Data Protection Policy

Policy Sponsor	Corporate Director, Business Services (SIRO)
Policy Owner	Head of Information Governance/DPO
Date Approved	May 2023
Date for review	Every three years unless there is a significant change
Distribution	Internal and External Use (unrestricted)

1. Purpose

The purpose of this policy is to provide Barnardo's colleagues and others working alongside us with a framework that outlines the appropriate use of personal data in accordance with relevant legislation.

Why does this Policy matter?

- Barnardo's exercises the responsible stewardship of personal data as part of its basis and values. Information plays an important role in enabling Barnardo's to work with children and young people, their parents and carers. We are committed to the organised, confidential and secure collection, creation, retrieval, storage, handling, transfer and preservation of this information; and to identifying and securely destroying information where it has no continuing business, legal or historical significance.

- Data Protection law places obligations on Barnardo's about the collection, use and storage of personal information and we are committed to ensuring the principles of the law including the rights of data subjects are upheld. These rights and obligations are set out in Barnardo's Privacy Notice.

- The UK's data protection regulator, the Information Commissioner's Office (ICO), has powers to impose substantial fines and other sanctions for failure to comply with our obligations and for actual data breaches

- The types of information and data that we are legally required to keep and for how long we should keep it is set out in a range of legislative documentation. The legislation also requires us do not retain data and information about our supporters, colleagues, service users or other people who can be identified where there is no reasonable business need.

2. Scope

This Policy covers the collection, use, storage or transfer of any 'personal data' (including 'sensitive personal data') and other forms of data and information by Barnardo's, or by anyone processing data on our behalf.

Adherence to this policy should be considered in conjunction with Barnardo's other statutory and regulatory requirements, including Privacy and Electronic Communications Regulations (PECR), the relevant Children's Acts and Home's Regulations, Companies Act, Finance Acts, and Health and Safety regulations.

3. Policy

This Policy applies to information and data in all its forms: whether on paper, stored electronically, held on film, microfiche or other media. It includes pictures, video and audio as well as text. It covers information transmitted by post, electronically, and by oral communication (including telephone and voicemail). It applies throughout the lifecycle of the information and data from its creation/collection through its use and storage to its disposal.

When designing or building new products, tools or services, Barnardo's will adhere to privacy by design principles and ensure all aspects of data protection and security are considered by undertaking the following assessments:

- Vendor onboarding Checklist
- Vendor Risk Management
- Processing Activity Assessments
- Data Protection Impact Assessments

When acting as a data controller, joint data controller or data processor, Barnardo's is required to comply with the principles of good information handling. In collecting, handling and processing personal data, Barnardo's will:

- Do so fairly and lawfully and in line with specific purposes
- Ensure that the data is held securely and is as accurate as possible
- Be open and honest with individuals whose information we hold;
- Only hold the data for as long as necessary, and
- Respect Individuals' rights.

Data must not be sent outside of the European Economic Area without special arrangements in place (speak to the HIG/DPO if this is proposed).

Barnardo's operates under the following lawful bases:

- Consent – for marketing emails and to process sensitive information about staff. This means we offer individuals a real choice and control over their data and require a positive opt-in.
- Legitimate Interests – for direct mail to supporters. This means we consider and protect people's rights and interests. A record of a legitimate interest assessments (LIA) must be kept demonstrating compliance.
- Contract, legal obligations and legitimate Interests – for dealing with job applicants, employees, volunteers and trustees. This means we use the contractual legal basis when we need to fulfil our contractual obligations.

- Public Task and Legitimate Interests – for working with service users in Children's Services. This means we process personal data 'in the exercise of official authority', to perform a specific task in the public interest which is set out in the law.

Access to Information

If individuals whose data we process exercise their legal right to make a request about their data, we will respond promptly and in line with the law. This means that our personnel, and anyone working on our behalf, must:

- Understand and maintain clear accountability for data protection.
- Understand our responsibilities when managing and handling data and are therefore appropriately trained and supervised.
- Store information consistently and comprehensively in line with procedures for collecting, storing and using data.
- Promptly and courteously deal with queries about personal data.

Regular reviews will be made of the way we collect, store and use data. More information about how to handle a Subject Access Request can be found here.

Confidentiality, Integrity & Availability

Barnardo's is committed to ensuring the confidentiality, integrity and availability of personal information:

- Confidentiality means ensuring that personal and confidential information is not disclosed – either purposefully or accidentally – to people who do not have the right to see it.
- Integrity means ensuring that data is accurate and unchanged.
- Availability means ensuring that data is available to those who are authorised to see it.

Staff members must only view, process, access or disclose personal data if they "need to know" the information for the purpose of providing Barnardo's services, or the day-to-day operation of the charity. Access to personal data must be limited to the minimum amount of personal data necessary for the purpose. We must make sure that data is kept up-to-date and take reasonable precautions against inadvertent or inappropriate disclosure or access.

Data Classifications

These are Barnardo's data classifications:

	What is it?	**Examples are…**
"Unrestricted" Information	Any information that could be made available to the general public.	Annual Reports, advertising material, brochures and Internet site information.
'Confidential' information	Anything that may 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.

Sharing Data & Information

We often need to share data with third parties for various essential business processes – e.g., for commissioner contracts, analytics software, email marketing, processing data for campaigns, CRM and administration of our employee payroll and benefits. See the Information Sharing Policy for more information.

If you're sharing sensitive or official data, please check with the Barnardo's Helpdesk if you need assistance with Encryption.

If you need to send sensitive or official data by post, you should ensure that it is securely packaged, and the courier collects a signature from the recipient as proof of delivery. Royal Mail and other companies that provide a 'signed for' facility should be used.

