INFORMATION CLASSIFICATION AND LABELLING 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-0111
Version: 1.4
Date: October 2023
Review date: October 2025

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	October 2023	Review

Accountable Owner		Approval date
Head of Information Governance	Peter Knight	08/12/2023
Senior Information Risk Owner (SIRO)	Chris Bally	05/07/2021

Responsible Owner		Approval date
DPO + Compliance Manager	Anna Stephenson	04/12/2023
Head of Information Governance	Peter Knight	08/12/2023

Reviewers	Role	Approval date
Policies Review Group: Russell Armstrong Philip Barbrook Anna Stephenson (policy review lead) 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	mySCC
Public	Yes	SCC website

1. **Introduction**

a) The purpose of this policy is to classify all written, spoken and technological information by its sensitivity so that controls can be deployed, and business decisions made to manage the risks effectively.

b) This policy relates solely to classification based on sensitivity and impact of information risks occurring and not on business value or any other measure (e.g. there can be SCC information that has no sensitivity but has great business value and vice versa).

c) SCC is a large and complex statutory public body that owns and creates significant amounts of information in all formats (and handles information originating from elsewhere).

d) Classifying information by sensitivity/impact means that the right controls can be put in place where they are most needed. In so doing, there is a need to balance security controls with usability and convenience for the staff who handle the information day-to-day.

e) This policy is designed to mitigate against the likelihood and impact of information risks – including cyber - and is part of the overall information security policy objectives of SCC.

f) All information should be handled appropriately in accordance with SCC policies and procedures and this policy should be read in conjunction with the following policies:

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

2. **Scope**

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

3. **Roles and responsibilities**

a) **Information Governance team**: has been tasked with implementing this policy and monitoring its effectiveness.

b) **Managers**: are responsible for ensuring that adequate induction and training is undertaken by staff and that support is provided to staff in relation to implementing this policy. Managers are also responsible for ensuring that

staff read and understand any updated guidance and/or communications.

c) **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.

d) **Users**: all users should attend the appropriate training courses. 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 and Information 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 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.

   Councillor training will be provided as part of the Councillor's Learning and Development Programme.

e) **Non-compliance with this policy**: non-compliance with this policy by staff 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.

f) **Security incidents**: users must report all suspected breaches of information security via IT Self Service – Report an Incident.

4. The Information Classification Scheme

SCC will classify information as follows (it should be noted that classification is based on sensitivity/impact rather than business value):

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.

CLASSIFICATION	DESCRIPTION OF INFORMATION TYPES
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);

CLASSIFICATION	DESCRIPTION OF INFORMATION TYPES
	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.

5. **Usage**

The SCC classification scheme will be used in the following ways:

Usage	Which staff?
Capturing, filing and sending information internally and externally: Corporate systems/applications - Non-SCC systems/services - Email - Removable media - Telephone - Video conferencing - SMS - Other media/formats Note: SCC does not permit the transfer of data via fax. [With rules on when the above can be used for different classification below]	All staff
Physical and environmental security	Managers in facilities at design phase and ongoing management to segment different rooms/premises by the sensitivity of the information GREEN/AMBER/RED
ICT system/service risk assessment and accreditation and incident reporting	ICT security managers to assess and manage and triage incidents according to sensitivity/impact GREEN/ AMBER/ RED. This then has a bearing on the impact level selected.
Screening of staff prior and during employment	HR department and senior managers deciding on type/level of screening depending on the GREEN/AMBER/RED sensitivity of the information that employees routinely handle in addition

	to whether the persons work with children and vulnerable people.

6. Labelling of SCC owned information

a) All information must be classified, but not all information should be labelled. Labels added manually by the end-user or automatically generated by a digital system for example can be an important additional control that leads to greater awareness of the relative sensitivity of a sub-set of information and can ensure that the right measures are in place. [1]

b) Labels should be used in the following cases:

Usage of labels	**Should a label be applied?**
SCC Information emailed to all **external** agreed business contacts using SCC email service	**Discretionary**[2] A prompt will warn the user prior to sending to non-trusted domains. **Only** where an email contains RED level information, a label of OFFICIAL-SENSITIVE must be added to the title line of the email as per drop-down and instructions.
SCC Information emailed to internal staff using SCC email service	**Discretionary*** **Only** where an email contains RED level information, a label of OFFICIAL-SENSITIVE must be added to the title line of the email as per drop-down and instructions.

