Suffolk
County Council

# Information Security Policy

| | |
|---|---|
| Document Owner | : Senior Information Risk Owner |
| Version | : 2.2 |
| Date | : August 2016 |
| Document ID | : ICT-PL-0006 |

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

## DOCUMENT CONTROL

### Changes History

| Issue No | Date | Amended By | Summary of Changes |
|---|---|---|---|
| 1.2 | April 2013 | Stephen Carr | Minor amendments for Annual Review |
| 1.3 | June 2014 | Neal Scarff | Amendments for Annual Review |
| 1.4 | August 2014 | Neal Scarff | Amendments for SIRO change |
| 2.0 | September 2014 | Philip Barbrook | Amendment to scope in information risk governance |
| 2.1 | July 2015 | Neal Scarff | Minor amendments for Annual Review |
| 2.2 | August 2016 | Russell Armstrong | Minor amendments. Removed ISO 27001 from Section 3.3 and replaced with Cyber Essentials, PSN, PCI & "10 Steps to Cyber Security". Added Tablets to information security assets in section 8.1. |

### Authorisation (Responsible Owner)

| Role | Name | Approval Date |
|---|---|---|
| Head of Performance and Information Management | Peter Knight | August 2016 |

### Approval (Accountable Owner)

| Role | Name | Approval Date |
|---|---|---|
| Senior Information Risk Owner | Chris Bally | August 2016 |

### Reviewers (Consulted)

| Role & Review Responsibilities | Name | Approval Date |
|---|---|---|
| Enterprise Architect | Philip Barbrook | August 2016 |
| Policy & Compliance Manager | Neal Scarff | August 2016 |
| IT Security Officer | Russell Armstrong | August 2016 |

### Distribution List - Once authorised (Informed)

| Name | Organisation |
|---|---|
| All Users | See Section 2 of the Policy |

### Review Period

| Date Document to be Reviewed | By whom |
|---|---|
| August 2017 | Head of Information Management |

## TABLE OF CONTENTS

## 1 WHY DO WE NEED AN INFORMATION SECURITY POLICY?

1.1 Suffolk County Council (SCC) is committed to preserving the confidentiality, integrity and availability of all the physical and information assets throughout the Council and will use all reasonable, appropriate, practical and effective security measures to protect the important business processes and assets in order to protect the information it holds, processes and stores.

1.2 SCC holds and processes personal information about the people of Suffolk, including the people who work with and on behalf of the Council. Information is received from many sources, including other public agencies and is also produced as part of providing day to day services. Information is a valuable Council asset and is used as the knowledge and evidence base for all Council plans, strategies and decisions. It includes all communications internally and externally with residents and partners as well as information about customers and service users.

1.3 Information security requirements will be aligned with organisational goals and other policies. These are intended to enable information sharing and for reducing information-related risks to acceptable levels.

1.4 SCC will ensure any deliberate act to jeopardise the security of information that is held, managed or stored by the Council will be subject to disciplinary and/or legal action as appropriate.

## 2 SCOPE

2.1 This policy statement applies to everyone who undertakes duties on behalf of the Council including councillors and applies to information which is either, printed or written on paper, stored electronically, shown on films or spoken in conversation (including phone recordings and taped interviews) and all devices, systems and networks used to manage and store information.

2.2 The Council's current service planning and risk management framework provide the context for identifying, assessing, evaluating and controlling information-related risks through the establishment and maintenance of an Information Security Management System (ISMS). The risk assessment statement and the risk treatment plan identify how information related risks are controlled. The Senior Information Risk Owner (SIRO) is responsible for the maintenance of the risk treatment plan.

2.3 In particular, business continuity and contingency plans, data back-up procedures, avoidance of malware and cyber threat actors, authorised access control to systems and information security incident reporting are fundamental to this policy. Control objectives for all of these areas are contained in the Manual and are supported by specific, documented policies and procedures.

2.4 Information Security Polices are subject to continuous systematic review and improvement.

2.5 For further advice on this policy, please contact your department's Strategic Information Agent, or Performance & Information Management.

## 3 POLICY STATEMENT

3.1 SCC will apply the National Archive's Principles of Information[1] which have been developed to provide high-level guidance for managing information within the public sector. The principles apply to all information that is created, collected, held, used, shared, transformed, published or processed by SCC and covers both structured and unstructured information, and information at all stages of its lifecycle. The protection of information assets will be appropriate and cost effective.

3.2 The Council has a top level Information Governance Board (IGB), responsible for advising on Information Management policy, co-ordinating Information Risk management and programme level governance for information risk projects. It is chaired by the Senior Information Risk Owner and includes the Head of Information Management, the Council's Caldicott Guardian(s), Senior Directorate Information Asset Owners and the Policy & Compliance Manager. The board will report to the Corporate Management Team (CMT), raising risk and issues of a corporate nature. The IGB will have an agreed Terms of Reference.

3.3 SCC will adhere to the Cyber Essentials, "10 Steps to Cyber Security (CESG)", PSN framework & PCI DSS Data Security Standards as their core frameworks for guiding the approach to managing information security and protecting the confidentiality, integrity and availability of information assets and business processes.

3.4 SCC will publish an 'information charter', detailing its approach to information management in terms of maximising the public benefit and how better use could be made of the Council's information assets.

## 4 RESPONSIBILITIES

4.1 Everyone undertaking duties on behalf of the Council, including councillors are responsible for protecting and managing information securely and reporting security incidents and identified weaknesses and must comply with this policy.

4.2 All line managers are responsible for ensuring that employees and anyone undertaking duties on behalf of the Council adhere to all information policies, standards and procedures and undertake annual training when dealing with sensitive information. This must be monitored and logged by the line manager.

