BritishRedCross

Business and corporate governance

Confidentiality Policy

This Policy sets out our commitment to the confidentiality of personal identifiable and confidential business information and our responsibilities regarding disclosure of such information.

Policy owner	Chief Information Officer
Policy lead	Head of Information Governance
Audience	All staff, volunteers and contractors (for example, third parties delivering services on behalf of the British Red Cross)
Legislation and regulation	Data Protection Act 1998 Human Rights Act 1998 The Common Law Duty of Confidentiality The Caldicott Principles Equality Act 2010
Formally endorsed by	Board of Trustees
Endorsement date	June 2017
Next review	June 2020

1 Introduction/background

1.1 The British Red Cross recognises it needs to protect and safely process personal identifiable and confidential business information that it gathers, creates, processes and discloses. This policy will provide assurance to our service users, learners, funders, our people and the public whilst meeting legal, regulatory and contractual requirements.

1.2 All of our people are bound by a legal duty of confidence to protect personal identifiable and confidential business information they may come into contact with during the course of their work.

Definitions

1.3 **Anonymised Information** does not identify an individual directly, and cannot reasonably be used to determine identity. Anonymisation requires the removal of name, address, full post code and other details that might support identification.

1.4 **Personal data** means any data by which an individual might be identified (for example: name, address, national insurance number, e-mail address, mobile phone number and IP address).

1.5 **Confidential** means information which is not common knowledge and is of value. This includes personal identifiable information as well as commercially sensitive documents such as contracts.

1.6 **Confidentiality** is protecting information from unauthorised disclosure.

1.7 **Sensitive information** shall have the same meaning as under the Data Protection Act 1998 ("DPA") and the Equality Act 2010, for example information relating to race or ethnic origin, political opinions, religious beliefs or other beliefs of a similar nature, trade union membership, physical or mental health, sexual life, criminal offences/proceedings, disability, pregnancy and maternity.

1.8 **Explicit consent** is when the individual has clearly agreed for information to be disclosed. It is a clear and voluntary indication of preference or choice usually given verbally or in writing and freely given in circumstances where the available options and consequences have been made clear.

1.9 **Implied Consent** means individual's agreement that has been signalled by behaviour of an informed individual.

1.10 **Disclosure** is the divulging or provision of access to data.

1.11 **Our People** are staff, volunteers and contractors (for example, third parties delivering services on behalf of the British Red Cross).

1.12 **Processing** refers to anything done with the information including its collection, recording, use (including viewing), disclosure and destruction.

Purpose and aims

1.13 This Policy supports the overarching Information Governance Policy. It sets out our commitment to the confidentiality of personal identifiable and confidential business information and our responsibilities regarding disclosure of such information.

1.14 The purpose of this Policy is to:

- Ensure our people are aware of their responsibilities for upholding confidentiality and preserving information security.
- Ensure compliance with statutory, regulatory and contractual requirements through the application of legislation and best practice; as well as to facilitate appropriate information sharing arrangements.
- Ensure service users, learners, funders, and our people are aware how their information may be used and, where reasonable, respect conditions requested by individuals to limit the use of their information.
- Establish clear lines of accountability to protect information and support our people in the provision of a confidential service, and to authorise disclosure.
- Ensure valid implied or explicit consent is obtained prior to disclosure.

Scope

1.15 This Policy applies to all of our people, as well as contractors; and applies to all personal identifiable or confidential business information processed by the organisation, whether held in paper, electronic or communicated verbally.

2 Standards

Confidentiality Principles

The following principles must be adhered to:

2.1 Personal identifiable or confidential information must be effectively protected against improper disclosure when received, stored, transmitted or disposed of.

2.2 Access to information must be on a need-to-know basis.

2.3 Disclosure must be limited to that purpose for which it is required. Recipients of disclosed information must respect it is given to them in confidence. If the decision is taken to disclose information, it must be justified and documented. Any concerns must be discussed with either a Line Manager or the Information Governance Team.

