BritishRedCross

Information governance

Data Protection policy

This policy sets out our commitment to safely and securely process the information that service users and supporters share with us, especially information that is sensitive in nature.

Policy owner	Chief Information Officer
Policy lead	Head of Information Governance
Audience	All staff, volunteers and third party organisations or contractors that undertake work on our behalf.
Legislation and regulation	*This policy meets our legal obligations under the EU General Data Protection Regulation (Regulation (EU) 2016/679) ('GDPR') and the Data Protection Act 2018 ('DPA') and all applicable law about the processing of personal data jointly referred to as the 'data protection legislation'*
Formally endorsed by	ELT
Endorsement date	June 2018
Next review	June 2021

1 Introduction

1.1 The British Red Cross helps millions of people in the UK and around the world to prepare for, respond to and recover from emergencies, disasters and conflicts.

1.2 We hold and process large volumes of information relating to our service users, supporters, staff, volunteers, and partner organisations.

1.3 This policy sets out the principles which we apply in processing personal data of employees, volunteers, service users, supporters, customers, consultants and business partners. It also sets out the obligations of our staff, volunteers and those working on our behalf in relation to personal data we hold or process.

1.4 This policy applies to all of our people, including staff, volunteers and third party organisations or contractors that undertake work on our behalf, in the UK and internationally.

1.5 This policy sets out how we will meet our obligations under Data Protection Legislation – as well as the expectations of our service users and supporters to ensure that we safely and securely process information they share with us, especially information that is sensitive in nature.

1.6 This is one of a number of policies and other guidance documents designed to support good practice in information governance and security, as well as

ensuring we meet legal requirements. We recommend that this policy is read in conjunction with the over-arching Information Governance Policy.

2 Policy statement

What is Personal Data?

2.1 This policy relates to 'personal data'. Personal data means any information relating to an identified or identifiable person ("data subject") who may be identified, directly or indirectly by reference to an identifier such as a name, an identification number, location data, online information (e.g. an IP address).

2.2 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.

Data Processing Principles

2.3 Under Article 5(2) of the GDPR we are required to demonstrate compliance with the data protection principles. These are:

- Lawfulness, fairness and transparency
- Limitation
- Minimal processing
- Accuracy
- Storage period limitation
- Integrity and confidentiality
- Accountability

2.4 Personal data must be processed lawfully, fairly and in a transparent manner. We need to be clear about the purpose or purposes for which we hold personal data so that we can then ensure that we process data in a way that is compatible with our original purpose. The lawful basis for processing are:

- **Consent:** the individual has given free, clear and unambiguous consent for you to process their personal data for a specific purpose.
- **Contract:** the processing is necessary to perform a contract, or because they have asked you to take specific steps before entering into a contract.
- **Legal obligation:** the processing is necessary for you to comply with the law (note: this is separate to contract obligations).
- **Vital interests:** the processing is necessary to protect someone's life.
- **Public task:** the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.

- **Legitimate interests:** the processing is necessary for your legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual's personal data which overrides those legitimate interests. Legitimate interests is different to the other lawful bases as it is not centred around a particular purpose (i.e., performing a contract with the individual, complying with a legal obligation, protecting vital interests or carrying out a public task), and it is not processing that the individual has specifically agreed to (consent). Legitimate interests is more flexible and could in principle apply to any type of processing for any reasonable purpose. Because it could apply in a wide range of circumstances, it puts the onus on you to balance your legitimate interests and the necessity of processing the personal data against the interests, rights and freedoms of the individual taking into account the particular circumstances. This is different to the other lawful bases, which presume that your interests and those of the individual are balanced. For guidance on legitimate interests please speak to the Information Governance team. Information on conducting a 'Legitimate Impact Assessment (LIA) can be found in section 3.19.

2.5 Personal data must be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes. In other words, there are clear limitations on how we can use information.

2.6 Personal data must be adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed. We will anonymise personal data wherever possible to reduce the risks to the data subjects concerned.

2.7 Personal data must be accurate and, where necessary, kept up to date; reasonable steps must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified in a timely manner.

2.8 Personal data must be kept for no longer than is necessary for the purposes for which the personal data are processed, see the records management policy for more information.

2.9 Appropriate technical or organisational measures must be adopted to ensure security of personal data, including protection against accidental or unlawful destruction, loss, alternation, unauthorized access to, or disclosure.

