BritishRedCross

Information governance

Information Governance Policy

This policy is the overarching Information Governance Policy for the British Red Cross and is the primary policy under which all other Information Governance policies, procedures and guidance relating to the management of information and data reside.

Policy owner	Chief Information Officer
Policy lead	Head of Information Governance
Audience	All staff and volunteers, and relevant stakeholders (for example, third parties delivering services on our behalf)
Legislation and regulation	Data Protection Legislation including GDPR and DPA and all applicable law about the processing of personal data and privacy
Formally endorsed by	Chief Information Officer
Last updated	May 2018
Next review	May 2021

1 Introduction

1.1 The British Red Cross recognises that for legal, organisational and reputational reasons, it needs to have in place appropriate systems, processes and training to ensure that all confidential, personal or sensitive information is processed securely and that unauthorised access is prevented.

1.2 All of our people, including relevant stakeholders, have a responsibility to protect information assets and maintain good Information Governance practice.

1.3 We also recognise that the effective, efficient and safe handling of data and information is an integral part of ensuring we uphold our obligations – as an employer and a service provider – to our staff, volunteers, service users and partner organisations.

1.4 This policy is the overarching Information Governance Policy for the British Red Cross and is the primary policy under which all other Information Governance policies, procedures and guidance relating to the management of information and data reside. Appendix 2 provides a list of related documents.

1.5 This policy sets out our intentions and principles regarding Information Governance and is designed both to ensure that we comply with all relevant legislation in respect of data protection and to ensure good practice in managing and safeguarding information related to its staff, volunteers, service users, donors and other stakeholders.

1.6 As we develop our policies and procedures around Information Governance we will seek to follow sector good practice/guidance and relevant industry standards such as the Caldicott Principles and the NHS Information Governance Toolkit.

Definitions

1.7 Information Governance is a framework for handling corporate, service user, staff and volunteer information in a confidential and secure manner to appropriate legal, regulatory, contractual, ethical and quality standards. It also encompasses Data Quality and the appropriate re-use or sharing of data. It provides a consistent way for our people to deal with the many different information handling requirements including:

- Information Governance Management
- Confidentiality and Data Protection assurance
- Information Security assurance
- Clinical Information assurance
- Secondary Use assurance
- Corporate Information assurance

1.8 The three characteristics of Information Governance are:

- **Confidentiality:** Preserving authorised restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.
- **Integrity:** Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity.
- **Availability:** Ensuring timely and reliable access to and use of information or an information system.

1.9 The three principles of ensuring confidentiality, integrity and availability of information are key to on-going successful Information Governance. We have a legal duty to protect information held, belonging to individuals. A duty of confidentiality may also arise as a result of a contract where one party agrees to keep confidential information provided by the other party.

1.10 We use the following definitions when describing information that may need particular protection:

- **Confidential** shall mean information which is not common knowledge and which is of value.
- **Personal data shall mean any information relating to an identified or** identifiable natural person (‘data subject’); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier (e.g. an IP address)

- **Special Category Data** (also known as sensitive personal data) is any data which by its nature is particularly sensitive. This would include personal data relating to or including racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, biometric data, data concerning health, sex life or sexual orientation.

2 Policy statement

Purpose and aims

2.1 This policy establishes our key Information Governance priorities in order to:

- Ensure the principles of Information Governance;
- Maintain Information Governance at a consistent standard across all information management systems; and
- Provide a framework to ensure compliance with legislation and directives and guidance from relevant authorities.

Scope

2.2 This policy applies to all our people, as well as relevant stakeholders (for example, third parties delivering services on our behalf). It applies to all information processed by us, whether held in paper, electronic or even communicated verbally.

2.3 This policy is supported by the Information Governance Strategy that describes the improvement plans and focus for the British Red Cross.

Standards

2.4 The following summarises the measures, controls and standards maintained by the British Red Cross in relation to Information Governance.

3 Information Governance Principles

3.1 We recognise the need for an appropriate balance between openness and confidentiality in the management and use of information.

3.2 We also recognise the need to share information with other organisations and other agencies in a controlled manner consistent with the interests of the service user and, in some circumstances, the public interest.

3.3 Accurate, timely and relevant information is essential to deliver the highest quality service. It is the responsibility of all of our people to ensure and promote information quality and to actively use information in decision making processes.

4 Key elements of the Information Governance Policy

4.1 There are six interlinked strands to the Information Governance Policy:

- **Openness and Freedom of Information**
- **Legal and Regulatory Compliance**
- **Information Security**

- **Information Quality Assurance**
- **Records Management**
- **Information Governance Training**

Openness and Freedom of Information

4.2 As a charitable organisation we are not generally subject to the Freedom of Information Act 2000. However, in circumstances where the organisation is delivering services on behalf of public sector partners, we recognise that information we hold in relation to these services may be subject to freedom of information requests. Any such cases will be dealt with in line with the legislation. The transparency and accountability policy provides further information.

