British Red Cross

Information governance

# Information Classification Policy

*This policy outlines the information classification scheme we have in place as well as our information handling standards. The aim of the policy is to ensure that information is appropriately protected from loss, unauthorised access or disclosure.*

| | |
|---|---|
| **Policy owner** | Chief Information Officer |
| **Policy lead** | Head of Information Governance |
| **Audience** | All British Red Cross people |
| **Legislation and regulation** | *Data Protection Act 2018*<br>*UK General Data Protection Regulation* |
| **Formally endorsed by** | Executive Leadership Team (ELT) |
| **Last updated** | May 2021 |
| **Next review** | May 2024 |

## 1 Introduction

1.1 The British Red Cross has a substantial amount of information which provides the foundation of our organisation. Information, like any other asset, must be appropriately protected.

1.2 In order to preserve the appropriate confidentiality, integrity and availability of information, we must ensure information is protected against unauthorised access, disclosure or modification. This is critical for all activities conducted across the organisation.

1.3 We have a duty and a responsibility to be as open and transparent as possible; however, information we hold has varying degrees of sensitivity and criticality and therefore some information requires additional protection or special handling.

1.4 This policy therefore outlines our information classification scheme and our information handling standards.

### Definitions

1.5 Full definitions can be found in Appendix 4.

## 2 Policy statement

2.1 Information should be classified, valued and risk assessed in accordance to its confidentiality, integrity and availability; regardless of the media on which it is stored, the manual or automated systems that process it, or the methods by

which it is distributed.

**2.2** All information will fall into one of three **information classification categories** based upon its confidentiality, integrity and availability.

2.3 When considering the classification of information, appropriate appraisal criteria as defined by our corporate policies should be used. For further guidance, please refer to our 'How to categorise information' appendix which supports this policy and is available on Red Room.

## Purpose and aims

2.4 The classification of our information assets supports our efforts to:

2.4.1 Appropriately protect our assets;
2.4.2 Support organisational assets and the effective use of information;
2.4.3 Meet external requirements and obligations.

2.5 There are risks associated with inappropriate handling of personal, sensitive, or confidential information. We have a responsibility to account for and to safeguard the information of our service users, our supporters and our people, as well as organisational data.

2.6 This policy aims to ensure appropriate protection and handling of our information assets, in accordance with their classification, to help mitigate risks, including those relating to data protection and confidentiality, financial and/or reputational risk.

## Scope

2.7 This policy applies to all our information, irrespective of the data location or the device it resides on. It should be used by all our people and any third party working on our behalf.

2.8 There may be specific legal or contractual stipulations relating to information classification that apply in addition to the standards set out in this policy.

## Standards

### Information Classification Scheme

**2.9** Our information classification scheme has three categories: **PUBLIC**, **INTERNAL USE** and **CONFIDENTIAL**.

2.10 The levels of classification are summarised in the table below:

| LEVEL | CONFIDENTIALITY | INTEGRITY | AVAILABILITY |
|---|---|---|---|
| 0 | **PUBLIC** | LOW | LOW |
| 1 | **INTERNAL USE** | MEDIUM | MEDIUM |
| 2 | **CONFIDENTIAL** | HIGH | HIGH |

### Confidentiality

2.11 Access to, and use of, LEVEL 2 (Confidential) information is restricted to

authorised users with an immediate need to know; and then only for so long as that need exists and only to the extent of that need. Information classified as LEVEL 2 (Confidential) must be subject to protection at all times.

2.12 To support assessing information, please refer to the guidance 'How to categorise information'.

2.13 When exchanging data with other organisations or third parties which has been classified/labelled, recipients should ensure that conflicts of variances in classification systems are resolved. Data imported onto our systems should be annotated with the approved organisational classification and any conflicting labelling by the originator should be removed.

2.14 Documents marked 'Public' may not be re-classified to any other level, but that documents in the three other levels are likely, over time, to move into the 'Public' classification.

### Integrity

2.15 Value of the integrity of information should be assessed as follows:

| Integrity value | Low | Medium | High |
|---|---|---|---|
| Description | Negligible or low impact arising from breach in Integrity | Moderate impact arising from breach in Integrity | High impact arising from breach in Integrity |
| Examples | Internal websites | Internal workflows | Donor facing websites/Treasury systems |

### Availability

2.16 The availability value of information should be based upon the impact of any period of partial or full unavailability:

| Availability value | Low | Medium | High |
|---|---|---|---|
| Description | Information where the owner is prepared to accept a medium to long term loss of availability of information/service | Information where the owner is prepared to accept a short to medium term loss of availability of information/service | Information where the service is critical and absolutely minimal loss of availability of information/ service is acceptable |
| Examples | Internal informative websites | Service user/ supporter informative websites | Core infrastructure systems |

## 3 Responsibilities

3.1 The **Chief Information Officer (CIO)** is the designated owner of this policy on behalf of the Executive Leadership Team.