2.10 We are committed to accountability in our work. Under GDPR, we are responsible for and are required to be able to demonstrate compliance with these principles.

3 Data protection standards

3.1 We are committed to meeting our obligations under data protection legislation complying with the data protection principles and ensuring data is processed fairly. We will:

3.1.1 Observe the law and abide by the principles of the data protection legislation.

3.1.2 Only use personal data in ways relevant to carrying out our legitimate purposes and functions as a charity and in ways that are not harmful to the interests of individuals. Data Subjects will be informed about how we will use their data at the time of collection and, where it is appropriate, will be asked to provide consent to use data by way of signed consent form.

3.1.3 Take due care in the collection and storage of all personal and special category data. Data about individuals will be kept secure with appropriate physical security procedures or through controls over the computer network as set out in the information security policy.

3.1.4 Work to ensure that our people understand their responsibilities under data protection legislation and abide by it when processing data, through appropriate training and guidance.

3.1.5 Our people will keep data accurate, timely and secure. Data will be retained in accordance with our records management policy and related retention schedules.

3.1.6 Keep notifications/ registrations with the Information Commissioner's Office (ICO) up to date.

3.1.7 Appoint a dedicated Data Protection Officer (DPO) as required by the data protection legislation.

Privacy Notices

3.2 Either before or at the time of collection of any personal data by us, we are required to inform data subjects about what kind of personal data we collect, the reason for collecting the data, the purposes of the processing, the legal basis which we are relying on, the data subjects' rights in relation to that data, security measures taken in relation to data, whether we transfer data to third parties, the retention period and any potential transfers of data outside of the EEA.

3.3 We provide this information to data subjects in our Privacy Notice. We will ensure that the Privacy Notice is kept up to date.

Data Subject Rights

3.4 Data Subjects are entitled to the following rights and we agree to honour those rights and comply with requests made by data subjects under those rights:

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.

The right of access	Data subjects can make what is known as a Subject Access Request ("SAR") to request information about the personal data we hold about the data subject (free of charge, save for reasonable expenses for repeat requests). For more on SARs please refer to the Subject Access Request Guidelines and Procedure
The right to correction	Data subjects have a right to require that any incomplete or inaccurate information is corrected.
The right to erasure (the 'right to be forgotten')	Data subjects have a right to require that we remove data we hold about them, unless we have reasonable grounds to refuse the erasure.
The right to restrict processing	Data subjects can request that we no longer process their personal data in certain ways, whilst not requiring us to the delete the same data.
The right to data portability	Data subjects can ask us to provide copies of personal data we hold about them in a commonly used and easily storable format.
The right to object	Unless we have overriding compelling legitimate grounds for such processing, data subjects may 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 data on the grounds of pursuit of our legitimate interests.
Rights with respect to automated decision-making and profiling	Data subjects have a right not to be subject 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.
Right to withdraw consent	If we are rely on consent to process a data subject's personal data, the data subject can withdraw their consent at any time. Even if a data subject has not expressly given their consent to our processing, they also have the right to object (see above).

3.5 We are required to provide data subjects with a reasonable access mechanism to enable them to access their personal data, and must allow them to update, rectify, erase, or transmit their personal data, if appropriate or required by law.

3.6 When requests to access, correct, amend or destroy personal data records are received, we must ensure that these requests are handled within a reasonable time frame and the time frames specified in the data protection legislation. The Information Governance team must also record the requests and keep a log of these.

Authority for Processing Data

3.7 Data processing will only be allowed where there is a clear rationale for the activity. If you are undertaking the processing of personal data and you do not believe it is within the scope of the relevant provisions in our Privacy Notice, please contact the Information Governance team for advice and support.

Special Category Data

3.8 Where special category personal data is being collected, the Information Governance team must make sure that the Privacy Notice explicitly states the purpose for which this sensitive personal data is being collected. The explicit consent of the Data Subject will be required to process this data unless the Information Governance team agrees otherwise in extraordinary circumstances.

3.9 Special category data (sensitive data) will 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.

Consent

3.10 Whenever personal data processing is based on the data subject's consent we must 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.

3.11 Personal data must only be processed for the purpose for which they were originally collected. In the event that we wish to process personal data for another purpose, we may require the consent of the data subject concerned.

Children

3.12 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 must ensure that parental/guardian consent is given prior to the collection.

Disclosures

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

Governance team should be contacted for support and advice on disclosure to third parties.