Even though we may use service providers and partners who collect, store or use personal data on our behalf, we remain responsible for that data in almost all cases. Therefore, we must ensure that those service providers have suitable systems, procedures and staff in place, have a written contract with us and, in some cases, a Non-Disclosure Agreement (NDA).

Retaining and Disposing of Data & Information

Barnardo's retains information and data for three key reasons:

- To comply with legislation and established best practice;
- To support our day-to-day activities and inform our longer-term planning;
- To tell the essential 'story' of Barnardo's and its activities over time through our archive.

Colleagues must securely dispose of personal data once they are no longer needed for Barnardo's purposes.

Please see the Record Management Policy and Retention Schedule for further information.

Data Breaches

We have a Data Breach Reporting Procedure which governs our approach to managing and reporting breaches whether we are Data Controller or Data Processor. If the breach is notifiable we will contact the ICO within the required 72-hour reporting period.

Use of CCTV

Barnardo's operates CCTV and other monitoring systems including audio. Barnardo's seeks to ensure that its CCTV systems are installed and operated in accordance with applicable law and that the scope, purpose and use of the systems are clearly defined. For more information see: CCTV and Monitoring Devices Policy

4. Definitions and Key Concepts

'Personal data' is any information that relates to an identifiable living individual that is stored electronically or in a searchable paper filing system. Examples include:

- Names and contact details (e.g., phone, email, address);
- Financial information (e.g., credit card, bank details);
- Any other personal details (e.g., family circumstances, medical history and, in some circumstances, photographs of people).

'Sensitive personal data' is data about an individual's racial or ethnic origin, religious or other beliefs, criminal record, sexual life, trade union membership, medical information or political opinions. The law places additional requirements on processing sensitive personal data.

5. Roles and Responsibilities

Roles	Responsibilities
The Senior Information Risk Owner (SIRO)	Mandates how Barnardo's legal and regulatory requirements are maintained and compliance with data protection policies and procedures.
All Managers	Are directly responsible for implementing the policy within their operational areas, and for adherence by colleagues they are responsible for. This includes ensuring their teams have completed the mandatory data protection training.
All trustees, staff and volunteers	that works at, for, or with Barnardo's, including Barnardo's Trustees, committee members, colleagues, advisers, volunteers and contractors has a responsibility to safeguard and protect Personal Identifiable Information (PII) in adherence with this policy, whether it be paper-based or maintained on electronic systems.
The Head of Information Governance/Data Protection Officer	has the responsibility for ensuring Barnardo's complies with the relevant Data Protection laws, maintaining the Policy, providing advice and guidance on all matters related to the Policy, reporting on and developing Data Protection practice.

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) Governs the processing of personal data in the UK by setting legal standards for data minimisation, user rights, lawful processing, accountability, and security.

The Data Protection Act 2018 Supplements and tailors the UK GDPR by defining national derogations, enforcement powers, criminal offences, and specific provisions for law enforcement and intelligence services.

The Privacy and Electronic Communications Regulations (**PECR)**. Regulates electronic marketing, the use of cookies and similar technologies, and confidentiality of communications across electronic channels.

Freedom of Information Act 2000 (FOIA) Provides public access rights to recorded information held by public authorities, subject to exemptions including those related to personal data.

While the organisation is not subject to FOIA as a charity, it supports public-sector bodies that are subject to the Act and therefore handles information in a manner that aligns with FOIA requirements, exemptions, and disclosure expectations where relevant.

Computer Misuse Act 1990
Establishes offences related to unauthorised access to computer systems, which underpins organisational security obligations.

Human Rights Act 1998 (Article 8 – Right to Privacy)
Embeds the right to respect for private life, reinforcing expectations of proportionality and necessity in data handling.

Equality Act 2010
Provides protections for special categories of data relating to protected characteristics and shapes organisational obligations around fair and non-discriminatory processing.

Common Law Duty of Confidentiality
Requires information given in confidence to be handled lawfully and only shared where there is consent, a legal obligation, or an overriding public interest.

7. Compliance and Oversight

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

- The Policy Owner will ensure that management information demonstrating adherence to and compliance with this Policy is produced and provided to relevant parties as required.

- 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. Equality Impact Statement

The organisation shall ensure that data protection practices are assessed for their potential impact on individuals and groups with protected characteristics under the Equality Act 2010. All data processing activities, including the design, review, and implementation of systems, procedures, and controls, must be evaluated for any direct or indirect discriminatory effects. This includes assessing the fairness of data collection methods, the accessibility of information and rights-request processes, the potential for operational or algorithmic bias, and any disproportionate impact associated with the use of special category data. Where risks are identified, appropriate mitigation measures must be implemented to ensure that data handling practices remain equitable, inclusive, and legally compliant.

9. Version History

Document History	Date	Author	Comments	Approval
1	JAN 2017	Cs Head of Business Support	Draft	
2	MARCH 2017	Cs Head of Business Support	Approved	CS Management team
3	SEPT 2017	Cs Head of Business Support	Approved – Policy replaces previous on Information Sharing	CS Management team
4	Aug 2018	Cs Head of Business Support	Approved – updated in line with GDPR	CS Management team
5	MARCH 2019	DPO	Final – updated to reflect corporate policy, replacing directorate policy	CLT
6	MARCH 2020	DPO	Review – SIRO Approved	SIRO
7	MARCH 2021	DPO	REVIEW – SIRO/Risk Committee	SIRO

8	APRIL 2022	DPO	Review and updated to reflect UK GDPR and adherence to regulatory and statutory requirements	SIRO/Risk committee
9	MAY 2023	Head of IG/DPO	Review and updated – privacy by design and to ensure obligations to Data subjects and GDPR principles are referred to.	SIRO/Risk Committee