Care of Information

(STANDARD)

Type	Standard
Current Version	2.1
Last Reviewed	22/07/2021
Next review	07/2024
Review Interval	3 Years
Distribution	Internal: [Confidential], [Non-confidential] External: [Not permitted], [As per request]
Document Owner	Data Protection Officer

1. Scope

Information needs to be protected throughout the lifecycle of any system – from inception, design, implementation, Business as Usual, and finally, decommissioning.

The Scope of this Standard covers all IT and Information Security work performed by the IS Department when managing and handling all types of information.

a. Purpose

Barnardo's IT systems are useful tools to help us work with the information that is part of our daily working lives. However, care of information isn't just 'an IT thing' about information on PCs, USB memory sticks or in emails – it involves thinking about printed paper documents, notes in notebooks and diaries, Faxes, even conversations that may be overheard.

As part of Barnardo's Information Security Management System, this document shall be reviewed at least annually by the Information Security Officer or assigned delegate. It shall be maintained to:

- ensure compliance with current legal and regulatory requirements,
- maintain compliance with ISO/IEC 27001 requirements,
- contribute to risk mitigation arising from Barnardo's current Information Security Risk Analysis and approved Risk Treatments.

b. Policy Statements

The Care of Information Standard derives its Policy statements from the Barnardo's Data Protection Policy which can be found

https://barnardosorguk.sharepoint.com/:w:/r/sites/ISMSLibrary/_layouts/15/Doc.aspx?sourcedoc=%7B726E149A-FB3C-4164-A44C-895CC9477733%7D&file=Data%20Protection%20Policy%20-%202021.docx&action=default&mobileredirect=true

c. Responsibilities

This document is intended for all staff within the Digital and Technology team and should be followed for all elements of work that is undertaken.

This document defines what we need to do to ensure that information is used effectively and safely so that:

- Information is made available to those who have a right and need to use it (not withheld unnecessarily).

- Information is maintained to avoid accidental loss or corruption.
- Information is protected, appropriate to its sensitivity.

If we get it wrong….

- overprotecting information is wasteful and can make it difficult to do the work we need to. On the other hand, ...
- not protecting something that needs to be protected could have very serious consequences: Barnardo's business reputation could be damaged, and the organisation could be subject to legal action, impacting our future work. If the information involves details about people, that may cause them distress or even put their safety at risk.

2. Standard

1. Information Classification and Sharing

1.1. Within Barnardo's, there are many types of information, and each has different sensitivities associated with it.

1.2. It is important that the information types can be identified and quickly understood to ensure that they are handled with the appropriate care.

See the Information Sharing Policy for complete information on sharing and handling information – the sections below provide a guide for the IS Department to follow.

1.3. The following descriptions are designed to help you identify the kind of information that you are using – and we'll use these later to clarify how to care for each type:

	What is it?	**Examples are…**
"Unrestricted"	Any information that could reasonably be made available to the general public.	Annual Reports, advertising material, brochures and Internet site information.
'Confidential' information	Anything that may be considered to be "Confidential to Barnardo's" Any information that relates to an individual and, hence, may be covered by the DPA. Information about our internal business processes that enable us to retain a position as a trusted service. Any information that if released could put individuals or Barnardo's reputation at risk.	Staff directory Business plans, financial information, personnel files, intellectual property. Client information including sponsor and donor information. Any commercial correspondence between Barnardo's and third parties.
'RESTRICTED' information	Detailed information which relates to the commercial and operational strategy of our business. Any information that relates to an individual's sensitive personal data and, hence, may be covered by the DPA.	Details of employee disciplinary hearings Company commercial forecasts, board strategy documents IT system technical information. Operational security details. Highly sensitive client, donor and sponsor information.

2. Creating and storing information

2.1. See Section 6 'Document creation, approval and issue control' which describes the basic information to be included in a document that will help readers to understand if they have a current, approved version.

2.2. There are no mandatory requirements for 'Unmarked' information.

2.3. The following instructions relate to the careful control of information that may be communicated in several formats.

What you are doing	How to handle Confidential information	How to handle RESTRICTED information
Marking of emails, Faxes, documents and notes.	Marked at the top with the word: "Confidential" All pages must be numbered	Marked at the top with the word: "RESTRICTED" All pages must be marked as page x of y (e.g., Page 7 of 14).
Storing paper Faxes, printed or photocopied documents and notes.	Paper documents may be left for short periods during the day. Ideally, they should be stored safely if left unattended for an extended period	Paper documents must not be left unattended unless in a drawer or cabinet.
Storing 'electronic' information (e.g., emails, Word documents and Excel spreadsheets, etc.)	All Barnardo's Confidential information shall only be stored on Barnardo's central IT Systems (e.g., Outlook and Content Server). It is not permitted to store Confidential data on portable devices (e.g., Laptops and mobile phones\tablets). It is permitted to hold confidential data on encrypted portable devices where access is required to undertake duties and access to central IT systems is not available.	All Barnardo's RESTRICTED information shall only be stored on Barnardo's central IT Systems (e.g., Outlook and Content Server), in a confidential area where possible. It is not permitted to store RESTRICTED data on portable devices (e.g., Laptops and mobile phones\tablets). It is permitted to hold RESTRICTED data on encrypted portable devices where access is required to undertake duties and access to central IT systems is not available.