4.3 Data subjects can exercise their right to access information relating to them. The subject access request procedure and guidelines provides further information.

Legal and Regulatory Compliance

4.4 We regard all identifiable personal information relating to service users as confidential.

4.5 All identifiable personal information relating to staff, volunteers, donors and third parties will be kept confidential except where required otherwise.

4.6 We will maintain policies and procedures to ensure compliance with the Data Protection legislation, the common law duty of confidentiality and the NHS Confidentiality Code of Practice.

4.7 Information will be defined and where appropriate kept confidential, underpinning the Caldicott Principles and regulations outlined in Data Protection Legislation.

4.8 Information Governance compliance requirements will be linked to disciplinary procedures for staff and volunteers, for action to be taken as appropriate.

Information Security

4.9 We will maintain standards and policies for the effective and secure use and management of our information assets and resources; and for the effective and secure transfer and disclosure of information into and out of the organisation.

4.10 Audits will be undertaken or commissioned to assess information and IT security arrangements on a regular basis.

4.11 We will promote effective confidentiality and information security practice to our staff and volunteers through policies, procedures and training.

4.12 Our Incident Reporting system Datix will be used to report, monitor and investigate all reported instances of actual or potential breaches of confidentiality and information security. Please refer to the incident reporting policy and procedure for further information.

4.13 Integrity of information will be monitored and maintained to ensure that it is appropriate for the purposes intended.

4.14 Availability of information for operational purposes will be maintained within set parameters relating to its importance via appropriate procedures and computer system resilience.

4.15 Risk assessment, in conjunction with overall priority planning our activity will be undertaken to determine appropriate, cost-effective information governance controls are in place.

Information Quality Assurance

4.16 We will maintain policies and procedures for information quality assurance. We will also undertake or commission assessments and audits of information quality on a regular basis.

4.17 Managers are expected to take ownership of, and seek to improve, the quality of information within their areas of responsibility.

4.18 Data standards will be set through clear and consistent definition of data items, in accordance with national standards.

4.19 Wherever possible, information quality should be assured at the point of collection. We will promote information quality through policies, procedures, user manuals and training.

Records Management

4.20 We will maintain policies and procedures for the effective management of records. Please refer to the records management policy for further information. We will also undertake or commission assessments and audits of its records management on a regular basis.

4.21 Managers are expected to ensure effective records management within their areas of responsibility.

4.22 We use the International Standards on Records Management: BS ISO15489 as the standard for records management. We will promote effective records management practices through policies, procedures and training.

Information Governance Training

4.23 We will maintain an Information Governance training programme for the effective delivery of Information Governance training, awareness and education.

4.24 Training will be provided at the point of induction, and will be refreshed through an annual mandatory Information Governance training for all our people who have access to confidential, personal and sensitive information. At the end of the training module a short test will be required, to ensure that our people understand the importance of Information Governance and their role in supporting this policy.

4.25 We will provide general Information Governance guidance on a regular basis through newsletters, articles, team meetings etc.

4.26 Evaluation of Information Governance training will be undertaken to assess the effectiveness of the training and influence changes to future training.

The HORUS Process

4.27 Our process to deliver good Information Governance is centred around how information is held, obtained, recorded, used and shared ('HORUS'), and how this will influence outcomes. Achieving a satisfactory outcome will rely on all HORUS standards being met. The diagram in Appendix 1 illustrates the key objectives and controls supporting meeting the HORUS standards.

5 Responsibilities

5.1 The Chief Information Officer (CIO) is the Executive Leadership Team (ELT) owner for the policy. The CIO is also the Senior Information Risk Owner (SIRO) with overall responsibility to lead on Information Governance and foster a culture that values, protects and uses information for the success of the British Red Cross and benefit of its supporters, service users, staff and volunteers.

5.2 The role of the Caldicott Guardian is carried out by the Chief Medical Adviser. The Caldicott Guardian is responsible for leading on confidentiality relating to identifiable personal data and for overseeing all arrangements including protocols and procedures, for the use and sharing of identifiable personal data as well as ensuring that confidentiality requirements are reflected in our strategies, policies and working procedures for our people.

5.3 The Chief Information Officer is responsible for ensuring information governance and information security standards are met.