2.4 Personal identifiable information, wherever possible, must be anonymised by removing as many identifiers as possible whilst not unduly compromising the utility of the data.

2.5 Access to rooms and offices where personal identifiable or confidential information is stored must be controlled and doors effectively secured. Measures should be in place to prevent oversight of personal identifiable information by unauthorised parties when sharing office space with others.

2.6 At the end of each day, all of our people should make sure their desk tops are clear of any records containing personal identifiable or confidential information. In particular they must keep all records containing personal identifiable or confidential information in recognised filing and storage places that are locked.

2.7 Unwanted printouts containing personal identifiable or confidential information must be put into a confidential waste bin. Discs, tapes, printouts, fax messages must not be left unattended, but filed and locked away when not in use.

Disclosing Confidential Information

2.8 Whether Personal information can be disclosed to others is dependent on a number of factors, including, whether the individual has consented to the information being shared, to whom the information is being disclosed and the reason for its disclosure. The approach may vary according to the individual circumstances - for example, considerations in disclosing personal information to the police will be different to disclosing information for research purposes.

2.9 To ensure that information is only shared with the appropriate people in appropriate circumstances, care must be taken to confirm they have a legal basis for access to the information before releasing it. It is important to consider what information is required before disclosing it, and only the minimal amount necessary is disclosed.

2.10 Information can be disclosed:

- When effectively anonymised.

- When required by law or under a court order. In this situation our people must discuss with their Line Manager or the Head of Legal before disclosing, who will inform and obtain approval of the Caldicott Guardian.
- In identifiable form, when it is required for a specific purpose, with the individual's explicit consent.
- In Child Protection and Vulnerable Adults' proceedings, if it is considered that the information required is in the public or child's/vulnerable adult's interest. In this situation our people must discuss with their Line Manager, the safeguarding and protection officers or the Information Governance Team before disclosing, who will inform and obtain approval of the Caldicott Guardian.
- Where disclosure can be justified for another purpose, this is usually for the protection of the public and is likely to be in relation to the prevention and detection of serious crime. In this situation our people must discuss with their Line Manager or the Information Governance Team before disclosing, who will inform and obtain approval of the Caldicott Guardian.

2.11 If our people have concerns about disclosing information they must discuss this with their Line Manager and/or safeguarding adults officer (for adult safeguarding matters) or safeguarding and protection officer (for children safeguarding matters) or the Information Governance Team.

2.12 Care must be taken in transferring information to ensure that the method used is secure. In most instances an Information Sharing Agreement will have been completed before any information is transferred, which will set out conditions for use and identify the mode of transfer. For further information contact the Information Governance Team.

2.13 Our people must ensure that appropriate standards and protections are in place in respect of telephone enquiries, e-mails, faxes and surface mail. See the Procedure for the secure transfer and receipt of information for guidance on the safe transfer of confidential or personal identifiable information.

2.14 Transferring confidential information by British Red Cross email to anyone outside the British Red Cross network may only be undertaken by using encryption.

2.15 Sending personal confidential information via email to individuals is permissible, provided the individual has explicitly consented and they have been informed of any potential risk.

Working Away from the Office Environment

2.16 There will be times when our people may need to work from another location or whilst travelling. This means that these staff and volunteers may need to carry information with them which could be confidential in nature e.g. on a laptop, USB

stick or paper documents. When carrying personal identifiable or confidential information they must ensure the following:

- It is in a sealed non-transparent container (i.e. windowless envelope or suitable bag) before being taken out of our buildings.
- It is kept out of sight whilst being transported.
- Minimise the amount of personal identifiable information that is taken away from our premises.
- When working away from our premises our people must ensure that their working practice complies with corporate policies and procedures. Any removable media must be encrypted as per the Information Security Policy and securely destroy any confidential information if not needed, don't put it in your re-cycle bin at home when you are finished with it.
- To ensure safety of confidential information our people must keep them on their person at all times whilst travelling and ensure that they are kept in a secure place if they take them home or to another location. Confidential information must be protected at all times and kept in lockable locations.

