# Information Classification Policy

## 1. Purpose

This policy supports the Information Governance Policy by setting out the British Red Cross' (BRC) information handling standards and information classification scheme, thereby confirming its commitment to also meeting legal and regulatory requirements in compliance with Data Protection legislation. This policy also ensures appropriate protection and handling of BRC's information assets by mitigating risks relating to data protection, confidentiality, finance and reputation.

This policy must be read in conjunction with the Information Governance Policy, Information Classification Procedure, Information Classification Procedure: Annex and Data Protection Policy.

## 2. Scope

This policy applies to all our people, and all personal data or confidential business information processed by the organisation, in paper form, electronically or communicated verbally.

## 3. Policy Statement

The organisation recognises that the information we hold has varying degrees of sensitivity and criticality. To preserve the appropriate confidentiality, integrity and availability of this information, the BRC must ensure information is protected against unauthorised access, disclosure or modification; it does this by complying with its information handling standards, and by:

**3.1.** Ensuring all information is classified into one of the three Information Classification Categories, 'Public', 'Internal Use' and 'Confidential', which are further defined by the Principles of 'Confidentiality', 'Integrity' and 'Availability' and their Levels and Values.

**3.2.** Utilising appropriate appraisal criteria when considering the classification of information.

**3.3.** Ensuring conflicts of variances in classification systems are resolved when exchanging data with other organisations or third parties which have been classified or labelled.

**3.4.** Annotating data imported onto our systems with the approved organisational classification and removing conflicting labelling by the originator.

**3.5. Lessons Learned from Policy Evaluation**

A review of this policy was undertaken, and feedback was garnered from the Information Governance Champions. This informed improvements to this policy document including roles updated due to organisational restructure, and procedural and process information has been relocated.

## 4. Responsibilities

The Executive Leadership Team (ELT) are responsible for ensuring compliance with this policy.

The Chief Operating Officer (Policy Owner) is responsible for ensuring that this policy allows achievement of external and internal standards.

The Head of Information Governance and Data Protection Officer (Policy Lead), together with the Policy Owner, is responsible for the development, monitoring, and review of this policy. The Policy Lead is also responsible for providing advice and ensuring training is provided to our people.

The Chief Medical Advisor is the Caldicott Guardian who is responsible for: ensuring that the personal information about those who use the BRC services is used legally, ethically and appropriately.

The Directorate Management Teams (i.e. Directors and Department Heads) are responsible for identifying, recording and accounting for key information assets in their domain and appointing Information Asset Owners.

Document authors are responsible for assigning a classification category to the documents they create and protectively marking the documents.

All Managers are responsible for operational implementation of, and compliance with, the policy and that any breaches are reported and investigated.

Information Asset Owners are responsible for the assets they own, ensuring they are recorded on the information asset register, and where possible, ensuring information produced or created from databases or using reporting software is protectively marked.

The Information Governance Steering Group has strategic responsibility for monitoring the implementation of this policy, its effectiveness and acting upon any risks or issues identified.

It is the responsibility of all our people to adhere to this policy including by participating in induction, training and awareness raising sessions to confirm their responsibilities to respect the security classification of any information as defined. They should also report any incidents, through the Datix Cloud IQ electronic incident reporting system.

## 5. Governance

| | |
|---|---|
| **Associated policy document/s** | • Business Continuity and Resilience Management Policy<br>• Confidentiality Policy<br>• Data Protection Policy<br>• Data Quality Policy<br>• Incident Reporting Policy<br>• Information Governance Policy<br>• Information Security Policy |

| | | |
|---|---|---|
| | • Records Management Policy | |
| **Policy(ies) superseded** | N/A | |
| **Legislation/ regulatory requirements and standards** | • Data Protection Act 2018<br>• General Data Protection Regulation (GDPR)<br>• Human Rights Act 1998<br>• The Common Law Duty of Confidentiality<br>• The Caldicott Principles<br>• Equality Act 2010 | |
| **Equality impact assessment** | No equality impact identified | |
| **Data Protection impact assessment** | No negative data protection impact identified; positive impact intended | |
| **Environmental impact assessment** | No environmental impact identified | |
| **Endorsing Authority; Endorsement date** | Chief Operating Officer; 09 2025 | |
| **Approval Authority; Approval date** | ELT; 09 2025 | |
| **Policy Owner** | Chief Operating Officer | |
| **Policy Lead** | Head of Information Governance and Data Protection Officer | |
| **Date effective** | 09 2025 | |
| **Interim update date** | N/A | |
| **Review date** | 09 2028 | |
| **Version** | 4.0 | |
| **Keywords** | confidential, information, classification, security, integrity, public, internal, availability, IG, data protection, information governance, confidentiality, asset, asset owner, protective, marking, creating, storing, processing, disposing, transferring, value, level, Datix | |
| **Revision history** | **Version** | **Summary of change (s)** |
| | 1.0 | Original policy document. |
| | 2.0 | New template, changes to legislative requirements and internal policy/ procedure. |
| | 3.0 | Small grammar changes, and changes in Legislation. |
| | 4.0 | Compliance with the Policy and Procedure Framework, updated associated policy names, grammar changes, roles updated due to organisational restructure, procedural and process information relocated. |

## Appendix: Definitions

**Confidential:** information which is not common knowledge and is of value. This includes personal identifiable information as well as commercially sensitive documents such as contracts.

**Datix Cloud IQ:** the incident reporting system used by the BRC to record all incidents, accidents, near misses and safeguarding concerns.

**Disclosure:** divulging or provision of access to data.

**Information Asset Owner:** a senior member of staff who is responsible for making decisions about an information asset/ system. The owner can assign day-to-day responsibility for each information asset to an administrator.

**Information classification:** information placed into categories depending on the harm that could result from loss or unauthorised disclosure. All information assets must be assessed to determine the appropriate classification category. The criteria to determine the appropriate classification category for BRC information can be found in the document 'Guidance: How to Categorise Information.'

**Information protection/ handling:** the information classification category that determines how information must be protected/ handled. Information in the Level 2 ('Confidential') category must be handled, transferred, stored and disposed of in according with the organisation's 'Guidance: Information Handling Standards' document.

**Our people:** staff, volunteers and contractors (e.g. third parties delivering services on behalf of the BRC).

**Personal data:** any data relating to an identifiable person who can be directly or indirectly identified in particular by reference to an identifier. This definition provides for a wide range of personal identifiers to constitute personal data (e.g. name, address, national insurance number, identification number, location data or online identifier, and the way organisations collect information about people).

**Processing:** anything done with the information including its collection, recording, use (including viewing), disclosure and destruction.

**Protective marking:** displays the classification category on electronic or paper documents and it indicates to others the classification category to ensure they are aware of the level of protection needed in handling, transferring, storing and disposing of information.