Barnardo's

Corporate Policy

Data Protection Policy

Sponsor:	Corporate Director – Business Services (SIRO)
Owner:	Head of Information Governance/Data Protection Officer
Date Reviewed:	May 2023
Review Period:	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. 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.

4. Roles and Responsibilities

The Trustees of Barnardo's are responsible for reviewing and approving the Data Protection Policy, receiving and reviewing data protection related reports.

The Corporate Leadership Team have oversight of and consulted on data protection matters.

The Senior Information Risk Owner (SIRO) Mandates how Barnardo's legal and regulatory requirements are maintained and compliance with data protection policies and procedures.

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.

Our **Data Protection Officer** is Martine King, and she can be contacted by using the following email address - dpo@barnardos.org.uk

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.

Everyone 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.

5. 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.	Staff directory Business plans, financial information, personnel files, intellectual property. Client information including sponsor and donor information.

	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.	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 Service Desk if you need assistance.

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 Records Management Policy and Retention Schedule for further information.

Data Breaches

We have a data breach 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 on the policies and procedures relating to CCTV, CCTV and Monitoring Devices Policy.

Procedures and guidance to support this policy can be found on the Information Governance pages on Inside Barnardo's.

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'.

7. Risk Assessment

The Policy Owner, with assistance from relevant individuals, will maintain a risk assessment of information and data sharing risks facing Barnardo's, to inform required changes to this Policy, any associated processes and procedures or training/awareness messages as required.

8. 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.

9. Document History

Version	Date	Author	Status	Approval (by / when)	Comments
1	January 2017	CS – Head of Business Support	Draft		
2	March 2017	CS – Head of Business Support	Approved	CS Management Team March 2017	
3	September 2017	CS – Head of Business Support	Approved	CS Management Team September 2017	Policy replaces previous Policy on Information Sharing
4	August 2018	CS – Head of Business Support	Approved	CS Management Team August 2018	Updated in line with GDPR
5	March 2019	Data Protection Officer	Final		Corporate Policy replacing

					Directorate Policy Updated formatting
6	March 20	Data Protection Officer	Review	SIRO March 20	
7	May 21	Data Protection Officer	Review	SIRO Risk Committee	
8	April 2022	Data Protection Officer	Review and Update	SIRO Risk Committee	Updated to reflect UK GDPR and adherence to regulatory and statutory requirements
9	May 2023	Head of Information Governance and DPO	Review and update	Director of Audit and Assurance	Privacy by Design and ensure obligations to data subjects and GDPR principles are referred to