Data Protection

The Guide

Believe in children

Barnardo's

Background

This leaflet explains laws which protect personal data. It tells you why they are important to you as an employee of, or a volunteer for, Barnardo's and what you need to pay attention to in your work.

The two laws are called the UK General Data Protection Regulation (UK-GDPR) and the 2018 Data Protection Act.

These laws matter to Barnardo's, and most other businesses, because we process hundreds of thousands of personal data records on behalf of our service users, customers and supporters, as well as our own personal data, for example about recruitment, employment, and volunteering. All this personal information must be kept safe, secure and private (protected) so we need to take extra care to make sure we understand and apply the laws which guide us to do that. Through this document, and regular training, we hope to provide you with the right data protection knowledge to help you do your job and make sure Barnardo's can comply with the laws. If we fail to protect personal data the consequences are potentially very serious. Every member of staff and volunteer can help us to stay within the law. That's why it's important that you read and understand this booklet.

If you have any questions or concerns now, or any time in the future, please ask your line manager or email our team at dpo@barnardos.org.uk

What does the law say?

The UK-GDPR is underpinned by six principles. Personal data must be:

- **Processed fairly, lawfully and in a transparent manner**, which means we must have a legal reason to record, store or share someone's data and we must tell them that we are doing this.
- **Collected for specified, explicit and legitimate purposes**, which means that we can only collect and record personal data if we have a reason to do it and we have explained this reason to the data subject.
- **Adequate, relevant and not excessive**, which means we should only record the information we need to support a young person, claim Gift Aid, recruit a volunteer, or enable a supporter to donate to Barnardo's.
- **Accurate and kept up to date**, which means that we must be sure that what we record is correct, and update it as soon as we know that a change is necessary.
- **Held for no longer than necessary**, which means that we need to decide up-front how long we should keep personal data, and then we should archive or delete it.
- **With appropriate security,** which means we must keep documents containing personal data locked away when not being used, mobile phones and laptops should be encrypted and password protected and personal IT equipment used for business purposes must have Barnardo's mobile device management installed.

It is your responsibility to help Barnardo's uphold these principles.

This booklet gives you the information you need on three key areas:

- **Key definitions**
- **What to do if you discover a data breach**
- **How to keep yourself and data safe**

Data Protection and Security training is undertaken on an annual basis in Barnardo's and your manager or supervisor will give you regular updates in meetings.

Please read this document carefully, keep it for reference, and complete the acknowledgement slip at the back and return to your line manager/supervisor.

We really appreciate your help, focus and commitment towards protecting personal data and helping Barnardo's maintain the security of digital and paper records.

Key definitions

Data

Data is just another way of saying **"information"**.

Information is vital to the way any organisation is run and Barnardo's is no exception – it's one of our biggest assets. Without information we cannot function so we need to protect and safeguard it, particularly if it's confidential and/or sensitive.

The information that really matters in the law is called Personal Data

What is personal data?

Personal data is anything that identifies a living person. No personal data should be collected without demonstratinga purpose for processing it and this includes names, addresses and images like photographs and videos. For example, if someone took part in the Big Toddle and you have a photograph of them wearing a school badge or logo, then you could look the school up online and find out where it is. You could begin to collect quite a bit of information about the child. It's important that we only collect the information we really need.

Here are some examples to help you understand what personal data is:

Example	Personal Data?	Justification
Barnardo's Annual Report	No ✗	The information in this report is in the public domain and therefore is not considered personal
Name and address	Yes ✓	An individual can be identified at a particular location. An address on its own is not considered personal data as it could relate to several people at that location
Your anonymous response to a survey question	No ✗	As the information is captured anonymously, there is no way for anyone to identify who the responder is
Work email address	Yes ✓	As a work email address generally contains an individual's first and last name, and usually identifies their place of work, it is personal data
Work ID badge	Yes ✓	If it displays a name and a picture, this is sufficient personal data to identify an individual

Special Category Data

Some personal data is particularly sensitive. This is called Special Category Data.

Importantly for Barnardo's, children are seen as a special group so their data is given stronger protection. **Other examples of special category data are:**

- Racial or ethnic origin
- Political opinions
- Religious or philosophical beliefs
- Trade union membership
- Genetic or biometric data (like fingerprints or blood group)
- Health status
- Individual's sex life or sexual orientation

Everyone has the right to receive a copy of the data that Barnardo's holds about them. This is called a **Subject Access Request**. This means that, as a member of staff or volunteer, you may request, the data that Barnardo's holds about you, or you may receive a request from a member of the public. If you do, please let your supervisor or line manager know immediately because we only have one calendar month to respond to requests.

Information Security

All personal data must be kept secure. Especially special category data. This is what Information Security means. Whatever type of information you create or handle, you are entrusted to look after it. Information is your responsibility which means that you may face consequences if you don't look after it properly – that could mean disciplinary action if you are an employee or we may ask you to stop volunteering for us.

Why this matters

If information is compromised, deliberately or accidentally, it could mean serious consequences for our future – these may be permanent or at least long-term. The loss or theft of information could destroy our financial position and damage our reputation. Our service users, customers and supporters may no longer trust us.

We could be fined a large sum of money. The fines and penalties for data breaches are much heavier under the UK-GDPR – up to **£17.5 million** or **4% of annual worldwide turnover** for a breach, and up to **£8.7 million** or **2% of annual worldwide turnover** for not being prepared. The person (or officer) who has the powers to enforce the Data Protection Act or UK-GDPR is called the Information Commissioner.

Data Subject	is a living individual that the personal data relates to.
Data Controller	is an organisation that gathers and controls the use of the data captured.
Data Processor	is an organisation that processes personal data gathered, on behalf of the Data Controller. In the event of a breach, liability is now jointly held by the data controller and the data processor – which means both parties could be fined.
Third Parties (Authorised)	are separate entities with whom the gathered personal data may be shared such as an organisation that processes payments for us.