2.17 If our people do need to take personal identifiable or confidential information home, they have personal responsibility to ensure the information is kept secure and confidential. This means that other members of their family, friends or colleagues must not be able to see or have access to the information.

2.18 Our people must not forward any personal identifiable or confidential information via email to their home e-mail account, nor use or store personal identifiable or confidential information on a privately owned computer or device.

2.19 For further guidance on maintaining the confidentiality and security of personal information whilst in transit, please refer to the Information Security Policy.

Carelessness

2.20 All of our people have a legal duty of confidence to keep personal identifiable or confidential information private and not to divulge information accidentally.

2.21 Our people may be held personally liable for a breach of confidence and must not:

- Talk about personal identifiable or confidential information in public places or where they can be overheard.
- Leave any personal identifiable or confidential information lying around unattended, this includes telephone messages, computer printouts, faxes and other documents, and
- Leave a computer terminal logged on to a system where personal identifiable or confidential information can be accessed, unattended.

2.22 Steps must be taken to ensure physical safety and security of confidential information held in paper format and electronically.

2.23 Passwords must be kept secure and must not be disclosed to unauthorised persons. Our people must not use someone else's password to gain access to British Red Cross information and action of this kind will be viewed as a serious breach of confidentiality. This is a disciplinary offence and constitutes gross misconduct which may result in summary dismissal. For further guidance on disciplinary, please refer to the Disciplinary Policy and Procedure and the Volunteer Complaints, Issues and Concerns Policy.

Abuse of Privilege

2.24 It is strictly forbidden for our people to knowingly browse, search for or look at any information controlled by the British Red Cross that relates to themselves, or other persons, without a legitimate purpose. Action of this kind will be viewed as a breach of confidentiality and of the Data Protection Act.

2.25 When dealing with personal identifiable or confidential information of any nature, our people must be aware of their personal responsibility, contractual obligations and undertake to abide by the policies and procedures of the British Red Cross.

2.26 If our people have concerns they should discuss it with their Line Manager or the Information Governance Team. If the concerns relate to safeguarding matters they should discuss it with a safeguarding and protection officer (for children safeguarding matters) or the Information Governance Team.

3 Responsibilities

3.1 The Chief Information Officer has been nominated as the **Senior Information Risk Owner (**SIRO). The SIRO is the designated owner of this Policy at ELT level with overall responsibility to lead on Information Governance and foster a culture that values, protects and uses information for the success of the organisation, and the benefit of both our service users and our people.

3.2 The **Chief Medical Advisor has been nominated as the Caldicott Guardian**. The Caldicott Guardian is responsible for leading on confidentiality relating to personal identifiable information of people who use British Red Cross services in the UK and for overseeing all arrangements including protocols and procedures, for the use and sharing of personal identifiable information as well as ensuring that confidentiality requirements are reflected in our strategies, processes, policies and procedures.

3.3 The **Executive Director of People and Learning** is responsible for ensuring that the contracts of all staff and mutual expectation of volunteers are compliant with the requirements of this Policy and that confidentiality is included in inductions and trainings for all our people who have access to confidential, personal and sensitive information.

3.4 The **Head of Information Governance** is responsible for maintaining this Policy, providing advice on request to any member of staff and volunteer and ensuring

training is provided to our people to further understanding of the principles and their application.

3.5 All **Line Managers** are responsible for ensuring that this Policy and its supporting standards and guidelines are built into local processes and that there is ongoing compliance. They must ensure that any breaches are reported and investigated.

3.6 It is the responsibility of our people to adhere to this Policy, with confidentiality a core obligation for all staff and volunteers.

