Information Security 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-0006
Version: 2.0
Date: March 2021
Review date: March 2023

DOCUMENT MANAGEMENT

Version	Date	Summary of Changes
1.0	October 2018	Insertion of initial text into template format
2.0	March 2021	Review and Updates

Accountable Owner		Approval date
Senior Information Risk Owner (SIRO)	Chris Bally	02/07/2021

Responsible Owner		Approval date
Head of Information Governance	Peter Knight	18/05/2021

Reviewers	Role	Approval date
Policies Review Group: Russell Armstrong Philip Barbrook Anna Stephenson Joanne Withey 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	Intranet - mySCC
Public	Yes	SCC website

1. Introduction

a) This document sets out how Suffolk County Council (SCC) ensures that its information is secured and how information risks are managed.

b) The SCC *Our Information, Our Priorities* framework sets out how the use and management of information and data supports SCC's overall priorities of inclusive growth, health, care and wellbeing, and efficient and effective public services.

c) This policy supports Objective 3 of the *Our Information, Our Priorities* framework, namely: "**Getting security & data protection right for the level of risk**".

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

- Our information, Our Priorities (ICT-PL-0118)
- Data Protection Policy (ICT-PL-0099)
- Law Enforcement Data Protection Policy (ICT-PL-0016)
- Classification and Labelling of Information Policy (ICT-PL-0111)
- Staff Acceptable Use of Information Systems Policy (ICT-PL-0117)
- Security Incident Reporting and Management Policy (ICT-PL-0109)
- Records Management and Information Handling Policy (ICT-PL-0098)

2. Scope

a) This policy applies to all risks relating to the confidentiality, integrity, and availability of written, spoken and computer information for SCC as a legal entity. Given the complexity of the Council's partnerships with other local authorities, schools, NHS organisations and other organisations, it is essential to define and review at regular intervals the scope of the overall security policy and the information security management arrangements as this has an important bearing on risk acceptance, transfer and liability.

b) This policy does not apply to divested and partner organisations and schools[1]. These organisations will need to put in place their own overarching security policies and understand their own individual security requirements and liabilities (e.g. a school procuring and running its own ICT services and therefore responsible for managing its own information risks).

c) Organisations not listed and out of scope may still be required to adhere to certain SCC sub-security policies to avail of services (e.g. network, email etc.) but will still be responsible for carrying out their own information assurance.

d) Being in or out of scope of the SCC information security policy does not have any automatic bearing on controllership as defined by data protection law. All

[1] Divested organisations (whose functions once formed part of SCC) are responsible for own information security policy.

legal entities have a responsibility to be clear on their liabilities as controllers/processors regardless of which security policies they adhere to.

e) Where two or more separate legal entities (e.g. councils) enter a joint service agreement it must be established which of the parties' Information Security Policy will be followed or where new policy and procedures need to be put in place.

3. Responsibilities

The following roles are responsible for ensuring compliance with this policy:

a) **SIRO**: this role is fulfilled by the Deputy Chief Executive and Director of Corporate Services who is the accountable owner of this policy.

b) The **Information Governance Team** is tasked with implementing this policy and monitoring its effectiveness.

c) **Managers** are responsible for ensuring that adequate induction and training is undertaken by staff and that support is provided to them where they are processing law enforcement personal data. Non-compliance with this policy

d) **The 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 this policy.

e) All **users** should attend the appropriate training courses relevant to their role in the organisation. 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, such as the 'Keeping Information Safe (Our Information, Our Responsibilities)' Information Security course. 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.

4. Non-compliance with this policy

a) Non-compliance with this policy may lead to further action and investigation under the council's disciplinary procedures. In certain circumstances, failure to comply with this policy may be considered gross misconduct resulting in dismissal.

b) Non-compliance with this policy could also lead to criminal or civil action if illegal activities are involved or legislation is contravened. SCC will not hesitate to bring to the attention of the appropriate authorities any use of its systems which it believes might be illegal.

c) Failure by councillors to comply with this policy may contravene the Members' Code of Conduct and could lead to a referral to the Council's Monitoring Officer.

d) **Security incident management**: All staff must report suspected security incidents via IT Self Service 'Report an Incident' as soon as possible after being made aware that one may have occurred.