	Users should lock their workstation when away from their desk	Users should lock their workstation when away from their desk

3. Exchanging information with other people

3.1. The following instructions relate to the careful handling and transferring of information that may be communicated in a number of formats.

What you are doing	How to handle Confidential information	How to handle RESTRICTED information
Transferring information within Barnardo's	**Email** Avoid the need to email an attachment by referring the recipient to the folder location of the information in Content Server. **Paper records** Paper records shall only be sent through the internal post system, marked with the recipient's name.	**Email** Avoid the need to email an attachment by referring the recipient to the folder location of the information in Content Server. Emails should also be sent with their sensitivity set to "Confidential". **Paper records** Paper records shall only be sent through the internal post system, marked RESTRICTED and with the recipient's name.
Transferring information outside of Barnardo's	**Email** Send the item in an encrypted form, using the encrypted email service. **Other electronic Media** Any information that is sent using removable media – eg CD, USB Stick or similar must be encrypted, and the password communicated separately. **Paper records**	Authorisation must be obtained in advance from either the relevant AD or the Information Security Officer. **Email** Send the item in an encrypted form, using the encrypted email service. **Other electronic Media** Any information that is sent using removable media – eg CD, USB Stick or similar must be encrypted, and the password communicated separately.

	Paper records shall be marked as "Private and Confidential". **Non-disclosure agreements and/or Data Processing clauses must be contractually in place with the recipient.**	**Paper records** Paper records shall be marked as "Private and Confidential". **Non-disclosure agreements and/or Data Processing clauses must be contractually in place with the recipient.**
Faxing	Only send a Fax when it has been determined that the intended recipient is available to collect the fax immediately.	This may be permitted in exceptional circumstances only; authorisation must be obtained in advance from either the relevant AD or the Information Security Officer.
Phone conversations	At all times - be aware of how your voice may be overheard. Do not discuss Confidential information in public places.	At all times - be aware of how your voice may be overheard. Do not discuss RESTRICTED information in public places. Do not leave RESTRICTED information on voicemail, follow-up with another call later.

4. Disposal of information that is no longer needed

4.1. The following instructions relate to the destruction of paper records and data media.

What you are doing	How to handle Confidential information	How to handle RESTRICTED information
Destruction of paper records	Ensure documents are physically shredded or disposed of in one of the confidential waste sacks.	Ensure documents are physically shredded or disposed of in one of the confidential waste sacks.
Destruction of data media (e.g. CDs, DVDs, USB hard drives or USB memory sticks)	Physically destroy removable media when no longer needed.	Physically destroy removable media when no longer needed.

5. Retaining information for reference

5.1. All information is retained and preserved in line with current legislative and regulatory rules about how long records and individual documents are preserved for use.

5.2. Dependent upon operational needs, retained information may be held in offsite archive locations as defined by the Data Protection Policy

6. Document Creation, Approval and Control

6.1. Format and control information

Although it is desirable for these instructions to be followed for all documents created by the IS department, they are only mandatory for documents classified as RESTRICTED.

6.1.1. Authors shall take advice from the 'Definition of Framework Documentation' found under the Information Security Framework Management section as to the generic format or template to use for any document type (e.g., policy, Standard, Procedure, Plan or Record)

6.1.2. Where possible, changes to existing documents shall be highlighted. For example, Word document authors should make use of functionality to 'track changes'. As a minimum, each document shall include:

6.1.2.1. a title cover sheet including the current copyright statement

6.1.2.2. a document reference, where this is different from the title

6.1.2.3. identification of the author (s)

6.1.2.4. the document versions or issue number

6.1.2.5. the document issue date

6.1.2.6. a change history table

6.1.3. Version numbers shall take the form "a.b" where "a" and "b" are integers. Draft version shall commence "a.1" and progress through "a.2", "a,3" etc. Definitive version shall follow the sequence "1.0", "2.0" etc.

6.1.4. Draft documents should include the version number in the file title for clarity.

6.2. Approval

6.2.1. All documents shall be subject to peer review by the responsible manager and nominated experts as may be needed.

6.2.2. Review comments may be recorded by email, hand-written on printed copies or marked up electronically within a version of the document under review (this file shall be renamed to avoid the original being overwritten).

