Barnardo's

Corporate Policy

Information Sharing Policy and Procedure

Sponsor:	Corporate Director Business Services (SIRO)
Owner:	Data Protection Officer
Date Approved:	August 2023
Date for Review:	Every 2 years
Distribution:	Internal and External Use (Unrestricted)

1. Purpose

Why does this policy matter?

- The UK General Data Protection Regulation (UK-GDPR) and Data Protection Act 2018 (DPA18) gives individuals' certain rights regarding their personal data and how it can be shared. Failure to comply with these legal obligations could result in a loss of trust from the public and material fines from the Information Commissioner's Office (ICO).
- Barnardo's has an obligation to safeguard its staff and its service users. Due to the sensitive nature of Barnardo's work, situations will arise where personal data will need to be shared with authorities and other agencies in order to protect individuals and resolve disputes and to ensure cohesive working with strategic partners.

2. Scope

The policy applies to everyone that works at, for, or with Barnardo's. This encompasses Barnardo's trustees, committee members, staff, advisers, volunteers and contractors. The policy refers to any personal data of which Barnardo's is the Data Controller; this is where we determine the nature and scope of data collected. This includes both paper and electronic records, emails, case studies, photographs, video and audio recordings (including CCTV), and additionally any verbally communicated information that has been compiled into notes.

This policy details the relevant grounds used to share information in order for Barnardo's to conduct its daily operations and effectively safeguard children, staff and the public.

The scope of this policy is to outline the key considerations which ensure that Barnardo's shares its data safely and securely.

Adherence to this policy should be considered in conjunction with Barnardo's other statutory and regulatory requirements including the Law Enforcement Directive (LED),

Human Rights legislations and the relevant Children and Young People Acts and the Caldicott Principles.

3. Roles and Responsibilities

All Managers are directly responsible for implementing the Policy within their operational areas and for adherence by all staff they line manage.

It is the responsibility of **all relevant staff, agency workers, contractors and volunteers**, as applicable, to comply with this Policy and to complete relevant training at appropriate intervals.

4. Glossary

Controller	Means the natural or legal person, public authority, agency or other body which, alone or with others, determines the purpose and means of processing personal data. (E.G., what to collect, how to share it and how long to keep it).
Data Subject	Means the living person the personal data relates to.
FOI Act	Means any law, enactment, regulation, regulatory policy, by-law, ordinance Subordinate legislation relating to Freedom of Information, including FOI Act 2000 and FOI (Scotland) Act 2002 as amended or replaced.
Joint Controller	Means the person/organisation will jointly decides what processing activity to undertake.
Personal Data	Means information related to an identified or identifiable natural person
Processing	Means anything which can be done with data including: Creating, collecting, recording, storing, adapting, archiving, deleting, sharing, consulting and using. .
Processor	Means the organisation/person instructed to process the data on behalf of the controller

5. Policy

Barnardo's mission is to achieve better outcomes for more vulnerable children and young people. To achieve this mission, it is necessary to collaborate and share information with other organisations and individuals as part of our daily practice. As Data Controller we must ensure that all data is secure, and individuals' rights are prioritised in line with the Information Commissioner's Office (ICO) guidelines.

Sharing Non-Personal Data

Individuals and organisations have a legal right to make a request under The Freedom of Information Act (FOI) for non-personal information that Barnardo's holds on behalf of a public body or commissioner. Although FOI obligations do not extend to Barnardo's as a charity, we are required to assist and support commissioners and supply them with the information they require to comply with their obligations under FOI legislation. If staff are requested to disclose information, they should first ensure the request is legitimate, ie; from a partner organisation that is subject to FOI, and they should then proceed in line with the relevant commissioner's requirements.

On occasion, requests are received from third parties who we are not required to provide information to under FOI. The decision about whether these requests are fulfilled is based on several factors, such as: legal requirements to share (a criminal investigation or court order); the nature of relationship that Barnardo's has with the requestor; whether sharing will impact any organisational partners; and the strategic importance of the data. Decisions to share data of this nature should not be made in isolation and should be discussed with a senior manager in conjunction with the respective area Data Protection Manager.

Sharing Personal Data – Third party processors

Barnardo's handles large volumes of data. To do this efficiently and effectively, we often use third parties to support us in our work. This could be hosting our data on their platforms, transferring data to a third party for storage or a third party supporting us in developing our reporting. It is vital that any third-party processor we use has the same high standards of data security that we would expect of our own systems. Therefore, we must undertake due diligence of all suppliers to assess the operational and technical capabilities to ensure their security standards are suitable for the nature of processing.

Where Barnardo's employs a third party to process personal data on our behalf they will be designated as Data Processor. Every time we use a Data Processor to process personal data, there must be a Data Processing Agreement in place, which is a written contract that binds the processor to Barnardo's in respect of its processing activities. Where data is transferred outside the UK, appropriate contractual clauses are in place in line with the relevant Data Protection legislation.

Sharing Personal Data – Third Party Commissioners

Where Barnardo's are commissioned to deliver services on behalf of a local authority/health authority/government agency they may be identified as a controller of the data (ie they determine the scope and nature of processing) or a joint data controller, (where both parties are processing the data for the same purpose), a controller to controller agreement should be set up to establish what data is being shared, the lawful basis for sharing and how this information will be transferred

Sharing Personal Data – Third Party Providers.

