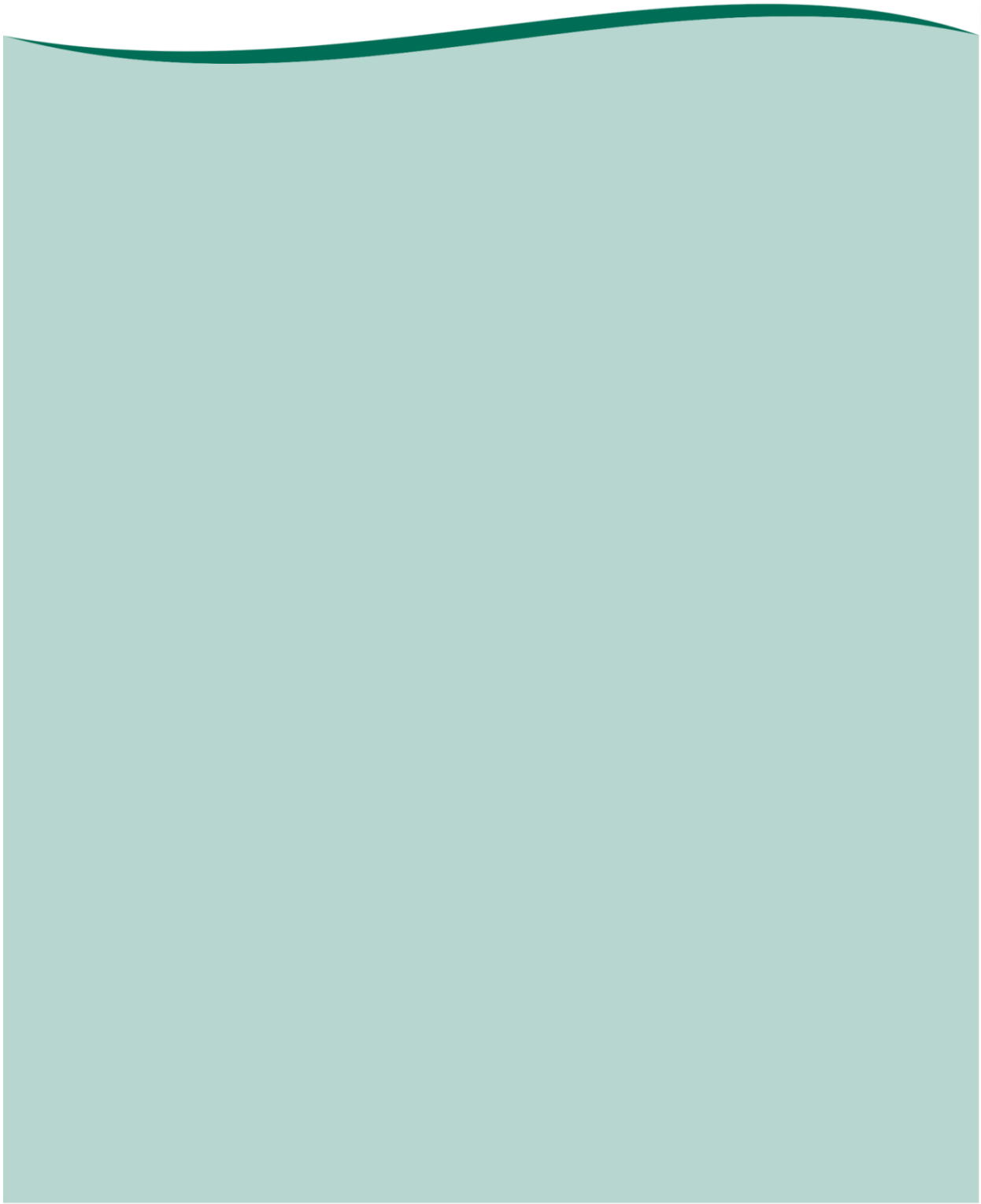
Information Classification Scheme



Document Control

Reference Number	Version 3.0	Status: Published	Sponsor(s)/Author(s) Sarah Davis-Solan, Tim Way
Amendments	Updated to reflect latest Government Classification scheme.		
Document objectives: To provide clear guidance on the information classification scheme in use at Wiltshire Council.			
Intended Recipients: All employees, contractors, and third parties creating and accessing Council information.			
Ratifying Body and Date Ratified	Information Governance Programme Board September 2017		
Date of Issue	September 2017		
Review Date	September 2018		
Contact for Review	Information Governance		
SIRO signature			