[1] http://www.nationalarchives.gov.uk/information-management/manage-information/planning/information-principles/

4.3 The Chief Information Officer (CIO) is responsible for approving information and IT policy decisions and the policy updates that result. The CIO is also acting as the Senior Information Risk Owner (SIRO) role, on a day to day basis, delegated from the Director of Resource Management (Section 151 Officer of the Council).

4.4 The Information Governance Board (IGB) are responsible for feeding in the organisational view into the development and approval of all information policies and standards. The IGB is also the co-ordination group for facilitating management of, and escalation to CMT if required, Corporate Information Risks. The SIRO will formally chair the IGB, and it will represent all Information Asset Owners (IAO) in the Council.

4.5 The Head of Information Management is responsible for updating all information policies, standards and procedure and ensuring they go through the governance process; managing the Information Governance Board and co-ordinating information out to all relevant parties.

4.6 The ICT-QA-0001 IT Quality Manual lays out the responsibilities for updating the IT policies, standards and procedures. The Policy & Compliance Manager is responsible for ensuring that they go through the governance process and for co-ordinating information out to all relevant parties.

## 5 APPLICABLE CONTROLS AND REFERENCES FOR AUDIT PURPOSES

- Public Services Network (PSN) Information Assurance Conditions
- NHS N3 IGSOC and IGTOOLKIT conditions
- Payment Card Industry Data Security Standard (PCI-DSS) statement of compliance
- Ministry of Justice statements of compliance
- Council Data sharing agreements and related memorandum of understanding (MoU)
- Risk assessment statements and associated risk treatment plans

## 6 REVIEW OF THE INFORMATION SECURITY POLICY

6.1 The Section 151 Officer is the Owner of the Information Security Policy and has approved management responsibility to the CIO, as SIRO, for the development, review and evaluation of the policy.

6.2 The Organisation has a defined procedure for the management review of the Information Security Policy, and this includes continuous improvement, and assessing policy changes that might be necessary in response to significant changes in the organisational environment, business circumstances, legal conditions or technical environment.

6.3 All changes to this Information Security Policy are subject to approval by the SIRO and Section 151 Officer.

6.4 This policy will be reviewed annually to respond to any changes in the risk assessment or risk treatment plan.

## 7 APPROVAL

A current version of this document is available to all members of staff on the Council Intranet. It does not contain confidential information and can be released to relevant external parties.

| | |
|---|---|
| Signature | Signature |
| ........................................ | ........................................ |
| Name | Name |
| GEOFF DOBSON | CHRIS BALLY |
| Director of Resource Management<br>(Section 151 Officer) | Senior Information Risk Owner (SIRO) |
| Date 5/9/2016 | Date 31/8/2016 |

# 8 DEFINITIONS

## 8.1 Information Security

In this policy, “information security” is defined as *‘Preserving the confidentiality, integrity and availability of all the physical and information assets of the Council’*:

***Preserving***

This means that management, all full time or part time staff, sub-contractors, project consultants and any external parties have, and will be made aware of, their responsibilities (which are defined in their job descriptions or contracts) to preserve information security, to report security breaches (in line with the policy and procedures identified in the Council’s Information Security Incident Management Policy & Procedure) and to act in accordance with the requirements of the ISMS. The consequences of security policy violations are described in the Council’s Human Resources policies. All staff will receive information security awareness training and more specialised staff will receive appropriately specialised information security training.

***The confidentiality,***

This involves ensuring that information is only accessible to those authorised to access it and therefore to preventing both deliberate and accidental unauthorised access to the Council’s information and proprietary knowledge and its systems including its networks, websites, extranets, and e-commerce systems.

***Integrity***

This involves safeguarding the accuracy and completeness of information and processing methods and therefore requires preventing deliberate or accidental, partial or complete, destruction, or unauthorised modification, of either physical assets or electronic data. There must be appropriate contingency arrangements for networks, e-commerce systems, web sites, extranets and data back-up plans, and security incident reporting. The Council must comply with all relevant data-related legislation.

***And availability***

This means that information and associated assets should be accessible to authorised users when required and therefore physically secure. The Council’s IT network must be resilient and the Council must be able to detect and respond rapidly to incidents (such as viruses and other malware) that threaten the continued availability of assets, systems and information. There must be appropriate business continuity plans in place.

***Of all the physical (assets)***

The physical assets of the Council including but not limited to computer hardware, data cabling, telephone systems, filing systems and physical data files.

***And information assets***

The information assets include information printed or written on paper, transmitted by post or shown in films, or spoken in conversation, as well as information stored electronically on servers, web site(s), extranet(s), intranet(s), PCs, laptops, mobile phones, tablets and PDAs as well as on CD ROMs, floppy disks, USB sticks, back-ups and any other digital or magnetic media, and information transmitted electronically by any means. In this context "data" also includes the sets of instructions that tell the system(s) how to manipulate information (i.e. the software: operating systems, applications, utilities, etc.).

***Of the Council***
The Council and its partners that use the Council's IT network, who have signed up to this security policy and have accepted the Council's ISMS.

### 8.2 ISMS

The ISMS is the Information Security Management System, of which this policy, the information security manual ("the Manual") and other supporting and related documentation is a part, and which has been designed in accordance with the specification contained in BS 7799:2-2005

### 8.3 Security Breach

A Security Breach is any incident or activity that causes, or may cause a break down in the availability, confidentiality or integrity of the physical or electronic information assets of the Council. Reporting of Security Breaches is described in the Acceptable Use of ICT Policy and the Security Breach Reporting Process.

### 8.4 Senior Information Risk Owner (SIRO)

This is the board level executive with particular responsibility for information risk.