3.2 The **Head of Information Governance** is the policy lead and is responsible for the ongoing review and maintenance of this policy and for responding to queries on a day to day basis.

3.3 The **Caldicott Guardian** is responsible for protecting the confidentiality of information and supporting the Caldicott function.

3.4 **Document Authors** are responsible for assigning a classification category to the documents they create and protectively marking the document.

3.5 **Information Asset Owners** are responsible for assigning a classification category to assets they own, ensuring the classification is recorded on the information asset inventory, and where possible, ensuring information produced or created from databases or using reporting software is protectively marked.

3.6 **All our people** are responsible for protecting information in accordance with this Policy and for meeting the standards set within it. They must respect the security classification of any information as defined. Data breaches should be reported via Datix, our incident reporting system.

3.7 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.

## 4 Laws and regulations

4.1 This policy supports our compliance with relevant UK legislation and regulation, including the *Data Protection Act 2018 and the UK General Data Protection Regulations*.

## 5 Monitoring and compliance

5.1 Regular internal audits on compliance with Information Governance policies will be undertaken by the Information Governance team. Audit findings will inform organisational improvement needs (e.g. training, policy or procedure development, increased communications etc.).

## 6 Training and support

6.1 All our people who handle information on our behalf are required to undertake Information Governance training as part of the induction process. This training must be taken annually, with completion rates closely monitored.

6.2 Additional support - either ad-hoc or regular – to further support compliance with our data management policies and/or procedures can be requested from the Information Governance team.

## 7 Review and maintenance

7.1 This policy was last updated in May 2021, and is next scheduled to be reviewed in May 2024.

# 8 Appendices

8.1 Appendix 1: related documents

8.2 Appendix 2: document provenance

8.3 Appendix 3: privacy impact assessment summary/equality impact assessment/environmental impact assessment – not applicable for this policy

8.4 Appendix 4: definitions

8.5 Appendix 5: legislative requirements

## Appendix 1: related documents

| Document title | Relationship to this policy |
|---|---|
| Business Continuity Management Policy | Ensures that we institute appropriate and proportionate measures in order to effectively plan for and manage business continuity arrangements. |
| Confidentiality Policy | Ensures confidentiality of personal identifiable and confidential business information and our responsibilities regarding disclosure of such information |
| Data Protection Policy | Sets out our data protection responsibilities. |
| Data Quality Policy and Procedure | Sets out a framework which is intended to assist the BRC ensure a high standard of data quality across all of the information collected. |
| Incident Reporting Policy and Procedure | This policy supports effective identification, reporting, managing and learning from incidents as an important part of managing risk, improving our services, and protecting those who use our services. |
| Information Governance Policy | The primary policy under which all other Information Governance policies, procedures and guidance relating to managing information and data reside. |
| Information Security Policy | This policy sets out an Information Security Framework which is intended to assist the British Red Cross to ensure a high standard of Information Security. |
| Records Management Policy | The effective management of records plays an important role in supporting our functions, enabling us to manage our operations successfully. |
| How to categorise information<br>Protective marking standards<br>Information handling standards | Procedural/guidance documents designed to support the implementation of this Policy |

## Appendix 2: document provenance

| Endorsed | Category | Summarise changes made | Reason for changes | Consulted | Endorsed by |
|---|---|---|---|---|---|
| 03/2015 | Scheduled | Current policy live | | Governance/ED F,P&R | The Board |
| 04/2018 | Scheduled review | New template, changes in legislative requirements and internal policy/procedure | Change to operating environment | CIO, Corporate Policy Manager, Governance | Chief Information Officer |
| 05/2021 | Schedule review | Small grammar changes, and changes in legislation | Changes in legal requirements | | Chief Information officer |

## Appendix 4: definitions

- **Information Classification** – puts information 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 our information can be found in the guidance document '**How to categorise information**.'
- **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.
- **Information protection/handling** – the information classification category 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 '**Information Handling Standards**'
- **Data** – data is a collection of facts from which information is constructed via processing or interpretation.
- **Information** – information is the result of processing, gathering, manipulating and organising data in a way that adds to the knowledge of the receiver.
- **Information Asset Owner (IAO)** – 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 Asset Administrator (IAA)** – the person responsible for the day to day operation of an information asset/system.
- **Personal data** - shall mean 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 (for example: name, address, national insurance number, identification number, location data or online identifier, and the way organisations collect information about people, etc.)
- **Sensitive information referred to as "special category" –** shall have the same meaning as under the UK General Data Protection Regulation (UK GDPR) namely data consisting of racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, biometric data, data concerning health or data concerning a natural person's sex life or sexual orientation.
- **Confidentiality** – access to data shall be confined to those with appropriate authority.
- **Integrity** – information shall be complete and accurate. All systems, assets and networks shall operate correctly, according to specification.
- **Availability** – information shall be available and delivered to the right person, at the time when it is needed.

## Appendix 5: legislative requirements

This policy is subject to all relevant laws passed in the areas in which we operate, whether or not they are specifically mentioned in this document.