Nottinghamshire County Council

Information Security Classification and Protective Marking Standard

At a glance …

- The Council has three information security classifications – PUBLIC; OFFICIAL; and OFFICIAL-SENSITIVE.
- These must be used to inform how information assets will be processed (e.g. handled, stored and disposed of).
- Classifications should be used to protectively mark documents. For electronic documents, created in Microsoft 365, protective marking will be applied when documents are classified.
- Protective marking will enable instant information about a document's security status and handling requirements at a glance and encourages everyone to think about how they handle information.
- The automated default marking of documents will be OFFICIAL. Staff will need to up or down grade the classification to reflect the content.
- Equivalent Government Security Classifications should be used when communicating to public sector partners

Introduction

1. This document sets out the standard by which the Council classifies and protectively marks information assets (in any format) to ensure that they are appropriately secured and protected.

Policy References

2. This document forms part of the suite of documents that comprise the Council's Information Governance Framework and is a requirement of the Information Compliance Policy, which makes a commitment that the Council will classify and use information according to its risk, sensitivity, value, and importance.

The Principles and Commitments

3. Classification, marking and control of information underpins the ability of the Council to secure and protect its information assets. All staff have a duty of confidentiality and to protect the Council's information regardless of its format.

4. The Council has three information security classifications, based on the risk and impact to an individual or organisation, and the financial, reputational and legal risk to the Council. These are set out in this Standard.

5. All information assets should be classified into one of the categories and be appropriately labelled (protectively marked) to ensure that their classification is readily identifiable. The

classification and protective marking will inform how information will be processed (including handling, storing and disposal).

6. The Council will, wherever possible, use technology to ensure the application of information security classifications (and the associated protective marking) so that demands on staff are minimised.

7. These three information security classifications are set out in the table below and can be seen alongside the equivalent Government Security Classifications to assist in handling information received from public sector partners. Government Security Classifications should be used when communicating to public sector partners through secure email or when sharing information.

8. Information of staff members which is not related to work should not be stored on NCC systems. Staff may store work related store work-related but personal documents such as CVs; job applications; work-related training assignments within their OneDrive (as per the Storing and managing information in OneDrive).

The Classifications

9. The agreed classification categories are as follows:

Information Risk Categorisation	NCC Classification Standard	Government Security Classification
No Risk	**PUBLIC**: This will typically include information that is already in and / or there is no sensitivity in releasing into the public domain.	OFFICIAL
Low Risk	**OFFICIAL**: This will typically include some personal information as defined in the Data Protection Act 2018 and also business information.	OFFICIAL
High Risk	**OFFICIAL-SENSITIVE**: This will typically include special category information and more sensitive personal information as defined in the Data Protection Act 2018 and also business information we generally refer to as “confidential”.	OFFICIAL SENSITIVE

10. Examples of the types of information used in NCC against each of these NCC classifications follows as a (non-exhaustive) guide.

Applying the Classifications – Examples

*Use of ‘**PUBLIC**’ classification and protective marking*

11. This will typically include information that is already in and / or there is no sensitivity in releasing into the public domain. It applies to information that does not contain personal or confidential information. Examples include, but are not limited to:

- Approved policies and procedures
- Documents available in the public domain or on the Council's public website
- Names and contact details of specific employees, citizens or businesses that are in the public domain or an individual has authorised
- Property addresses which do not identify the individual owner or residents
- Information owned by the Council and made available under the Publication Scheme or released as an access request (includes information where copyright restrictions may apply)
- Information made available under any Government Codes of Practice on data transparency
- Anonymised data where personal data cannot be identified or traced

*Use of '**OFFICIAL**' classification and protective marking*

12. This will typically include some personal information as defined in the Data Protection Act 2018 and also business information. It applies where there is a requirement for controls and security measures for access, storage and handling of information to ensure that it is not released into the public domain, other than to those individuals or organisations that need to have access for a legitimate business reason. Examples include, but are not limited, to:

    - Any information that can uniquely identify an individual such as name, address, postcode, date of birth (if combined with other information)
    - Staff directory with contact numbers, address, position, what I do etc if not already public
    - Commercial or financial information
    - Pseudonymised data (that would otherwise be Sensitive (including special category data)
    - Policies and procedures in draft for approval, not yet released into the public domain and would not be released to the public in draft form
    - Information that does not contain personal data but is aimed at an internal audience (but may be fully or partly released under the Freedom of Information Act if requested, e.g. guides, local procedures)
    - Information that does not contain personal data but should not be made public for copyright reasons

*Use of '**OFFICIAL-SENSITVE**' classification and protective marking*

13. This will typically include special category information and more sensitive personal information as defined in the Data Protection Act 2018 and also business information we generally refer to as "confidential". It applies where there is a need to enhance certain management and handling controls for information assets deemed to be confidential and sensitive requiring restricted access. Examples include, but are not limited to:

