Barnardo's
Corporate Policy

Information Governance Policy Statement

Risk Owner:	Data Protection Officer
Supported by:	Senior Information Risk Officer
Date Approved:	April 2022
Date for Review:	April 2025
Distribution	Unrestricted - Internal & External

1. Purpose

The purpose of this statement is to outline Barnardo's commitment and overarching approach to robust information governance.

2. Statement

Barnardo's recognises the following significant Information Governance responsibilities:

- Service users, customers, business contacts, celebrities, politicians, supporters, committee members, staff and volunteers are required to entrust the charity with large volumes of sensitive data. This must remain confidential at all times.

- The movement of sensitive personal and commercial information outside of the organisation's physical perimeter (paper documents, electronic communications, obsolete IT devices) is still the charity's responsibility.

- Service delivery depends on maintaining the confidentiality, integrity and availability of our information resources, even in the event of hardware or facilities failure.

- Barnardo's is subject to regulatory and legislative constraints.

- Barnardo's reputation depends on the appropriate care and security of all and any data within our infrastructure. We have an obligation to protect data and should not take any risks or actions that may potentially violate the confidentiality, integrity, or availability of data; cause unnecessary exposure of them; or violate contractual or regulatory requirements.

Our ambition is to monitor the organisation and to strive to deliver continuous improvements in data privacy. Specifically, the charity pledges to:

- Comply with all relevant regulations and codes of practice

- Act to prevent data privacy breaches of any sort through effective privacy by design, data minimisation, DPIA risk analysis, and appropriate information security management.

- Ensure that all staff and volunteers receive targeted training in data privacy responsibilities appropriate to their roles within the charity.

- Implement a documented strategy to manage data privacy proactively, maximise organisational learning and deliver continuous improvements in data privacy.

These commitments are delivered by the implementation of a documented data protection programme owned by the Senior Information Risk Officer.

The data privacy requirements are actively communicated to all staff and people acting for or on behalf of the charity, or on our premises.

3. Scope

The scope of Information Governance incorporates the following areas as set out in our Information Governance Assurance Framework:
Data Protection, Information Security, Risk and Compliance, Record Management, Data Governance and Data Analytics.

This statement applies to all of Barnardo's and its subsidiaries including all staff, agency workers, contractors and volunteers.

4. Definitions and Key Concepts

We are committed to the following three principles that are essential to all organisations managing personal data:

Availability: Data must be available when and where it is needed. It must be made accessible swiftly and securely for staff as well as within and between organisations.

Integrity: The data must be valid and trustworthy, relevant, up to date, and protected from loss, damage, and unauthorised alteration.

Confidentiality: Personal identifiable data must be handled and used safely

5. Roles and Responsibilities

All staff (including those in roles below)	Processing information, managing records, and complying with security standards and requirements in line with this policy, as well as other related policies and guidance to

	comply with legislative and business requirements
The Chief Executive Officer (CEO) and the Board of Trustees	Ensuring that systems are in place to support compliance with information law, access and management of records, information security and continuity of service
Corporate Leadership Team	Approving and signing off relevant policies
Senior Information Risk Owner (SIRO)	Ownership of the Information Governance Policy. Responsibility for 'managing information risk across the organisation and for ensuring that the data and information assets of Barnardo's are identified, processed, transmitted, stored and used in line with the principles of good information governance and in compliance with Barnardo's legal, statutory and organisational requirements.'
The Caldicott Guardian	Providing advice and oversight to ensure that confidential personal information relating to people who use the services we regulate is obtained, used, handled and shared in accordance with the Caldicott Principles
Data Protection Officer (DPO)	To carry out the tasks under Article 39(1) of GDPR, to: a) Inform and advise on compliance with GDPR. b) Monitor compliance with GDPR. c) Provide advice as regards data protection impact assessments. d) Cooperate with the ICO. e) Act as contact point with the ICO on issues relating to processing. To carry out these tasks with due regard to risks relating to the processing of personal data.

6. Associated Legislation, Guidance, References and Documents

Data Protection legislation sets out essential principles, which are the foundation on which our organisation is bound and measured.

- 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.

- 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'.

- **PECR** are the Privacy and Electronic Communications Regulations. Their full title is The Privacy and Electronic Communications (EC Directive) Regulations

2003. They are derived from European law. They implement European Directive 2002/58/EC, also known as 'the e-privacy Directive'.

- The **Caldicott Report** was a review commissioned in 1997 by the Chief Medical Officer of England due to increasing worries concerning the use of patient information in the National Health Service (NHS) in England and Wales and the need to avoid the undermining of confidentiality because of the development of information technology in the NHS, and its ability to propagate information concerning patients in a rapid and extensive way.

- The UK Caldicott Guardian Council is a subgroup of what's called the National Data Guardians panel. The **National Data Guardian** (NDG) advises and challenges the health and care system to help ensure that citizens' confidential information is safeguarded securely and used properly. The NDG's role is to help make sure the public can trust their confidential information is securely safeguarded and make sure that it is used to support citizens' care and to achieve better outcomes from health and care services. Although sponsored by the Department of Health and Social Care, the NDG operates independently, representing the interests of patients and the public.

7. Compliance and Oversight

In addition to the compliance and oversight arrangements set out under Roles and Responsibilities, the following applies:

- The Risk Owner will ensure that management information demonstrating adherence to and compliance with this Policy is produced and provided to relevant parties as required and on request complete a business self-assessment.
- The Audit and Assurance Team will periodically and independently review adherence to and compliance with this Policy and associated procedures and processes across the Charity in line with their approved audit and inspection plans.

8. Document History

Version	Date	Author	Comments	Approval
4	April 2022	Martine King	Updated to include IG scope	Approved by A&A director – Gursh Bains

9. Distribution

Policy published on Inside Barnardo's: May 2022
Distribution - Unrestricted - Internal & External