[1] The use of labels can be counter-productive if not deployed in the right way or inconsistently applied. Common problems include the use of labels to such a great extent that 'user fatigue' develops (and you no longer really separate out the sensitive from the non-sensitive) and the use of labels that are not understood by external contacts and customers/patients become confused or even alarmed by the label. For this reason, labels should only be mandatory or discretionary in the following stated scenarios:

[2] Although users have discretion, the email service will be configured so as generate warning prompts based on content according to a set of parameters. These are designed to get users to pause, think, and then act.

Usage of labels	Should a label be applied?
SCC digital information filed and managed on SCC official systems by its staff	**Discretionary** **Only** where it is RED level, a label of OFFICIAL–SENSITIVE shall be added to title line of document and file name
SCC paper information filed and managed on in SCC official buildings for records storage	Discretionary **Only** where it is RED level a label of OFFICIAL – SENSITIVE shall be added to the title line of the document or envelope if internal
SCC Information emailed to customers/clients/patients	Do not use labels
SCC Information sent to customers/clients/patients by paper mail	Do not use labels
Removable media	Do not use labels
Telephony/video conferencing/SMS	Do not use labels
Buildings/rooms	Do not use labels

7. **Handling information labelled by non-SCC organisations**

a) The SCC classification scheme has been designed so that it aligns with the UK Government Classification Framework as far as possible.

b) Labelling RED level SCC information as OFFICIAL-SENSITIVE means that any UK Government department or agency or other public body which has adopted the framework (e.g. some Police, local authorities etc.) will understand what this means. And in turn, SCC should understand the equivalent sensitivity if it receives information labelled OFFICIAL-SENSITIVE.

c) Some bodies may also send information to SCC using descriptors e.g. OFFICIAL-SENSITIVE PERSONAL or OFFICIAL-SENSITIVE COMMERCIAL.

d) Individual information sharing agreements should clarify where labels are to be used.

e) Anything received by SCC from an external party should maintain the original OFFICIAL-SENSITIVE label when it is filed into its internal information/records systems.

f) SCC personnel may also receive information which has labels which do not easily equate to anything that is used internally. This can range from ‘NHS CONFIDENTIAL or ‘PATIENT CONFIDENTIAL’ (in the case of NHS)

to labels used by private sector suppliers 'PRIVATE', 'COMPANY CONFIDENTIAL', 'NON-DISCLOSABLE', 'FOI Exempt'. This can be confusing and where information sharing is routine equivalency of labels must be agreed.

g) In the case of suppliers, SCC should insist as part of the contractual process that they follow the SCC classification scheme in regard to the services they are discharging for SCC (e.g. when sending sensitive RED customer data to SCC to use the OFFICIAL-SENSITVE label).

h) Getting suppliers to understand how SCC views relative sensitivity is a critical part of supplier management and where personal data is used under contract, the Data Protection Impact Assessment should capture specific directions in this respect.

8. **Different information service/media types and classification ceiling**

System/service/media	Sensitivity ceiling
SCC internal digital information systems	RED
SCC internal paper record cabinets on premises and limited volumes in agreed home-working scenarios	RED
SCC email	RED
SCC telephones (mobile and fixed)	RED
SCC messaging tools and video conferencing	RED
SCC owned removable media	RED (must seek advice for bulk data transfers)
SCC public facing websites	GREEN
Non-SCC business partner (e.g. Vertas, NHS) owned systems/services	Sensitivity level must be agreed prior to sharing via information sharing agreement/instructions
Employees' own email service	GREEN
Employees' own telephone/video	GREEN
Employees' own paper stores at home	GREEN
Employees' own personal computers/devices/removable media	GREEN
Employees' own 'cloud' or other digital services Note: employees should be storing all SCC information on agreed corporate systems. But in exceptional circumstances the SCC information processed on personal assets must be no higher than GREEN.	GREEN