Data Protection Policy

1. Purpose

This policy sets out the British Red Cross' (BRC) commitment to meeting the legal obligations of data protection legislation and how the BRC protects personal and special category data.

This policy must be read in conjunction with the overarching Information Governance Policy.

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, whether held in paper form, electronically, or communicated verbally.

This policy applies to 'personal data' and 'special category data' (also known as 'sensitive personal data'), hereon referred to under the label of 'personal data'.

3. Policy Statement

This policy is one of many corporate policies and procedures, and guidance documents designed to support good practice in Information Governance and security.

3.1. Data Protection Principles

Under Article 5(2) of the UK General Data Protection Regulation (GDPR), the BRC is required to demonstrate compliance with data protection principles. We will do this by:

3.1.1. Processing personal data lawfully, fairly and in a transparent manner. The lawful bases for processing are:

i. Consent.

ii. Contract.

iii. Legal Obligation.

iv. Vital Interests.

v. Public Task.

vi. Legitimate Interests.

3.1.2. Collecting only minimal personal data that are relevant to the purpose(s) for which they are to be processed.

3.1.3. Ensuring personal data are accurate and, where necessary, kept up to date.

3.1.4. Only storing personal data for as long as necessary and/ or as per stated limitations (refer to the Records Management Policy).

3.1.5. Storing personal data safely and securely.

3.2. Data Protection Standards

3.2.1. The BRC is committed to meeting its obligations under the data protection legislation complying with the data protection principles and ensuring personal data are processed fairly. We will:

i. observe the law and abide by the principles of the data protection legislation;

ii. keep notifications/ registrations with the Information Commissioner's Office up to date;

iii. appoint a dedicated Data Protection Officer as required by the data protection legislation.

3.3. Privacy Notices

3.3.1. Either before or at the time of collection of any personal data, we will inform a data subject via our Privacy Notice:

i. about what kind of personal data we collect;

ii. the reason for collecting the personal data;

iii. the purposes of the processing;

iv. the legal basis which we are relying on;

v. the data subjects' rights in relation to the personal data;

vi. security measures taken in relation to personal data;

vii. whether we transfer personal data to third parties;

viii. the retention period;

ix. any potential transfer of personal data outside of the UK.

3.3.2. We will ensure that the Privacy Notice is kept updated.

3.4. Data Subject Rights

3.4.1. We will ensure that data subjects are entitled to the following rights:

i. **The Right to be Informed:** data subjects have a right to know about our personal data protection and data processing activities, details of which are contained in our Privacy Notice.

ii. **The Right of Access:** data subjects have a right to submit a Subject Access Request (SAR) to request information about

the personal data we hold about them (refer to the Subject Access Request Procedure).

iii. **The Right to Correction:** data subjects have a right to require that any incomplete or inaccurate information is corrected.

iv. **The Right to Erasure (the 'Right to be Forgotten'):** data subjects have a right to require that we remove personal data we hold about them unless we have reasonable grounds to refuse the erasure.

v. **The Right to Restrict Processing:** data subjects have a right to request that we no longer process their personal data in certain ways, whilst not requiring us to delete the same personal data.

vi. **The Right to Data Portability:** data subjects have a right to request copies of personal data we hold about them in an easily accessible and storable format.

vii. **The Right to Object:** unless we have overriding compelling legitimate grounds for such processing, data subjects have a right to object to us using their personal data for direct marketing purposes (including profiling) or for research or statistical purposes, and may also object if we are processing their personal data on the grounds of pursuit of our legitimate interests.

viii. **Rights with Respect to Automated Decision-Making and Profiling:** data subjects have a right not to be subjected to automated decision-making (including profiling) if those decisions have a legal (or similarly significant effect) on the subject. This may not apply if the automated processing is necessary for us to perform our obligations under a contract, is permitted by law, or if explicit consent has been provided.

ix. **Right to Withdraw Consent:** if we are relying on consent to process a data subject's personal data, the data subject has a right to withdraw their consent at any time. Even if a data subject has not expressly given their consent to our processing, they have the right to object (refer to Section 3.4.1. vii).

3.5. Consent

3.5.1. Whenever personal data processing is based on the data subject's consent, we will retain a record of such consent. We will ensure that their consent (whenever consent is used as the lawful ground for processing) can be withdrawn.

3.6. Children

3.6.1. Where collection of personal data relates to a child under the age of 16, and we are relying on consent to process that data, we will ensure that parental/ guardian consent is given prior to personal data collection.

3.7. Disclosures

3.7.1. We will not allow personal data collected from data subjects to be disclosed to third-parties except in circumstances allowed by data protection legislation (i.e. where personal data is required to be disclosed as part of a criminal investigation).