5. Leadership and commitment

a) The Chief Executive Officer and Corporate Leadership Team (CLT) shall demonstrate leadership and commitment with respect to information security management by ensuring that the SCC Information Security Policy is compatible with the strategic direction of council and within the law, for example by:

i. Establishing high-level information security objectives for the organisation and reviewing these at regular intervals.

ii. Designing, implementing and continually improving council-wide information security management arrangements that integrate relevant functions of the organisation such as Information Management, IT, Property, business continuity, HR and internal audit.

iii. Ensuring that the resources needed for the effective operation of the Council's information security management arrangements are available and supported by the CLT.

iv. Assigning the role of Senior Information Risk Owner (SIRO) at executive-level to ensure the above is undertaken and performance is reviewed and reported to the CLT at regular intervals.

v. Delegating responsibility for the development of relevant policies, processes and procedures, and monitoring their effectiveness, to the council's Corporate Information Governance Board.

vi. Ensuring that the information security policy and objectives are communicated to all staff, business partners and the wider public to ensure that trust and confidence is maintained statutory and other functions of SCC.

6. Planning

a) Having established the contours of the SCC information security management arrangements - where responsibility begins and ends for the CLT and cognisant of all interested parties - SCC will:

i. Establish the factors that provide opportunities for the setting up and running of the information security management arrangements and ensure that these are exploited - e.g. mature risk management processes in finance or existing ICT staff trained in ITIL or other methodology using documented processes.

ii. Establish the risks that may prevent the information security management arrangements from being established, working as intended and able to achieve continual improvement - e.g. lack of staff resourcing, cultural issues, and organisational structure that has grown up organically or other factors that would impact detrimentally on the Council's information security management arrangements.

iii. Consider how far the information security management arrangements will work across relevant Council functions - e.g. Information Governance, IT, Internal Audit, Legal etc.

iv. Act to address the above at CLT level.

7. Security personnel resources

a) After planning and review the CLT shall determine and provide the resources needed for the establishment and continual improvement of the Council's information security management arrangements:

i. Be clear that roles in information security are part of a professional specialist discipline and career home and not a generalist administration role.

ii. As a minimum there should be a designated permanent role, or roles, that encompass all information risks (not just 'IT security') and are of appropriate grade and standing.

iii. The permanent role of Data Protection Officer will be filled to carry out the responsibilities as set out in data protection law for SCC as controller.

iv. The appointed person(s) shall be competent and have the necessary specialist training and experience.

v. To provide ongoing training and support for information security personnel e.g. resource to gain necessary professional accreditation and qualifications and for this to be documented).

vi. To ensure that security personnel participate fully in SCC governance structures and fora.

8. Staff awareness and communications

a) The CLT shall put in place the means to conduct internal and external communications and awareness relevant to its information security management arrangements. The outcomes should be:

   i. The SCC Information Security Policy and associated guidance should be freely available to all employees via the corporate Intranet (mySCC), to interested parties and the wider public via the website;

   ii. There is a form of mandatory induction – currently called 'Keeping Information Safe (Our Information, Our Responsibilities)' - on information security/data protection for all personnel who are within scope of the Policy, and that this is followed;

   iii. There is a process to enable information security updates, advice and other content to be available or communicated to relevant audiences in a timely manner.

9. Information Risk Assessment

a) SCC shall identify key assets and their owners and document in a high-level Register of Datasets (Information Asset Register) following an agreed standard template. Impacts on assets must be assessed in terms of the confidentiality, integrity and availability.

b) SCC shall use a standard information security risk assessment template and associated process and impact levels. This will ensure that repeated information security risk assessments produce consistent valid and comparable results across all directorates and business units. In particular:

   i. The business context must be fully understood prior to assessment

   ii. Risk owners, and owners of assets must be identified

   iii. Plausible worst-case scenarios and business impact must be understood and documented – using a standardised 1-5 scale – if overall risks to confidentiality, integrity and availability materialise

   iv. Vulnerabilities and likelihood must be assessed

   v. Overall risk analysis must use the criteria above.