3.7 There is a confidentiality clause in staff contract and volunteers' mutual expectations.

3.8 **Our people** are expected to participate in induction, training and awareness raising sessions to confirm their responsibilities to uphold confidentiality. They should report any confidentiality risks they identify, or confidentiality incidents, through the Datix electronic incident reporting system.

3.9 Any breach of confidentiality, inappropriate use of service user, learner, funder, staff or volunteer records or abuse of computer systems is a disciplinary offence, which could result in dismissal or termination of employment and withdrawal of volunteering' For further guidance, please refer to the Disciplinary Policy and Procedure and the Volunteer Complaints, Issues and Concerns Policy.

4 Laws and regulations

4.1 There are a range of legal, regulatory and contractual provisions that limit or prohibit the use and disclosure of information in specific circumstances. This section sets out the key points our people should know.

Data Protection Act 1998

4.2 The Data Protection Act imposes constraints on the processing of personal information in relation to living individuals. It identifies eight data protection principles that set out standards for information handling. In the context of confidentiality, the most significant principles are:

- The 1st, which requires processing to be fair and lawful;
- The 2nd, which requires personal data to be processed for one or more specified and lawful purposes, and;
- The 7th, which requires personal data to be protected against unauthorised or unlawful processing and against accidental loss, destruction or damage.

4.3 Further explanation of the Data Protection Principles can be found in the Data Protection Policy.

Human Rights Act 1998

4.4 Article 8 of the Human Rights Act establishes a right to 'respect for private and family life'. This underscores the duty to protect the privacy of individuals and preserve the confidentiality of their personal identifiable information.

4.5 The Act also requires that any intrusion into the private and family life of an individual must be in accordance with the law, proportionate and necessary for one of the following reasons: national security; public safety; the economic well-being of the country; for the prevention of disorder or crime; for the protection of health or morals or for the protection of the rights and freedoms of others.

Equality Act 2010

4.6 The Equality Act 2010 legally protects people from discrimination in the workplace and in wider society, with nine protected characteristics. Further information can be found in the Equality and Diversity Policy.

The Common Law Duty of Confidentiality

4.7 The common law duty of confidentiality means that information confided by an individual or otherwise obtained (e.g. when receiving service), where it is expected that a duty of confidence applies, should not generally be used or disclosed further, except as originally understood by the confider or with their subsequent permission. This duty may be set aside and confidential information disclosed where it is it is a legal requirement to do so or in the public interest. 'Public interest' is an exceptional circumstance that justifies overruling the right of an individual to confidentiality in order to serve a broader societal interest. Decisions about the public interest are complex and must take account of both the potential harm that disclosure may cause and the interest of society in the continued provision of confidential services.

The Caldicott Principles

4.8 The Caldicott Principles provide guidance on the use and protection of personal confidential data, and emphasise the need for controls over the availability of such information and access to it. As a provider under contract of NHS services, we were required to appoint a Caldicott Guardian who is responsible for compliance with the confidentiality principles.

4.9 The seven Caldicott Principles are:

1. Justify the purpose for using or sharing person identifiable information.
2. Only use person identifiable information when absolutely necessary.
3. Use the minimum necessary person identifiable information.
4. Access to person identifiable information should be on a strict need to know basis.
5. Those handling person identifiable information should be aware of their responsibilities.

6. Understand and comply with the law: Every use of person identifiable information must be lawful.

7. The duty to share information can be as important as the duty to protect patient confidentiality.

5 Monitoring and compliance

5.1 All risks and incidents relating to Confidentiality must be reported using the Datix electronic incident reporting system. The Incident Reporting Policy and Procedure provides more guidance on this process.

5.2 Reporting of risks and incidents is important to ensure that appropriate action is taken so that risks/incidents do not reoccur and we learn from them.

5.3 Regular internal audits on compliance with all Information Governance policies will be undertaken. Findings will inform continuous organisational improvement (e.g. training, policy development, and communications).

6 Training and support

6.1 In order to support our people to meet the standards set out in this Policy, an Information Governance training module has been developed. This can be accessed from the eLearning Platform, as well as via our intranet site Red Room.