Where Barnardo's commission services (e.g., Occupational Health), it is likely both parties will be controllers in their own right. For example, Barnardo's will control staff data up to the point that a staff member engages with an independent occupational health provider. Any data created as part of that service will be controlled by the provider. In these instances, a controller to controller agreement should be set up to establish what data is being shared, the lawful basis for sharing and how this information will be transferred.

Third party suppliers who process data on behalf of Barnardo's will be expected to complete a Vendor Risk Assessment and this should be completed before any contractual agreement has been signed and ratified.

Sharing Personal Data on social media

Personal data should not be shared on social media platforms without the explicit consent of the data subject or their guardian.

Contractual Agreements

Each agreement should clearly state who is responsible for managing and owning personal data and what legal obligations apply to the Data Controller under this agreement. These agreements need to be signed and ratified before any data can be shared.

Transparency

Barnardo's will ensure Privacy Notices, the Service User "Your Data, Your Rights" leaflet and the staff handbook are kept updated to date so that data subjects understand how their personal data is shared and for what purpose. Where data sharing is not covered by contract/agreement or this policy, the view of the Data Protection Officer and, where appropriate, the Caldicott Guardian, should be obtained as appropriate.

Securely Transferring Data

All data that is shared with individuals, government agencies or third parties should be transferred via secure transfer methods. The transfer method to be used should be agreed and documented in the contract or data sharing agreement. Where this arrangement is not formerly set out, you should share data through Barnardo's agreed data sharing tool or via encrypted email or failing that, to a confirmed address of the requestor, using signed for post. If it is not possible to transfer data by these means, then information should be transferred in person.

Barnardo's expects the same high standards of data management as its commissioners and will only share or receive data if they use software that adequately stores and transfers data securely.

Safeguarding (Vital Interest)

The GDPR (article 6.1.d) permits the sharing of personal data without the consent of the data subject to safeguard the data subject or others from harm or where it is in their vital interest. Safeguarding concerns must always be shared with the local authority and may be shared with the police if this is necessary to protect the data subject or others. The data subject, or their guardian, should be informed that the data has been shared unless this would place the individuals concerned at further risk.

Sharing Information as Daily Practice

Some personal data may need to be shared with third parties to allow services supporting vulnerable children to run effectively, this is justified in line with GDPR 6.1(e-f). When data is shared for the purpose of performing a public task or as part of legitimate interest, data subjects are informed and data is anonymised, if appropriate. The nature of data being shared should be set out in the data sharing agreement/contract.

If sharing information is not for the purposes of carrying out a public task or in the legitimate interest of service-users, personal data should only be shared with the explicit consent of the data subject, or their guardian. For individuals making a Subject Access Request refer to the Data Protection Policy.

Sharing Outside of Contractual Agreement

There are cases where third parties request personal information outside of an agreement. Barnardo's insists these requests are made in writing outlining an explicit legal basis for the request. This helps Barnardo's to identify whether the request is voluntary or mandatory.

In the case of mandatory requests, Barnardo's will verify that there is a corresponding statute or Court Order that requires Barnardo's compliance, before responding in accordance with any specified timeframes mentioned in the request. Where there are concerns that sharing the data is not in the subject's best interests, consideration must be given to engaging legal counsel to make representation to the Court.

If a request is not mandatory, Barnardo's will still accept some requests to share data, if they agree with the relevant grounds for sharing data outlined in Schedule 2 of the Data Protection Act 2018, namely:

- the Prevention or Detection of Crime (Before disclosing personal data, Barnardo's verifies whether refusing to disclose would materially harm the resolution of the investigation).
- for the purposes of legal proceedings (establishing, exercising, and defending legal rights); or
- the assessment or collection of tax or duty.

Data subjects are informed that their data is going to be shared, for both mandatory and voluntary requests, where appropriate. Each request or obligation to share data is responded to promptly, in line with any specific contractual obligations that may apply. Each of these requests is stored for auditing purposes, and for the benefit of the data stakeholders.

Sharing data outside of a contractual agreement should always be discussed with the relevant Data Protection Manager.

6. Associated Legislation, Guidance, References and Documents

Data Protection Legislation sets out essential principles for information sharing, which are the foundation of our practice.

The **UK General Data Protection Regulation** (**UK GDPR**)
The UK GDPR sets out the key principles, rights and obligations for most processing of personal data in the UK, except for law enforcement and intelligence agencies.
The UK law that aligns with EU GDPR 2018 replacing the General Data Protection Regulation (GDPR).

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'. The must ensure the data is processed; fairly, lawfully and transparently.

From January 2021, DPA 2018 became supplementary to **UK GDPR**

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.

Barnardo's Caldicott Guardian is the Corporate Director of Development and Innovation.

7. Risk Assessment

The Policy Owner, with assistance from relevant individuals, will maintain a detailed risk assessment of information and data sharing risks facing Barnardo's, using this 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	Senior Information Risk Officer, 28/03/19	Corporate Policy replacing Directorate Policy Updated formatting
6	May 2021	DPO	Reviewed		Updated to reflect UK GDPR and includes statutory and regulatory requirements
7	August 2023	DPO	Review	Senior Information Risk Owner	Updated to include links to contractual agreements and procedures and a glossary of terms And further explanation of UK GDPR