Associated Documentation
Policies

- Information Security Policy
- Information Governance Policy
- Information Classification Scheme
- Wiltshire Council privacy policy
- Wiltshire Council data protection policy
- Information Governance Communication and Engagement Strategy
- Guidance notes on safe and secure delivery of personal information
- Information Governance Policy
- Records Management Policy

Legal framework

- Government Classification Scheme
- Data Protection Act 1998

Contents

1 Introduction

1.1.1 Wiltshire Council (the council) needs to collect, store and manage information to provide services and to carry out council business. This information must be accurate, and available to the right people at the right time.

1.1.2 Compromise, loss, or misuse of that information, whether accidental or deliberate can lead to disciplinary or legal sanctions. Protective marking provides a standardised method of classifying our information, to help us to manage and protect it appropriately.

1.1.3 Everyone working for or with the Council has a personal responsibility to protect and manage its information assets. This includes classifying information correctly.

1.2 Government Security Classification (GSC)

1.2.1 GSC is HM Government's administrative system for the secure sharing of information.

1.2.2 The system requires all employees to take personal responsibility for thinking about the security of the information they handle.

1.2.3 The Council policy is in line with GSC guidelines.

2 Purpose

2.1.1 The purpose of this policy is to enable confident use of Protective Marking classifications to ensure that all Council information is created, maintained, shared and protected appropriately.

3 Scope

3.1.1 This policy applies to all information, collected or created by the Council.

4 Classifications

4.1.1 The previously used classifications of PROTECT, RESTRICTED, CONFIDENTIAL, UNCLASSIFIED and NOT PROTECTIVELY MARKED have been replaced with one classification of OFFICIAL.

4.2 OFFICIAL

4.2.1 The OFFICIAL classification includes all routine operational information, including information which could have serious consequences if it was lost, stolen, or published outside of the council.

4.2.2 All information created by the Council will be classed as OFFICIAL. However, within the classification, information must be handled in accordance with the requirements of the law including The Data Protection Act and Freedom of Information Act.

4.2.3 There is no requirement to label OFFICIAL information.

4.3 OFFICIAL-SENSITIVE Caveat

4.3.1 The OFFICIAL-SENSITIVE caveat applies to information which should be managed in a specific way. The caveat should be used when:

a) Compromise, loss, theft or misuse could have a significant impact on an individual, organization, or on council business, AND

b) Where access to the information should be restricted to those who “need to know” (to carry out their role, or to provide required services)

4.3.2 Examples of information where OFFICIAL-SENSITIVE would apply include:

a) Medical records – where not made anonymous

b) Case management files – more specific (i.e. legal, personal care)

4.3.3 OFFICIAL-SENSITIVE Information must be labelled.

4.4 Descriptors

4.4.1 Where information is classed as OFFICIAL-SENSITIVE, descriptors must be applied in the format OFFICIAL-SENSITIVE[DESCRIPTOR] to clarify the type of information and the reason why it is sensitive.

4.4.2 Descriptors include, but are not limited to:

a) Personal

b) Commercial

c) Legal proceedings

d) For publication (time sensitive information)

5 Information Management and Handling instructions

5.1.1 You should always follow council policies for working in an open or hot-desk environment, for working remotely, and for secure transfer of data.

5.1.2 Refer to Appendix 1 for specific information management.

5.2 OFFICIAL-SENSITIVE

5.2.1 Specific handling instructions or restrictions must be clearly stated, along with the classification.

5.2.2 If you are the originator of information classed as OFFICIAL-SENSITIVE, you will need to consider any what handling restrictions apply. Handling instruction include, but are not limited to:

a) Do not share without originator approval

b) Do not edit, copy or share without originator approval

c) Do not email

d) Do not print

e) Restrict to specific audience

5.3 Receiving classified information

5.3.1 If you receive information classified as OFFICIAL-SENSITIVE, you must follow any handling instructions specified by the originator.

