Information Governance Policy

1. Purpose

This policy demonstrates the British Red Cross' (BRC) commitment to supporting the Information Governance (IG) Strategy by maintaining the IG Framework, and the provision of effective and standardised controls for handling information. It also allows the BRC to meet its legal, regulatory and contractual requirements.

This policy also supports the BRC's IG Improvement Plan in its attainment of the requirements of the National Health Service (NHS) England's Data Security and Protection Toolkit Standard, as a Voluntary Sector Organisation.

2. Scope

This policy applies to all staff, volunteers, third-party organisations, and stakeholders (our people) who undertake work on our behalf, both in the UK and internationally, and covers all information processed by the BRC, held in paper form, electronically, or communicated verbally.

3. Policy Statement

The BRC recognises the importance of securely managing information and the need for systems, processes, and training to protect confidential business information, and personal and special category data.

3.1. Principles

The IG principles are key to on-going successful IG. The BRC has a legal duty to protect information it holds on individuals, including within contracts, where one party agrees to keep information provided by another in a confidential manner. We will do this by:

3.1.1. Confidentiality: preserving authorised restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.

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

3.1.2. Integrity: preventing improper information modification or destruction, ensuring non-repudiation and authenticity.

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

3.1.3. Availability: ensuring timely and reliable access to information or information systems.

It is the responsibility of all our people to ensure and promote information quality and to actively use information in decision-making processes.

3.2. Key Elements

There are six interlinked elements to the IG Policy:

3.2.1. Openness and Freedom of Information

3.2.1.1. As a charitable organisation the BRC is not subject to the Freedom of Information Act 2000. In circumstances where the organisation is delivering services on behalf of public sector partners, we do 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 (refer to the Transparency and Accountability Policy).

3.2.1.2. We will comply with legislation regarding data subjects who have a right to access information relating to themselves (refer to the Subject Access Request Procedure).

3.2.2. Legal and Regulatory Compliance

3.2.2.1. All identifiable personal information will be kept confidential except where exemptions apply.

3.2.2.2. We will maintain policies and procedures to ensure compliance with the Data Protection legislation, The Common Law Duty of Confidentiality and the NHS England Confidentiality Code of Practice.

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

3.2.2.4. IG compliance requirements will be linked to the Disciplinary Policy and Disciplinary Procedure, Raising a Concern Policy and Raising a Concern Procedure for staff and stakeholders, and Volunteer Complaints, Issues and Concerns Policy, and appropriate action will be taken as required.

3.2.3. Information Security

3.2.3.1. 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.

3.2.3.2. Audits will be undertaken or commissioned to assess information and Information Technology security arrangements.

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

3.2.3.4. Datix Cloud IQ will be used to report, monitor, and investigate all instances of actual or potential breaches of confidentiality and information security (refer to the Incident Reporting Policy and Incident Reporting Procedure).

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

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

3.2.3.7. Risk assessment, in conjunction with activity priority planning, will be undertaken to determine appropriate and cost-effective IG controls are in place.

3.2.4. Information Quality Assurance

3.2.4.1. We will promote and maintain policies, procedures, user manuals and training for information quality assurance and undertake or commission assessments and audits of information quality.

3.2.4.2. We will ensure, via our managers, ownership and improvement of information quality within areas of responsibility.

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

3.2.4.4. Wherever possible, information quality will be assured at the point of collection.

3.2.5. Records Management

3.2.5.1. We will promote and maintain effective records management practices through policies, procedures and training (refer to the Records Management Policy) and undertake or commission assessments and audits of records management.

3.2.5.2. We will ensure, via our managers, effective records management within areas of responsibility.

3.2.5.3. We will use the International Standards on Records Management (BS ISO 15489) for records management.

3.2.6. IG Training

3.2.6.1. We will maintain a programme for the effective delivery of IG training, awareness and education.

3.2.6.2. IG training will be provided at induction and annual mandatory training is required for staff with access to confidential, personal and sensitive information, and every two years for volunteers with identical access.

