# Information Risk Classifications

The risk classifications below are based on information risk and the impact on an individual(s), the Office of the Police and Crime Commissioner for Warwickshire ('OPCC') or any third parties if the information was inappropriately released, accessed or lost:

**NO RISK**
**LOW RISK**
**HIGH RISK**
**VERY HIGH RISK**

They should be used as a guide to setting the appropriate protective making used by the OPPC when working internally or with external partners. The protective marking will inform how information should be handled, stored and disposed of. The equivalent public sector protective markings and the new Government security classifications are shown in the table at the end of this guide, to assist in handling information received from partners.

Below are examples of the types of information used by the OPPC together with the equivalent risk classification and protective marking they fall within.

**NO RISK**
**Protective Marking: PUBLIC** or no marking

**Types of OPPC information**

- Policies and procedures
- Documents available in the public domain or on the OPPC website
- Organisational information including staff details already in the public domain
- Open data
- Information owned by the OPPC and made available under the Publication Scheme
- Anonymised / depersonalised data where individuals cannot be identified or traced

**LOW RISK**
**Protective Marking: INTERNAL**

**Types of OPPC information**

- Policies and procedures in draft for approval, not yet released into the public domain but of a routine and non-sensitive nature
- Information that does not contain personal information but is aimed at an internal audience (but may be fully or partly released under FOI if requested) for e.g. internal guidance or procedures
- Staff directory with contact numbers, address, position, if not already public

## HIGH RISK
**Protective Marking: CONFIDENTIAL**

This will include both personal and some sensitive personal data as defined under the Data Protection Act 1998 ('DPA') and information generally referred to as "confidential". Additional security measures are required for storage, handling and disposal.

**Types of OPPC information**

- Personal details relating to a complainant or employee such as name, address and contact details
- Information restricted by legal statute
- Part of an employee record/case file or complainant record/case file for e.g. employee appraisal
- Single documents where the OPPC has a duty of confidence
- Bank & financial details
- Draft documents before approval for release into public domain where these have a commercial or confidential value
- Discussion papers and options relating to proposed changes to confidential strategies, policies and plans, before the changes are announced for e.g. police and crime plan, policing strategies, community safety or crime prevention strategies
- Tender submissions before the award has been announced (but consider changing to "PUBLIC" post award unless commercially sensitive)
- Contracts containing commercially sensitive information

## VERY HIGH RISK
**Protective Marking: CONFIDENTIAL - RESTRICTED**

This will include sensitive personal data for e.g. physical or mental health details as defined by the DPA and information we generally refer to as "strictly confidential", especially where larger volumes of records are held. Additional security measures are required for storage, handling and disposal.

**Types of OPPC information**

- A complete set of a complainant's file
- Physical identifiers such as DNA, finger prints and other genetic sample
- Vetting and CRB information
- A complete set of an employee or volunteer's HR file
- Investigation files leading to disciplinary action or dismissal for an OPCC employee, the chief constable or an employee of the chief constable
- A complete employee record / case file, especially if containing health or other sensitive personal information
- Documents and communication of a serious case review
- An individual's complete case file that involves court proceedings or investigations leading to prosecution

- ➢ RIPA details for surveillance purposes
- ➢ Police national computer / database information
- ➢ Contact details and / or information about a high risk vulnerable child or adult or a high risk offender
- ➢ Medical information
- ➢ Partial or complete complainant, officer, employee, offender or business records for a volume of individuals, where the individuals can be identified
- ➢ Other volumes of information including databases, systems and extracts.

**Risk classification mapping to public sector / Government security classifications**

| Information Risk Classification | WCC Protective Markings | Government Security Classifications | Old Protective Markings* / Business Impact Levels |
|---|---|---|---|
| NO RISK | **PUBLIC** or no marking | **OFFICIAL** | UNCLASSIFIED* |
| LOW RISK | **INTERNAL** | **OFFICIAL** | N/A |
| HIGH RISK | **CONFIDENTIAL** | **OFFICIAL OFFICIAL-SENSITIVE** | PROTECT* NHS CONFIDENTIAL IL2 |
| VERY HIGH RISK | **CONFIDENTIAL-RESTRICTED** | **OFFICIAL OFFICIAL-SENSITIVE** | RESTRICTED* NHS CONFIDENTIAL IL3 |