5.3.2 You should also, where possible, use the same transmission method as the originator. For example, use secure encrypted email to send information you received via secure email – unless the handling instructions specify that the information must not be forwarded.

6 Responsibility

6.1 All employees

6.1.1 Al employees are responsible for ensuring that the protective marking requirements in this policy are adhered to.

6.1.2 All employees must undertake any protective marking training the Council offers.

6.1.3 All employees should flag up inappropriate management of information to their line manager, or to the Information Governance team where necessary.

6.2 Information originators

6.2.1 Information authors or originators are responsible for classifying their documents in line with this policy.

6.3 Line managers

6.3.1 Line managers are responsible for ensuring that all employees are aware of, and are adhering to this policy.

6.3.2 Line managers are responsible for identifying training needs within their teams.

6.4 Information Asset Owners (IAO)

6.4.1 IAO are responsible for understanding the value, sensitivity and threats to their information assets.

6.5 Information Governance

6.5.1 The Information Governance (IG) team are responsible for reviewing and maintaining this policy and any related policies.

6.5.2 IG will report on compliance, and escalate any issues to the Senior Risk Information Officer (SIRO).

6.6 Retrospective information

6.6.1 There is no requirement to re-classify existing information. Unmarked information should be classified on review.

6.6.2 If information has not been classified, and it is unclear when it was created, it should be treated as OFFICIAL.

6.6.3 Classifications should be reviewed at regular intervals; information sensitivity can change over time.

7 Freedom of Information requests

7.1.1 Where there is a need to contact the originator before sharing information in response to a freedom of Information (FOI) request, this will be carried out by IG.

8 Sharing OFFICIAL-SENSITIVE information

8.1.1 When there is a new requirement to share OFFICIAL-SENSITIVE information internally, the following information should be recorded, and shared with IG:

a) data flow document

b) date of share

c) length of time that information will be shared for

8.1.2 When there is a new requirement to share OFFICIAL-SENSITIVE information externally, the following information should be recorded, and shared with IG:

a) data flow document

b) data sharing agreement, which should include:

i. date of share
ii. length of time that information will be shared for
iii. who the information will be shared with
iv. purpose of sharing

9 Archiving paper records

9.1.1 No need to classify archived paper records.

10 Appendix 1 Information Management instructions

	OFFICIAL	OFFICIAL-SENSITIVE
Document handling	• Document does not require any marking	• Document should be marked OFFICIAL-SENSITIVE top and bottom, and have specific handling instructions listed
Storage	• Adhere to clear desk/screen policy • Keep locked in secure cupboard within council building	• Adhere to clear desk/screen policy • Keep locked in secure cupboard within council building
Remote Working	• Ensure information cannot be overlooked • Lock laptop screen when you are away	• Ensure information cannot be overlooked • Lock laptop screen when you are away
Internal post	• Internal envelope	• Double envelope, sealable plastic bag, or dispatch bag
Moving assets by post	• Check address information is correct before sending • Mark as “private and confidential”, “personal”, “confidential” as required	• Check address information is correct before sending • Mark as “private and confidential”, “personal”, “confidential” as required • Consider using hand delivery or recorded delivery, depending on the sensitivity of the information
Internal e-mail	• Send internally to recipients who require and are entitled to the information	• Mark as OFFICIAL-SENSITIVE, and • Use specific handling controls to dictate audience and activities
External email	• Send externally to recipients who require and are entitled to the information • Use password protection or otherwise protect depending on the contents	• Mark as OFFICIAL-SENSITIVE, and • Use specific handling controls to dictate audience and activities • Send externally to recipients who require and are entitled to the information • Use secure email or password protection or otherwise protect depending on the contents
Disposal / Destruction	• Use provided paper bins in council premises	• Use provided confidential bins in council premises

	• Use confidential bin where information is confidential	
Retention	• Dispose of in line with council retention policy.	Use specific handling controls to dictate length of retention
Incident Reporting	• Report of any loss or compromise to the IG team.	Report of any loss or compromise to the IG team. Escalation to SIRO.