RED which is highly likely to affect the health or safety of one or more individuals. OR any privacy breach which because of the high profile nature of the person(s) affected or other circumstances is likely to lead to national media attention and cause significant reputational damage.

An integrity issue which means data relating to 100+ staff or customers is in effect no longer usable or understandable (and cannot be rectified) and is likely to impact health, and safety or key services.

Sustained loss of availability of information which has serious impact on delivery on the delivery of a number of critical services, resulting in business continuity plans being invoked for at least one business area.

5. EXTREME

Loss of data or privacy breach relating at large scale (i.e. 100,000+ persons or datasets on potentially all customers in Suffolk); likely national/international media adverse publicity, prolonged damage employee/customer trust and could lead to consequences to large numbers of individuals such as identity theft, financial loss etc.

Integrity problem which leads to significant amounts of data on

100,000+ persons being unreadable or unusable and does directly lead to health and safety issues or significant services issues (e.g. entire data set for customer group corrupted beyond use that must be re-created).

Outage or other issue which leads to general failure of IT so that applications/services which are critical to the business are not running for a prolonged period. Business Continuity Plans across SCC are invoked.

6. **Logging security incidents**

SCC provides a central process for handling information security incidents in a consistent manner. It will also ensure that any requirements of data protection law are adhered to, particularly the reporting of incidents that result in a breach of personal data to the Information Commissioner (IC) within the required 72 hours timescale, where appropriate.

7. **Business Continuity**

The Information Governance team will work with those tasked with IT, business continuity, and with external bodies such as Police, National Cyber Security Centre and elsewhere as necessary.

8. **Investigations**

Incident investigations shall be carried out with due regard to impact/severity. This may include Internal Audit and/or external audit involvement. All users who may be involved in an information security incident must cooperate with any investigation requirements into that incident.

9. **Feedback on incidents**

Formal feedback on information security incidents will be provided to relevant governance structures regularly (no less than twice a year) and to the Corporate Leadership Team at least annually.

APPENDIX A

SCC Information Classification Guidance

The purpose of this guidance is to classify all written, spoken and technological information by its sensitivity so that you can decide the appropriate measures you need to take to protect it.

SCC uses a traffic light rating system (i.e. Red, Amber, Green) to identify the sensitivity of its information. Please see the table below for information to help you classify the data you are working with:

SCC classification levels	Definition	Examples of information
RED	Information which poses high risk to privacy. This could include: information about an individual's ethnicity • political opinions • religious or philosophical beliefs • trade union membership • genetic data • biometric data where it is used to identify people • sex life and sexual orientation • gender reassignment • criminal offence data • health information	• Health & Social Care records • Financial information • Employee data • Health, safety and wellbeing • Corporate information e.g. information which would have a significant impact on the reputation or business of SCC
AMBER	Information which poses little or no risk to an individual's privacy. **N.B.** It should be noted that if the information is contained within a RED level document, or if you are using large volumes	• Business contact information including email addresses, postal addresses and phone numbers • Customer names and addresses

	of AMBER level data, it should be treated as RED level data – see above	• Unique identifiers such as NHS numbers, NI numbers, case management system ID numbers, e.g. Liquid Logic
GREEN	Information which poses no risk to privacy	• Information that would be disclosed under a Freedom of Information (FOI) or Environmental Information (EIR) request • Information that is routinely published, e.g. staff salaries, statements of accounts, Cabinet meeting minutes