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.

Owner: SIRO
Document ID: ICT-PL-0109
Version: 1.3
Date: March 2021
Review date: March 2023

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

Accountable Owner		Approval date
Senior Information Risk Owner (SIRO)	Chris Bally	05/07/2021

Responsible Owner		Approval date
Head of Information Governance	Peter Knight	21/04/2021

Reviewers [	Role	Approval date
Policies Review Group: Russell Armstrong Philip Barbrook Anna Stephenson Joanne Withey (policy review lead) Corporate Information Governance Board - ratification	 IT Security Manager Enterprise Architect DPO & Compliance Manager DP & Training Manager	18/05/2021 29/07/2021

Publication information		
	Published (if YES, enter document location)?	**Location**
All staff	Yes	mySCC
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 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.

c) 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.

d) This policy should be read in conjunction with the following policies:

- Data Protection
- Acceptable Use of Information Systems
- Information Classification & Labelling
- Records Management

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 and reporting outcomes when requested to by SIAs.

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) **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 ICT 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.

f) **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.

g) **Security incidents** - users must report all suspected security incidents to 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**

All incidents must be reported via IT Self Service *'Report an* Incident' as soon as they become aware that one may have occurred.

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

5. **Grading by impact:** C=Confidentiality I=Integrity A=Availability

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 C - 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]). I - 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 inconvenience or delays. A - 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 C - 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. I - 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. A – 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 C – 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

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

nature of the person(s) affected or other circumstances is likely to lead to national media attention and cause significant reputational damage. I – 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. A – 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 C – 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. I – 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). A – 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 will provide a central team tasked with logging and handling information security incidents in a consistent manner using the grading schema. It will also ensure that any requirements of data protection law are adhered to, particularly the reporting of breaches of personal data within the required timescale.

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 scheme

CLASSIFICATION	DESCRIPTION OF INFORMATION TYPES
GREEN	No Impact - Information formally made public by SCC or information which would have no impact on privacy, business, or corporate reputation if it was to be put into the public domain by any other means.
AMBER	Strictly internal or agreed partners - SCC corporate information which is intended strictly for internal use by staff and agreed partners.
	Information posing little/no risk to privacy - This could also include customer names, addresses and client numbers that pose little or no risk to privacy.
RED OFFICIAL-SENSITIVE	Health & care personal data - personal data which reveals anything about the health or care arrangements of any individuals or families. This includes details about ethnicity. gender reassignment, marriage and civil partnership, pregnancy and maternity, race, religion or belief, sex, and sexual orientation.
	Financial personal data - personal data which reveals anything about the financial circumstances of any individuals or families
	Employee & partner personal data - personal data on employees of SCC and its partners. This includes details about ethnicity. gender reassignment, marriage and civil partnership, pregnancy and maternity, race, religion or belief, sex, and sexual orientation.
	Impact on health, safety & wellbeing - anything which, if disclosed, would impact on the health, safety and wellbeing of people. This includes details about ethnicity, gender or sexuality.
	Corporate information which would have a significant impact on the reputation or business of SCC it is was seen by non-intended recipient because of commercial, legal, fraud, investigatory or areas where confidentiality is necessary.

	Special category data as defined under data protection law (UK GDPR and DPA 2018) i.e. personal data revealing **racial or ethnic origin;** personal data revealing **political opinions;** personal data revealing **religious or philosophical beliefs;** personal data revealing **trade union membership;** **genetic data;** **biometric data** (where used for identification purposes); data concerning **health;** data concerning a person's **sex life**; and data concerning a person's **sexual orientation.** Note: personal data about criminal allegations, proceedings or convictions falls under separate legislation but is classified as red level data.