Transfer of Data to Third Parties

3.14 If we are using any third-party supplier or business partner to process personal data on our behalf, we are responsible for ensuring that the processor has agreed to adopt security measures to safeguard personal data that are appropriate to the associated risks.

3.15 We will also require that certain protections required by the GDPR are included in the contract with that supplier, including that:

- the supplier provides an adequate level of data protection;
- the supplier will only process personal data in accordance with our instructions or to carry out its obligations to us and not for any other purposes.

3.16 If we are processing personal data jointly with an independent third party, we must explicitly agree with that third party our and their respective responsibilities in the relevant contract.

Transfer of Data outside of the EEA

3.17 Before transferring personal data out of the European Economic Area (EEA) we must ensure that adequate safeguards are in place which may include the signing of a relevant agreement or ensuring that an adequacy notice is in place. Before transferring personal data outside of the EEA you must check with the Information Governance team whether or not the transfer meets relevant requirements.

Data Protection Impact Assessments (DPIA)

3.18 In order to maintain compliance with data protection legislation it is important that we identify early whether any new systems, processes, services or projects are likely to impact on data protection. When using our standard business case or service tender template, our people must consider whether there are any data protection implications. If there are, a DPIA must be completed with the support of the Information Governance team.

Legitimate Impact Assessment (LIA)

3.19 When relying on legitimate interest as the lawful basis for processing data, you must complete an LIA with the support of the Information Governance team. A LIA helps determine whether that is appropriate and documents the outcomes of the assessment to serve as evidence for your decision to rely on legitimate interest.

4 Responsibilities

4.1 The owner of this policy on behalf of the Board of Trustees is the Chief Information Officer, who maintains overall legal, compliance and information governance responsibility relating to personal data.

4.2 The Executive Leadership Team are responsible for being champions of data protection good practice in the organisation and ensuring compliance with the Policy within their directorates.

4.3 The organisational lead on data protection is the Head of Information Governance who is responsible for ensuring maintenance and implementation of this policy, advising on data protection issues, liaising with the ICO and providing support on subject access requests.

4.4 Heads of service, departments and line managers are responsible for ensuring compliance with the policy within their areas of responsibility.

4.5 All of our people have a responsibility to meet the obligations in this policy.

5 Training and support

5.1 This policy supports effective risk management by setting out our data protection standards. We take all possible steps to protect information we hold and to minimise the risks associated with accidental disclosure of any confidential personal or sensitive information we hold.

5.2 There is a data protection element in our mandatory Information Governance training module to be completed by all of our people.

5.3 The Information Governance team can provide additional training and support to individuals or teams as required.

6 Monitoring and compliance

6.1 Regular internal audits on compliance with all information governance policies will be undertaken by the internal audit team. Audit findings will inform organisational improvement needs in relation to information security.

7 Reporting

7.1 Data protection and/or information security incidents should be reported in Datix, consistent with the incident reporting policy and procedure.

8 Review and maintenance

8.1 This policy was last reviewed in June 2018 and is next scheduled for review in June 2021. It will be updated earlier as required.

9 Appendices

9.1 Appendix 1: related documents

9.2 Appendix 2: document provenance

9.3 Appendix 3: impact assessments summary

Appendix 1: related documents

Document title	Relationship to this policy
Confidentiality Policy	Ensures confidentiality of personal identifiable and confidential business information and our responsibilities regarding disclosure of such information
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 effective 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 our information classification scheme and information handling standards, and aims to ensure information is appropriately protected from loss, unauthorised access or disclosure.
Information Governance Policy	This is our primary policy under which all other Information Governance policies, procedures and guidance relating to managing information and data reside.
Information Security Policy	Sets out our Information Security 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.
Subject access request - guidelines and procedure	Provides guidelines on how to comply with requests made under the data protection legislation.

Appendix 2: document provenance

Date	Category	Summarise changes made	Reason for changes	Consulted	Endorsed by

March 2014	Interim update	Updated to reflect developments in information governance: add sections on subject access requests, incidents, and privacy impact assessments.	To improve internal practice relating to data protection and ensure compliance.	Key stakeholders.	Head of Legal
April 2017	Interim update	Updated policy to reflect organisational change, extended date of next review, and other minor edits.	Organisational change	Legal, Governance	Chief Finance Officer
May 2018	Scheduled review	Update policy to reflect GDPR and make obligations clear; streamlining as part of scheduled review.	Change to operating environment.	Key stakeholders	Chief Information Officer