3.8. Transfer of Personal Data to Third-Parties

3.8.1. We will ensure that a third-party supplier or business partner processing personal data on BRC's behalf has agreed to adopt security measures (level appropriate to potential associated risks) to safeguard personal data.

3.8.2. We will also ensure that certain protections required by UK GDPR form part a contract with a supplier, including that the supplier:

i. provides an adequate level of personal data protection.

ii. will only process personal data in accordance with our instructions or to carry out its obligations to us and not for any other purposes.

3.8.3. In instances where personal data are processed jointly with an independent third-party, we will explicitly agree with the third-party, BRC's and their respective responsibilities in the relevant contract.

3.9. Transfer of Personal Data Outside of the UK

3.9.1. Before transferring personal data out of the UK, we will ensure that adequate safeguards are in place (e.g. completion of a Transfer Risk Assessment, signing of the International Data Transfer Agreement (IDTA), IDTA Addendum) or that an Adequacy Notice is in place.

3.10. Data Protection Impact Assessments

3.10.1. To be compliant with data protection legislation we will identify early, using a Data Protection Impact Assessment, whether any new policies, systems, procedures, processes, services or projects are likely to impact on data protection.

3.10.2. When using the BRC standard business case or service tender template, our people will consider data protection implications.

3.11. Legitimate Impact Assessment

When relying on legitimate interest as the lawful basis for processing personal data, our people will determine whether the legitimate interest is appropriate before proceeding.

3.12. Lessons Learned from Policy Evaluation

A review of this policy was undertaken, and feedback was garnered from the Information Governance Champions, the Information Governance 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 Information Technology systems and projects.

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

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

The Information Governance Team provide: support and advice on disclosure of personal data to third-parties; will advise whether or not the transfer of personal data outside of the UK meets relevant requirements with the completion of a Transfer Risk Assessment; and will support our people with the completion of a Data Protection Impact Assessment or Legitimate Impact Assessment.

It is the responsibility of all our people to adhere to this policy including by complying with the data protection principles, participating in induction, training and awareness raising sessions to confirm their responsibilities to uphold information governance. They should also report any information governance 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 Quality Policy • Incident Reporting Policy • Information Classification Policy • Information Governance Policy • Information Security Policy • Patient Safety Incident Response Framework Policy • Records Management Policy • Risk Management 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
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	GDPR, General Data Protection Regulation, personal identifiable information, personal data, information security, Information Governance, risk, data, Datix, standards, incident,

	legitimate impact assessment, LIA, data protection impact assessment, DPIA	
Revision history	**Version**	**Summary of change (s)**
	1.0	Original policy document. Updated to reflect developments in information governance: add sections on subject access requests, incidents, and privacy impact assessments.
	1.1	Updated policy to reflect organisational change, extended date of next review, and other minor edits.
	2.0	Updated policy to reflect GDPR and make obligations clear; streamlining as part of scheduled review.
	3.0	Updated policy to reflect update to UK GDPR, as well as minor grammatical and streamlining changes.
	4.0	Roles updated, procedural information removed, updated legislation, alignment with the Policy and Procedure Framework.

Appendix: Definitions

Adequacy Notice: legal notice issued to confirm that a country data protection laws and practices meet the required standards for ensuring adequate protection of personal data.

Data Protection Impact Assessment: process used to identify, assess, and mitigate the risks associated with processing personal data, when introducing new data processing activities or technologies. It helps organisations ensure compliance with data protection laws) and protects individuals' privacy rights.

Data subjects: individuals whose personal data is processed by an organisation. Their rights, including access, rectification, erasure, and objection, are protected under data protection laws. This includes service users, staff, volunteers, and others whose data is handled by the organisation.

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

Information Commissioner's Office (ICO): UK's independent authority responsible for upholding information rights and ensuring compliance with data protection laws, such as the UK GDPR and the Data Protection Act 2018.

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

International Data Transfer Agreement (IDTA): a legal contract used to regulate the transfer of personal data from one jurisdiction to another, ensuring that data protection standards are upheld when personal data is sent across borders.

Legitimate Impact Assessment: process used to evaluate whether the processing of personal data is justified under the principles of legitimate interest as outlined in data protection laws.

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).

Privacy Notice: statement provided by an organisation to inform individuals about how their personal data will be collected, used, stored, and protected. It is a key element of data transparency and compliance with data protection laws.

Special Category Data (also known as sensitive personal data): data which by its nature are particularly sensitive. This includes 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. It can only be processed under strict conditions, including: having the explicit consent of the individual; being required by law to process the data for employment purposes; needing to process the information in order to protect the vital interests of the data subject or another.

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

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

Standard: accepted, consistent, agreed way of completing a task to ensure best practice.

Third-party organisations: external entities that an organisation may engage with to provide services, products, or support, which may involve processing personal data or accessing company systems. These entities are not part of the primary organisation (the data controller) but may handle data on its behalf, often as data processors.

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