WCC Information Risk and Protective Marking standard

This standard forms part of WCC's Information Governance Framework.

Protective Marking is a process by which an indication of the sensitivity or otherwise of a document, is visually added to the document/information being shared. It informs how information **must** be handled, stored and disposed of.

WCC's protective marking scheme adheres to the Government Security Classifications Policy (GSCP), based on the risk and impact to an individual or organisation and the financial, reputation and legal risk to the Council. This brings the Council into line with other Local Authorities and Public Sector organisations. Furthermore, using standard, nationally recognised markings makes them more understandable when sharing with Partner organisations.

There is one exception to this: for any information that is personal to you e.g., Your CV or work-related training coursework there is the additional marking of 'Not protectively marked'. This is because the system enforces protective marking of all information.

The following WCC Protective Marking **must** be used internally and when communicating to public sector partners through secure email and/or when sharing information:

Not protectively marked = information which is no or very low risk and does not require a protective marking. I.e., Public / Personal (non-work) information.

Official = used for the majority of Council information which may contain basic, non-sensitive, information. I.e., non-public work information that may contain no or low volume basic personal information and where there may be some consequences if the data was lost/stolen.

Official-sensitive = sensitive business / special category personal information of very high data breach risk. I.e., information that if compromised will have damaging consequences for a person, people or the Council. **

*** Where the WCC markings of Protect / Confidential and Restricted / Confidential Restricted markings have been applied previously, these have the same meaning as Official-sensitive.*

Below are *examples* of types of information used in WCC to be used as a guide.

If in doubt, ask Information Management for clarification.

Not protectively marked (No / Very Low Risk)

This marking should be used for any personal (non-work related) information as well as work information that can be made public.

Types of WCC No / Very Low Risk information:

- Policies and procedures.
- Documents available in the public domain or on the WCC public website.
- Names and contact details of specific employees, citizens or businesses that are in the public domain or an individual has authorised.
- A property address where it does not identify the individual owner or residents.
- Open data, i.e., data that can be freely used, re-used and redistributed by any one – see also the ICO’s guide to the Re-use of Public Sector Information.
- Information owned by WCC 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.
- Your C.V.
- Work related training coursework.

Official (Low Risk)

Information aimed at staff or partners that if it contains personal information is of a minimal amount / low volume with no sensitive/special category personal information (see Appendix 1 for example personal data types) referenced. I.e., information published to the intranet and/or where there is a low risk if more widely shared and which may have to be released under an FOI request.

Types of WCC Low Risk information:

- 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 either does not contain personal data or a minimal amount but is aimed at an internal audience (but may be fully or partly released under FOI if requested), e.g., guides, local procedures.
- Information that does not contain personal data but should not be made public for copyright reasons.

Official – Sensitive (High Risk / Very High Risk)

Information where there is a need to enhance certain management and handling controls for information deemed to be confidential or highly confidential and sensitive. I.e., information that would warrant a need for **restricted** access.

This can include high volumes of information detailing Article 6 level personal information (see Appendix 1 for example personal data types) or information containing sensitive / special category personal information, as well as business information generally referred to as or has an expectation of being “confidential”.

This information will require controls and security measures for access, storage and handling to ensure they are not released into the public domain other than to those individuals or organisations that need to have access.

Types of WCC High Risk information:

- Personal information relating to any customer or staff such as name, address and contact details, together with other personal data such as: VAT number, National Insurance (NI) number, bank details, for which we have a duty to keep the data confidential or withhold as personal data under an FOI request. This includes identifiers that can reference customers/staff, i.e., HR number, customer number, NHS number.
- NHS Patient Identifiable Data.
- Exempt Committee papers excluded from the public under the Local Government Act.
- Part of an employee record/case file or customer record/case file, e.g., service user care plan, employee appraisal. If there are many documents as a set, they should be treated together as High Risk
- Single documents where we have a duty of confidence.
- Staff directory with contact numbers, address, position, what I do etc, if not already public
- Bank Mandate, Financial Assessment.
- 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 and any post award 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.

Types of WCC Very High Risk information:

- A complete employee/customer record/case file containing health or other sensitive personal data
- An individual's set of social care/health paper files or an electronic record equivalent
- Part of a case file that should not be released to the individual, e.g., Care record restricted section, 3rd party references or may cause harm if released
- Documents and communication while part of a serious child case review, safeguarding adult review or domestic homicide review
- Mental health assessments
- Legal court bundle for child protection case
- A complete individual's or business case file that involves court proceedings or investigations leading to prosecution.
- RIPA details for surveillance purposes
- Contact details and address of a high-risk vulnerable child or adult, e.g., in a refuge or at risk
- Some sensitive property plans, e.g., plans and maps of WCC building stock that have security implications or external property plans held by Fire & Rescue or Emergency/Resilience Planning

Other information including databases, systems and extracts may attract higher risk due to the volume of records, typically in the 1,000's, and require specific measures, such as:

- Applications/databases/electronic folders containing personal data, e.g., CareFirst, ESCR, HRMS, Agresso, Library Management System, CRM
- Applications/databases/electronic folders containing commercially sensitive, investigation or legal proceedings, e.g., Legal VisualFiles, Trading Standards
- Boxes of paper records containing personal or confidential information in transit from offices or during office moves
- The equivalent electronic records in transit to and from WCC, e.g., output from scanning or conversion, volumes of data sharing or processing

Appendix 1: Personal Data Types

Personal information/data is any information relating to an identified or identifiable natural person.

Lower Risk Personal Data Types (GDPR Article 6):

- Any personal information that would not otherwise be deemed as particularly sensitive (see below for types that would be).

Special category / sensitive personal information (GDPR Article 9):

The below is to offer examples only and should not be taken as an exhaustive list.

- race;
- ethnic origin;
- political opinions;
- religious or philosophical beliefs;
- trade union membership;
- genetic data;
- biometric data (where this is used for identification purposes);
- health data;
- sex life; or
- sexual orientation.

For more information on what classifies as special category personal information, as defined by UK data protection legislation, see WCC's Data Protection regulation guidance at www.warwickshire.gov.uk/im.