5.4 The Head of Information Governance is the overall Information Governance and policy Lead. The Head of Information Governance will provide direction in formulating, establishing, promoting and maintaining the policies and documentation that demonstrate commitment to and ownership of Information Governance responsibilities. The Head of Information Governance will ensure that appropriate training is made available to our people. The Head of Information Governance will ensure the annual NHS IG Toolkit assessments and audits of Information Governance policies and arrangements are carried out, documented and reported and that the annual assessment and improvement plans are prepared for approval by the SIRO. The Head of Information Governance is also responsible for maintaining a central registry of information assets with details of Information Asset Owners.

5.5 The Information Security Lead will be carried out by the Information Security Manager. The Information Security Lead is responsible for ensuring information security measures are implemented across all IT systems and projects.

5.6 The Executive Leadership Team are Information Asset Owners and responsible for ensuring Information Governance good practice and compliance within their directorates and the information assets owned within these directorates.

5.7 Information Asset Administrators are responsible for managing their information assets including associated risks. Information Asset Administrators are required to routinely risk assess their information assets and report these findings to the

Information Governance team. Information Asset Administrators should know what information is contained within their asset, ensure the asset is held securely, restricting access as appropriate and is used appropriately.

5.8 The Data Protection Officer is responsible for ensuring maintenance and implementation of the Data Protection Impact Assessments, advising on data protection issues, liaising with the Information Commissioner's Office and providing support on subject access requests.

5.9 It is the responsibility of all line managers to ensure that the overall Information Governance Policy, strategy, framework and its supporting policies, standards and guidance, are built into local processes and that there is on-going compliance. Managers should inform staff about their Information Governance responsibilities and where to get advice on Information Governance issues and how to report actual/suspected confidentiality and information security incidents.

5.10 It is the responsibility of our people to adhere to this policy. This includes undertaking the 'information governance' e-learning module within their first three months of starting work or volunteering, and completing annual refresher training.

5.11 A data protection and confidentiality clause has been incorporated into all staff contracts and volunteers' mutual expectations, and the text included is provided in appendix 4. All our people with access to British Red Cross information are required to sign a declaration of confidentiality and information security.

5.12 Our people should report any information governance risks they identify, or information governance incidents, through the incident reporting policy.

6 Laws and regulations

6.1 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.

7 Monitoring and compliance

7.1 Regular internal audits on compliance with Information Governance policies will be undertaken by the internal audit team. Audit findings will inform organisational improvement needs e.g. training, policy/procedure development, increased communications or other remedial actions.

8 Training and support

8.1 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.

8.2 Additional support - either ad-hoc or regular – to further support compliance with this policy can be requested from the Information Governance team.