7 Review and maintenance

7.1 This Policy is next scheduled for review in June 2020.

Appendix 1: related documents

The British Red Cross will maintain the following key policies and procedures to support effective Information Governance:

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 Audit Procedures	This procedure sets out the arrangements for routine internal audits in relation to confidentiality.
Data Protection Policy	Sets out our data protection responsibilities.
Data Quality Policy	Sets out a framework to ensure a high standard of data quality across information collected.
Disciplinary Policy and Procedure	The purpose of the disciplinary policy and procedure is to ensure we operate effectively, and to promote and support the value we place upon expected behaviours and conduct of our staff.
Equality and Diversity Policy	This policy details how the British Red Cross will treat all volunteers, employees, contractors and stakeholders with dignity and respect, regardless of age, disability, gender reassignment, marriage and civil partnership, pregnancy and maternity, race, religion or belief, sex and sexual orientation
Incident Reporting Policy and Procedure	Supports the effective identification, reporting, managing and learning from incidents as an important part of managing risk, improving our services, protecting our people and those who use our services.
Information Governance Policy	This is the primary policy under which all other Information Governance policies, procedures and guidance relating to the management of information and data reside.
Information Security Policy	Ensures 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.
Safeguarding Adults at Risk Policy; and Safeguarding Children and Young People Policy	These policies providing a clear framework for our approach to safeguarding adults, children and young people.
Volunteer Complaints, Issues and Concerns Policy	This policy and procedure ensures volunteer complaints, issues and concerns by or about volunteers are handled in a consistent, fair and transparent way.

Appendix 2: document provenance

Date endorsed	Category	Summarise changes made	Reason for changes	Consulted	Changes endorsed by
January 2007	New	New Policy drafted.	N/A	Key stakeholders.	Board of Trustees
January 2014	Interim update	Next review date added.		People and Learning	Head of Reward and Recognition
August 2016	Interim update	Push back the review date to January 2017.	Due to changes taking place within the P&L directorate	People and Learning	Head of Reward and Recognition
November 2016	Interim update	Removed reference to 'human resources'.	Made relevant changes to document with HR becoming P&L Advice and Support.	People and Learning	Head of Reward and Recognition
January – April 2017	Scheduled review	Significant changes to the policy to ensure it is fit for purpose.	Scheduled review of policy	All directorates.	Board of Trustees

Appendix 3: equality impact assessment

An equality impact assessment was completed on this policy. Some amendments were made to acknowledge the complexities involved in the confidentiality of the protected groups. If you would like a copy of the completed assessment, please contact the policy lead, the Head of Information Governance.

Appendix 4: Reporting of Policy Breaches

What should be reported?

Misuse of Personal data and security incidents must be reported so that steps can be taken to rectify the problem and to ensure that the same problem does not occur again.

All breaches should be reported to the Information Governance Team. If staff and volunteers are unsure as to whether a particular activity amounts to a breach of the policy, they should discuss their concerns with their Line Manager or the Information Governance Team. The following list gives examples of breaches of this policy which should be reported:

- Sharing of passwords.
- Unauthorised access to the British Red Cross systems, either by staff, volunteers or a third party.
- Unauthorised access to information without a need to know.
- Disclosure of information to a third party without justification, and you have concerns that it is not in accordance with the Data Protection Act and Duty of Confidentiality.
- Sending information in a way that breaches confidentiality.
- Leaving information unattended in a public area.
- Theft or loss of Personal-identifiable or confidential information.
- Disposal of information in a way that breaches confidentiality i.e. disposing of Personal identifiable information in ordinary waste paper bin.

It is not possible to provide detailed guidance for every eventuality. Please contact the Information Governance Team with any queries.

Reporting of Breaches

A regular report on breaches of confidentiality is presented to the Information Governance Steering Group, to enable monitoring of compliance and continuous improvements to be made to our internal processes.