3.2.6.3. We will provide general IG guidance through newsletters, articles, briefings and meetings.

3.2.6.4. Evaluation will be undertaken to assess the effectiveness of training and to support opportunities for learning and continuous improvement.

3.2.7. The HORUS Process

3.2.7.1. The BRC will deliver good IG by focussing on how information is held, obtained, recorded, used, and shared ('HORUS'), and influence on desired outcomes. Achieving a satisfactory outcome will rely on all HORUS standards being met (refer to the Information Governance Policy: Annex for a diagrammatic representation of the key objectives and controls that allow the HORUS standards to be met).

3.3. Lessons Learned from Policy Evaluation

A review of this policy was undertaken, and feedback was garnered from the IG Champions, the IG Steering Group, the Data Governance Group and key stakeholders. This informed improvements to this policy document including roles updated due to organisational restructure, procedural and process information being relocated, and legislation updated.

4. Responsibilities

The Board of Trustees (BoT) has ultimate responsibility for this policy and are responsible for responding to corporate risks.

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.

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

The Head of Platforms and Security is the Information Security Lead who is responsible for implementing security measures across IT systems and projects.

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

The Senior Director of People is responsible for ensuring that British Red Cross employment contracts are compliant with, and induction programmes inclusive of, the requirements of this policy.

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 uphold IG. They should also report any IG risks or incidents, through the Datix Cloud IQ electronic incident reporting system.

5. Governance

Associated policy document/s	• Business Continuity and Resilience Management Policy • Code of Conduct • Confidentiality Policy • Data Protection Policy • Data Quality Policy • Disciplinary Policy • Incident Reporting Policy • Information Classification Policy • Information Security Policy • Patient Safety Incident Response Framework Policy • Raising a Concern Policy • Records Management Policy • Risk Management Policy • Transparency and Accountability Policy • Volunteer Complaints, Issues and Concerns Policy
Policy(ies) superseded	N/A
Legislation/ regulatory requirements and standards	• Data Protection Act 2018 • General Data Protection Regulation (GDPR) • Human Rights Act 1998 • The Common Law Duty of Confidentiality • The Caldicott Principles • Equality Act 2010 • Freedom of Information Act 2000
Equality impact assessment	No equality impact identified
Data Protection impact assessment	No data protection impact identified
Environmental impact assessment	No environmental impact identified
Endorsing Authority; Endorsement date	ELT; January 2025
Approval Authority; Approval date	BoT; February 2025
Policy Owner	Chief Operating Officer
Policy Lead	Head of Information Governance and Data Protection Officer

Date effective	02 2025	
Interim update date	N/A	
Review date	02 2028	
Version	4.0	
Keywords	confidentiality, GDPR, General Data Protection Regulation, personal identifiable information, information security, information quality, risk, data, special category, personal, Datix, audit, risk, HORUS, records, standards, ISO,	
Revision history	**Version**	**Summary of change (s)**
	1.0	New policy document.
	2.0	Updated policy to reflect GDPR and clarified obligations; streamlined as part of scheduled review.
	3.0	Update to legislation; small grammar correction
	4.0	Roles updated; procedural information removed; updated legislation; alignment with new Policy and Procedure Framework.

Appendix: Definitions

Audit: an official inspection of an organisation's or area's records and/ or data.

Commission: to instruct an external authority to carry out an assessment and/ or audit.

Confidential: information which is not common knowledge, and which is of value.

Confidentiality: personal information that cannot be divulged to third parties without the express consent of the person.

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

Framework: a basic structure underlying a system or concept.

Information Governance: a unified approach for handling information, which complies with the law and outlines best practice.

Integrity: the accuracy, consistency and reliability of information.

Personal data: 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).

Risk Assessment: a careful examination of what could cause harm to people to determine if adequate precautions have been taken.

Special Category Data (also known as sensitive personal data): 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.

Staff: people employed by the BRC including agency, temporary staff and contractors.

Stakeholders: third parties delivering services on the BRC's behalf.

Volunteer: a person who operates for the BRC but does not get paid for their service.