9 Review and maintenance

9.1 This policy was last updated in May 2018, and is next scheduled to be reviewed in May 2021.

10 Appendices

10.1 Appendix 1: HORUS Process

10.2 Appendix 2: related documents

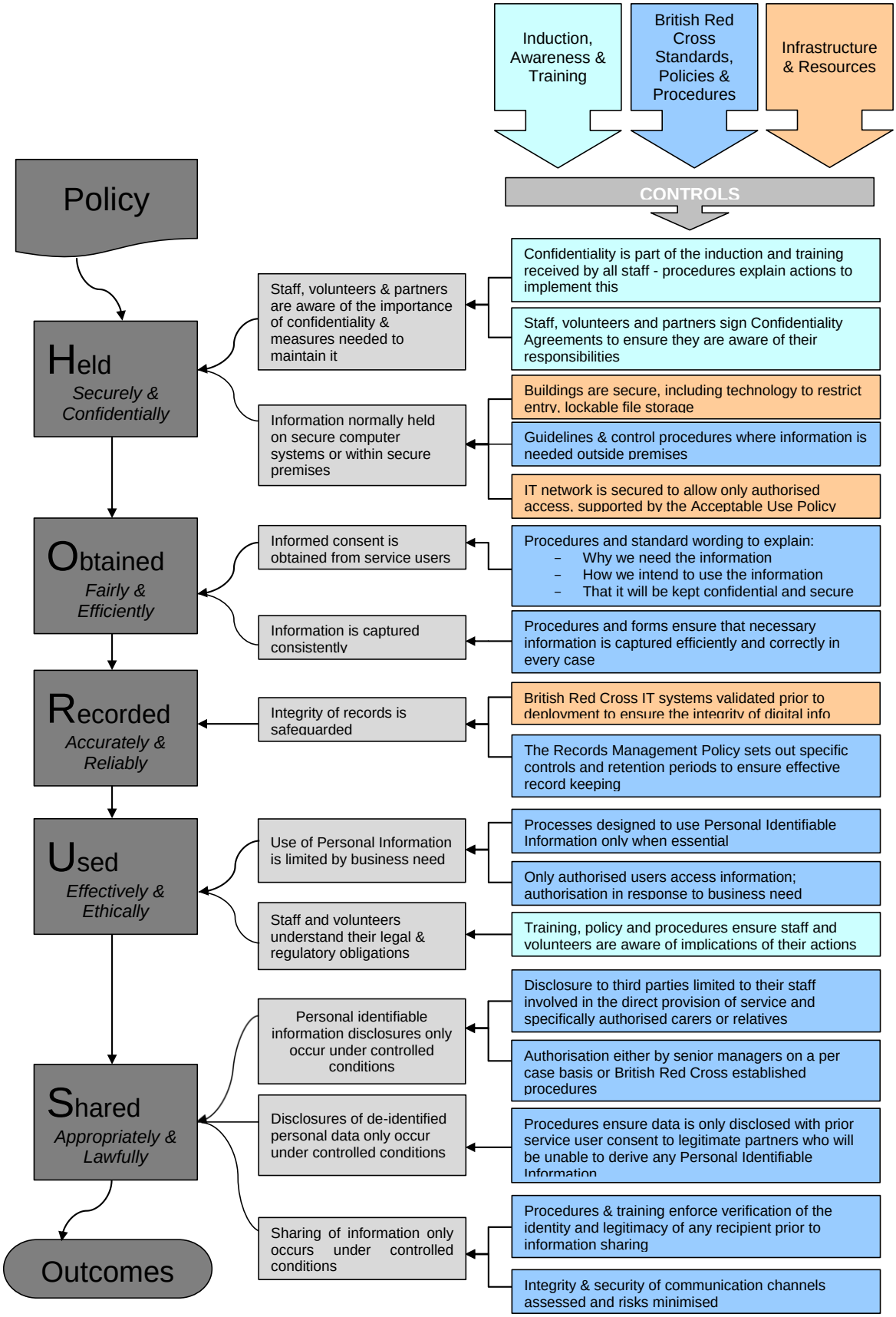
10.3 Appendix 3: document provenance

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

10.5 Appendix 4: data protection and confidentiality clauses

BritishRedCross

Appendix 1: HORUS Process



Appendix 2: 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	This policy 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 the effective identification, reporting, managing and learning from incidents as an important part of managing risk, improving our services, and protecting our people and those who use our services.
Information Classification Policy	This policy outlines the British Red Cross' information classification scheme and information handling standards, and aims to ensure that information is appropriately protected from loss, unauthorised access or disclosure.
Information Security Policy	Sets out our Framework to support 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.
Risk Management Policy	Sets out our approach and commitment to risk management.

Appendix 3: document provenance

Date endorsed	Category	Summarise changes made	Reason for changes	Consulted	Changes endorsed by
March 2015	Current live version	New policy developed and implemented	Approval of suite of information governance policies	Key stakeholders	Board of Trustees
May 2018	Scheduled review	Update policy to reflect GDPR and clarify obligations; streamlining as part of scheduled review	Changes in external environment/legal requirements	Governance, CIO	Chief Information Officer

Appendix 4: Data protection and Confidentiality Clauses

Clause included in staff contracts:

"You shall comply with the Society's data protection policies when handling personal data in the course of employment. You will also comply with any Information Governance policies of the Society from time to time in force.

Failure to comply with the Society's data protection policies or Information Governance policies may be dealt with under our disciplinary procedure and, in serious cases, may be treated as gross misconduct leading to summary dismissal.

The Society will collect and process information relating to you in accordance with the privacy notice which is on the internet.

In order to carry out its legal obligations as an employer (such as ensuring employees' compliance with the Society's data protection, Information Governance and related policies, and for other business reasons), the Society may monitor the use of systems including the telephone and computer systems, and any personal use of them, by automated software or otherwise. Monitoring is only carried out to the extent permitted or as required by law and as necessary and justifiable for business purposes."

Clause included in volunteers' mutual expectations:

As a British Red Cross volunteer you may see or hear personal information relating to people who use British Red Cross services, as well as fellow volunteers and employees. You may also see or hear confidential information about the British Red Cross itself. We have policies and procedures that volunteers must follow relating to information security, confidentiality, records management and the handling of personal data which enable us to meet our data protection obligations.

Advice on how to respond to a request for information you believe is confidential or sensitive from people or organisations outside of the British Red Cross must be sought from your line manager. It is also important that you are familiar with the support network open to you within the organisation should you need to discuss any information you have been given.

If you do not follow the organisation's rules regarding the control of relevant information (Information Governance) we may consider that you have not met our expectations of you as a volunteer, which may lead to your opportunity to volunteer being withdrawn."