    - Special categories of personal data as defined under the Data Protection Act 2018 including information pertaining to health (including NHS Patient Identifiable Data); religious beliefs; sexuality; criminal records etc
    - Social Care Records
    - Personal financial information relating to individuals such as VAT number, National Insurance (NI) number, bank details (including mandates and statements), financial assessments; Payment Card Data
    - Confidential commercial financial information
    - Exempt Committee papers excluded from the public under the Local Government Act.
    - All or part of an employee record/case file or customer record/case file (e.g. service user care plan, employee appraisal) containing health or other sensitive (including special category) personal data.
    - Contact details and address of high-risk vulnerable children or adults (e.g. in a refuge)

- Part of a case file that should not be released to the individual (e.g. Care Documents and communication while part of a serious child case review, safeguarding adult review or domestic homicide review etc).
- Draft documents before approval for release into public domain where these have a commercial value.
- Discussion papers and options relating to proposed changes to confidential strategies, policies and procedures, before the changes are announced (e.g. reorganisation of public services).
- Tender submissions before the award has been announced (but some should be changed to Public post award) and where some of the data is commercially sensitive.
- Contracts containing commercial information that are not to be fully released under FOI.
- Investigation files leading to disciplinary action or dismissal for an employee held by HR or a manager.
- Legal court bundle for child protection cases.
- All or part of an individual's or business case file that involves court proceedings or investigations leading to prosecution.
- RIPA details for surveillance purposes.
- Some sensitive property plans (e.g. plans and maps of Council building stock that have security implications or external property plans held by Emergency Planning.
- Enterprise wide applications/databases/electronic folders containing personal data / commercially sensitive / investigation or legal proceedings.
- Boxes of paper records containing personal or confidential information.
- The equivalent electronic records in (e.g. output from scanning or conversion, volumes of data sharing or processing)
- Anything that people may regard as particularly private and would reasonably expect us to keep private or they have shared with us in confidence.

Labelling (Protectively Marking) Information with their Classification

14. Information assets should be protectively marked as follows:

    a) Protective markings will, wherever possible, be applied to documents in upper case in the Council's official type case (currently Arial 12) using the appropriate classification of PUBLIC, OFFICIAL, OFFICIAL-SENSITIVE.
    b) The automated default marking will be OFFICIAL. Staff will need to up or down grade the classification to reflect the content.
    c) When working with electronic Microsoft documents, protective markings will be in the top, middle (header) of each page. This will be applied automatically when the document is classified where the technology permits.
    d) There may be exceptional circumstances in which the protective marking applied automatically needs to be removed from its automatic positioning (e.g. where the position throws out formatting). In this case, the author should attempt to add the appropriate classification to the document in another visible way.
    e) Any information that is not specifically marked will be deemed to be 'OFFICIAL.' However, the officer responsible for processing such a document must consider its contents and handling requirements before deciding what should be done with it.
    f) Material that has already been printed should have the classification marked at the top of each page. Multiple page documents must be stapled.
    g) Classification markings may be manually augmented in order to provide more descriptive handling (e.g. PUBLIC – Policy Document; OFFICIAL – Draft Procedure; OFFICIAL SENSITIVE – Personnel Records)

Advice and Support

15. If you have any issues over the clarity of this document, how it should be applied in practice, require advice or have any suggestions for amendments, please contact data.protection@nottscc.gov.uk or call 0115 8043800.

Compliance and Monitoring

16. Wilful or negligent disregard for information governance policies, standards and procedures will be investigated and may be treated as a disciplinary matter which could lead to dismissal or the termination of work agreement or service contracts.

17. Compliance with the Standard will be monitored by the Data Protection Officer (or their nominee(s)).

Review

18. This standard will be monitored and reviewed every two years but may be revised early should business process or developments in documents and records management require it.

Further information

Information Governance Team
Email: data.protection@nottscc.gov.uk
Telephone: 0115 8043800

Document Control

Owner	Data Protection Officer (CA)
Author	Data Protection Officer (CA)
Last Reviewer	Data Protection Officer (CA)
Approver	Data Protection Officer (CA)
Date of Approval	23/04/2021
Date of next review	22/04/2023
Version	1.3
Classification	**PUBLIC**

Version	Date	Changes and Approver
1.0	03/10/2018	Approved by Information Governance Group
1.1	10/09/2020	Amended to add additional Non-NCC classification category; reference protective marking and enhance examples of information types by classification. Approved by Information Governance Board (IGB).
1.2	26/01/2021	Amended to change Non-NCC category to My Info and positioning of the corresponding protective marking to the classification to top in the header. The assumption on unmarked documents changes from PUBLIC to OFFICIAL as that is the default. Approved by DPO under delegation from IGB.
1.3	23/04/2021	Amended to remove 'My Info' Classification. Reference made to OneDrive guidance. Approved by DPO under delegation from IGB.