   vi. Analysed risks must be prioritised and summarised into a format that can be easily understood by risk owners to agree subsequent risk treatment plans.

c) SCC shall perform information security risk assessments at planned intervals when significant changes are proposed to occur or where recommended in

wake of significant information security incidents, or required as part of a Data Protection Impact Assessment. Such assessments can be at organisational-level, function, project or service level.

d) Where an information security risk is deemed to be of high significance, this risk should be considered for inclusion on the council's Corporate Risk Register by the risk owner. Any information security risks included on the Register should be monitored and updated in accordance with the agreed overall approach to management of the Corporate Risk Register.

10. Information security risk resolution

a) SCC must define and use consistently an information risk treatment process that:

i. Selects appropriate information security risk resolutions in response to information risk assessment results.

ii. Determines all the controls that are necessary to implement the information security resolutions.

iii. Ensures that all relevant mandatory controls and standards are implemented in regard to codes of connection and compliance with external bodies such as PCI Security Standards Council and NHS Digital network connectivity of information governance unless agreed otherwise.

iv. Ensures that significant incidents are reported as per policy so that lessons learned reports feed into resolution plans.

v. Have the capability to produce a statement of applicability on demand that contains the necessary controls and justifications for any exclusions and whether implemented.

vi. Have the capability to formulate information risk resolution plans as required.

vii. Obtains the risk owners' formal approval of information security risk resolution plans and acceptance of the residual information security risks.

viii. SCC to formally security accredit its key services and review on an annual basis.

ix. Where non-SCC organisations and suppliers are involved, SCC must seek agreement on which party is responsible for discharging the different components of the resolution.

b) SCC must implement the agreed information security resolutions and retain documentary evidence.

11. Monitoring arrangements

a) SCC shall routinely evaluate the effectiveness of the information security management arrangements and to be clear about:

   i. What is to be monitored and measured including security processes, controls and analysis of incidents

   ii. The methods for evaluating so that there are comparable and reproducible results

   iii. The personnel who undertake the evaluation and how communicated to the SIRO so that any necessary action may be taken.

12. Internal Audit

a) In addition to the above, SCC shall conduct internal audits at planned intervals that provide information on whether the information security management arrangements conform to the requirements as planned and implemented. The audit shall:

   i. Work according to an agreed frequency (e.g. annual).

   ii. Define the scope of the audit and criteria.

   iii. Persons carrying out the audits are qualified, objective and impartial.

   iv. Such an audit can be incorporated into the internal audit function covering other areas.

13. Management review and improvement

a) The SIRO, in conjunction with the Corporate Information Governance Board, should review the SCC information security management arrangements at planned intervals to ensure its continuing suitability and effectiveness. This will be measured against the overall information security objectives.

b) Escalation of issues to the Corporate Leadership Team should be undertaken by the SIRO if required. Such a review will include consideration of:

   i. Status of actions from previous management reviews

   ii. Changes in external and internal issues which are relevant

iii. Non-conformities and preventative/corrective actions

iv. Monitoring and measurement of results

v. Audit results

vi. Results of high level or key risk assessment and risk resolution plans

vii. Feedback from interested parties including customer groups in Suffolk

viii. Significant security incident reports impacting on SCC or relevant incidents reports from elsewhere.

c) The outputs of the management review shall include decisions related to the continual improvement, opportunities and any changes needed to the information security management system.

d) The CLT, acting through the CEO and SIRO, will react when major non-conformity occurs, over and above any regular audit and management review, and act to deal with it including agreeing changes to the Council's information security management arrangements.

e) SCC recognises the circular nature of information security management: to plan, action, check and plan again to make continual improvement.

14. **Documentation**

a) SCC shall hold documented information relating to the design and effective running of its information security management arrangements:

i. To be held in a digital format in the approved corporate records management system.

ii. For information relating to the arrangements to be held as one or more discrete functions within a file plan/business classification scheme and managed according to SCC records disposal and retention schedules.

iii. To be easily accessible to persons requiring them to support the smooth running of the information security management arrangements and auditors, kept up to date and subject to the security and access permissions commensurate with the sensitivity.