Information Security Policy

Type	Policy
Current Version	5.1
Last Reviewed	29/11/2022
Next review	11/2024
Review Interval	24 months
Distribution	Internal: [Confidential], External: [Not permitted], [As per request]
Document Owner	Information Security Officer

1. Purpose

Information plays a crucial role in helping Barnardo's achieve its aims - to work alongside the most vulnerable children and young people. Therefore, it is critical to Barnardo's business that the confidentiality, integrity and availability of information are maintained.

The purpose of this Policy is the protection of the confidentiality, integrity and availability of Barnardo's information assets from threats, deliberate or accidental, internal or external. Barnardo's uses ISO27001 as a framework to manage information security.

The achievement of Information Security objectives builds upon everybody's commitment, with each employee made fully aware that security is the outcome of everybody's behaviour, and that negligence of a single individual can frustrate the collective effort. Everyone is expected to respect and adhere to the security provisions issued by the organisation, and to cooperate with our Security Controller by reporting any weakness in the information security protection system and by providing suggestions for improvement.

2. Scope

This is scope of the policy The scope of this policy extends to:

- All information processed by Barnardo's, especially:
  - Personal Data (including sensitive personal data)
  - Business information.
- All IT Systems used in support of Barnardo's operational activities to store, process and transmit information.
- All users of Barnardo's Information Systems and equipment. This includes, but is not limited to employees, contractors, agency workers, secondees and volunteers.
- All external companies that provide contracted information services to Barnardo's.

Adherence to this policy should be considered in conjunction with Barnardo's other statutory and regulatory requirements.

3. Terms and Definitions

- **Confidentiality** - Information is secure and only made available to staff who need to use it.
- **Integrity** - Information is accurate and complete, and is used safely and reliably.
- **Availability** - Information is accessible and useable when required by authorised users.
- **ISO27001** - The international information security standard.
- **PCI-DSS** - Payment Card Industry Data Security Standard
- **Asset** - Anything that has value to the organisation.
- **Control** - Means of managing risk, including policies, standards, procedures or processes.
- **Information Security** - Preservation of confidentiality, integrity and availability of information
- **Risk** - Combination of the probability of an event and its consequence.
- **Third Party** - Person or body that is recognised as being independent.
- **Threat** - Potential cause of an unwanted incident, which may result in harm to a system.
- **Vulnerability** - Weakness of an asset that can be exploited by one or more threats.

4. Policy

The objective of this Policy is the protection of Barnardo's information assets. **They need protection from threats, deliberate or accidental, internal or external.** Barnardo's uses the ISO27001 standard as a framework to manage information security.

To support this objective, the Directors of Barnardo's accept their role in being fully accountable for information security and are committed to ensuring:

- Information is protected from all threats, whether internal or external, deliberate or accidental.
- Information is only accessible to authorised persons from within or outside the company.
- Confidentiality of information is maintained.
- Integrity of information is maintained throughout the process.
- Business Continuity plans are established, maintained and tested.
- All personnel are trained on Information Security and are informed that compliance with the policy is mandatory.
- All breaches of information security and suspected weaknesses are reported and investigated.
- Computer resources, information and information processes are consistently protected according to approved organisational security practices, and legal, regulatory and contractual requirements.
- Information shared via IT Systems with partners, stakeholders, service providers and the Government, is managed securely.
- Procedures exist to support the policy, including appropriate technical control measures, passwords and continuity plans.
- Business requirements for availability of information and systems will be met.

The Information Security Policy applies to all forms of information including:

- Speech, spoken face to face, or communicated by phone.
- Hard copy data printed or written on paper.
- Information stored in manual filing systems.
- Communications sent by post / courier, fax, electronic mail.
- Stored and processed via servers, PCs, laptops, mobile phones, PDA's.
- Stored on any type of removable media such as but not limited to CD's, DVD's, tape, USB memory sticks, digital cameras.

Risk Strategy

Barnardo's information risk strategy is aimed at being balanced. On the one hand avoiding unacceptable high risks, but also avoiding overly bureaucratic and expensive controls. It seeks to put controls in place that are proportionate to the level of risk exposure. Formal methods are used to assess and manage risk, consistent with Barnardo's overall approach to risk management.

Associated Guidance and Documents

1. Information Security Management System Framework
2. IT Code of Practice

5. 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 has to 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*

6. Enforcement

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

7. Roles and Responsibilities

The Trustees of Barnardo's are legally responsible for information security**.** The Director of Information Services is accountable for ensuring that cost-effective security and legal controls are implemented that are appropriately matched with identified risks. They are supported in this task by the Information Security Officer, Managers and other users of Barnardo's IT Systems.

The Information Security Officer has the role and responsibility for managing information security at an operational level. The Information Security Officer is responsible for maintaining the Policy, providing advice and guidance on all matters related to the Policy, reporting on and ensuring the Information Security Management System is maintained and continually improved.

All Managers are directly responsible for implementing the policy within their operational areas, and for adherence by staff they are responsible for.

It is the responsibility of all staff, volunteers and contractors to comply with this policy.

8. Revision History

This is the revision history section.

Version	Date	Author	Status	Note
1.0	12-11-2009	Chris Page	Definitive	First Definitive Version
2.0	14-11-2011	Chris Page	Definitive	Definitive Version
2.9	23-8-2016	Rob Pyatt	For Review	Converted into new format – Content unchanged
2.95	13-10-2016	Chris Page Rob Pyatt	Reviewed and approved	Awaiting final review from IS Director
3.0	14/2/2017	Bob Darby	Approved	Definitive Version
4.0	7.4.2020	Martine King	Approved	Updated to reflect GDPR and NHS data Standards
5.0	21.6.2021	Martine King	Approved	Updated to take account of UK-GDPR, additional statutory and regulatory requirements and reflect the PCI-DSS framework
5.1	29.7.21	ISO	Review	Updated to new Policy template, and additional content added.
5.1	29/11/22	Steve John	Reviewed	No changes