6.2.3. Evidence of approval shall be recorded prior to issue. This may be by physical signature on a printed copy or electronically by email or other means. The document information (version number, etc.) shall be updated to reflect this. Approved documents should include the version number in the file title for clarity.

6.3. Issue control

6.3.1. Content Server is Barnardo's adopted system for storing and recalling all electronic documents and records.

6.3.2. Information about how to use Content Server effectively is in the training information provided online.

Group-based access control in Content Server makes folders available to defined groups of staff.

6.3.3. These may be confidential (only visible to the group members) or visible to other staff on a read-only basis.

6.3.4. Content Server presents the last stored version to users, retaining previous versions for retrieval if needed.

To help with the control of documents in Content Server:

6.3.5. A folder should be created for draft documents as they are developed to avoid confusion about which document to use and to prevent accidentally overwriting the current approved version in use.

6.3.6. If a document has a defined set of users (for example, an instruction or 'how to' guide for administrators) then those staff should be notified by email when a new version is made available for them to use in Content Server.

6.4. Information Back-up and Restoration

As noted above, Content Server presents the last stored version of documents to users, retaining previous versions for retrieval if needed. If it appears that a record or individual document cannot be located, please contact the Information Services Helpdesk for help. If necessary, information can be restored from their back-up media.

6.4.1. Content Server data is backed up routinely as defined in the backup routine.

6.4.2. If Content Server is unavailable, recovery actions defined in the business continuity plan will be started to restore this as soon as practicable.

6.4.3. Paper-based information is securely stored as described above. At the discretion of the information owner, paper-based records considered critical to Barnardo's may be scanned into an electronic format and stored in Content Server as a back-up strategy.

3. Associated Legislation, References, and Documents

1. *The UK General Data Protection Regulation (UK-GDPR) is the UK law that aligns with EU GDPR 2018 replacing the Data Protection Act 1998 in the UK.*
2. *The Data Protection Act 2018: is the UK's implementation of the General Data Protection Regulation (GDPR). Everyone responsible for using personal data must follow strict rules called 'data protection principles'.*
3. *ISO/IEC 27001:2013: is a specification for an information security management system (ISMS). An ISMS is a framework of policies and*

procedures that includes all legal, physical and technical controls involved in an organisation's information risk management processes.

4. *PCI-DSS: Is a standard designed to create a secure environment for companies that accept and process card transactions and consumer data.*

5. *NHS DSPT: The Data Security and Protection (DSP) Toolkit is an online tool that enables Barnardo's to measure performance against the data security and information governance requirements mandated by the Department of Health and Social Care (DHSC), notably the 10 data security standards set out by the National Data Guardian in the 2016*

6. *Gambling Commission RTS:*

7. *Barnardo's IT Code of Practice*

4. Enforcement

Any employee found to have violated this Standard may be subject to disciplinary action, up to and including termination of employment.

5. Revision History

This is the revision history section.

Version	Date	Author	Status	Note
0.1	15/10/2009	S Johnson	For review	Initial draft for review
0.2	18-08-2010	Rob Pyatt	For review	Extensive reworking of original text to make it easier to read. Released as document 7-2-2_-_data_classification_policy
0.3	28-02-2011	S. Johnson	For review	Proposed revision for business-wide communication
0.4	31-5-2011	Rob Pyatt / Chris Page	For review	Reviewed to accommodate smaller scope. Simplified to remove classifications that are not going to be used. Tidied up formatting.
0.5	13-6-2011	Rob Pyatt	For review	Changed following discussions with IS director.
0.6	15-6-2011	Rob Pyatt	For review	Further changes to align with business practice.
0.7	15-6-2011	Chris Page	For review	Following review with IS Director
1.0	16-6-2011	Rob Pyatt & Chris Page	For approval	Now definitive version following final review by IS Director.

1.1	26-7-2011	Rob Pyatt	For review	Corrected wording in Restricted column on Page 6 and added "Other electronic Media"to Transferring information outside of Barnardo's
1.2	07/08/2013	Chris Page	For review	Review
2.0	23-8-2013	Bob Darby, Chris Page	For approval	Reviewed and approved. Now a definitive version
2.0	10-8-2018	Rob Pyatt	For review	Reviewed. No changed necessary
2.0	6-3-2019	Rob Pyatt	For review	Reviewed. No changes necessary
2.0	19-02-2020	Steve John	For review	Reviewed. No changes necessary
2.1	28-07-2021	Phil Cordey	For review and approval	Document refreshed and updated to fall in line with Data Protection Policy
2.2	04/2022	Martine King & Mustafa Mustafa	For Review	Updated to reflect new classifications and extended review period (3 years)