What to do if you discover a data breach

A data breach means that personal information has not been protected properly and has been compromised either by accident or deliberately. This could mean it has been destroyed, lost, changed, or revealed to someone else without permission.

Here are some examples of breaches:

- Email sent to the wrong recipient with an attachment that contains personally identifiable information
- Case notes or letters that contain personal information left on a photocopier, in a meeting room, or placed in a waste paper bin
- Our systems compromised by a hack
- Disclosure of confidential information on social media websites
- Sending personal data in a letter to an incorrect recipient
- Computing devices containing personal data being lost or stolen
- Alteration of personal data without permission

A breach could have disastrous consequences, from the loss of access to vital systems to the leaking of sensitive service user data. Sixty-nine per cent of data breaches are caused by authorised users.

If you discover a data breach get as much information as possible:

- How did you find out about the breach?
- What data is affected, is any of it “personal”?
- How did we get the data in the first place?
- Is it something we did or has been done to us?
- Tell your line manager or Data Protection Manager. They will ask for your help to fill in a Breach Report using the information above. In some cases, it might be necessary to co-ordinate and launch a full investigation.

Case study 1

Sarah is a volunteer supporting Gemma, a young person with learning disabilities in the community. Sarah has a copy of a medical consent form at home, containing details of Gemma’s medical conditions, which she needs in case Gemma is taken ill when they are out. Sarah records the support she provides on a secure system called Huddle, using her own computer.

One day Sarah is recording the last outing when the doorbell rings, she leaves the computer and the medical form unattended. Her son and his friends come into the room and see the information; they know Gemma because she used to go their school and one of them lives next door to her. The boy who lives next door to Gemma tells his mother what he has read and she makes a comment to Gemma’s mother. Gemma’s mother is very upset about the breach of her daughter’s data and removes Gemma from the service. She also complains to the local authority that commissions Barnardo’s to provide the service.

Consequences:

Gemma's personal data was accessed by people who had no right to see it. Always keep personal data locked away where no-one else can access it when not in use and don't leave a computer unattended if personal data is visible. As a result of this breach Gemma lost her service.

- The trust between Gemma and her family and Barnardo's was lost and Barnardo's reputation with the local authority was damaged.
- Gemma's mother could make a complaint to the Information Commissioner about what has happened, which could result in a fine for Barnardo's. This is especially serious because it is information about a child and included sensitive medical data.

It is important that personal data is always kept secure; if you use your own computer to record information about people you support as a Barnardo's volunteer you must always use Huddle or another secure system approved by your supervisor. Another charity was fined £40,000 because volunteers recorded information about people they were supporting on their own computers without the authority or the appropriate due diligence undertaken.

Case study 2

A new customer, Mr Brookes, comes into a Barnardo's shop to donate some clothes and says he's happy for Barnardo's to claim Gift Aid on his donation. Mike, a volunteer, hasn't yet been trained on using the till point to capture the customer's details, so instead he writes Mr Brookes' name and address on a piece of paper so that he can do it later (he doesn't want Barnardo's to lose out on the extra money). Mike is then interrupted by another customer and leaves the paper on the desk where it is picked up by another customer who knows Mr Brookes. He gives it to the store manager, who has no idea what it is and puts it in the bin.

Consequences

- This is a data breach as Mr Brookes' data has been read by someone else and then subsequently lost.
- Barnardo's has lost out on the gift aid associated with Mr Brookes' gift.
- Mr Brookes' friend could tell him that he'd found his name and address lying about in the shop, which could make him think twice about donating to a Barnardo's shop again.
- He may choose to make a complaint to the DPO at Barnardo's.

If you sign-up a gift aid donor, you should ask the donor for their personal details at the till point and enter them immediately, so no paper trail is kept. The till produces a receipt for the donor to sign and this should be filed, with the daily paperwork in a locked cabinet.

Case study 3

Amira is very keen to volunteer for Barnardo's. She fills in her application form and hands it to a member of the sales team, Matt, because the Manager is busy with a customer. Just then a customer comes in with a huge box of books and Matt becomes distracted trying to help the customer. Matt leaves Amira's application form on the shop counter whilst he struggles with the box. The application form gets caught up with other paperwork and placed on the desk in the back office, where it remains unnoticed for some days. Another volunteer clears the back office desk and the application form gets put in the bin.

Consequences

- Nobody contacts Amira about her application, so she gets a job in the British Heart Foundation shop and she tells everyone and anyone how rude Barnardo's have been to ignore her.
- Confidential data was left out on the store counter and then on the desk in the back office. This is a breach.
- Her data has been lost, so this is a data breach. The form should have been shredded or put in confidential waste, now it's in the general waste where it can be stolen.

If someone comes in and hands in a Volunteer Application form the manager, sales associate or key holder must ensure that it is stored in a locked filing cabinet to ensure that the prospective volunteer's personal details are kept confidential at all times. Each volunteer has a personal folder, containing all their information, which should be stored in a locked filing cabinet.

Case Study 4

Gloria is a member of a local Barnardo's Helper Group and is helping at a fundraising event organised by the group. She is approached by Susan, who wants to make a donation of £100.

Gloria accepts the cheque and asks Susan to write down her name, address, telephone number and email address so that she can arrange for a formal thank you to be sent to her.

Susan writes down these details which she gives to Gloria. Gloria puts the £100 cheque in the cash tin but does not attach Susan's details to the cheque.

After Susan leaves, Gloria goes home, completely forgetting that she has put Susan's details in her coat pocket.

Consequences

- We are unable to send a formal letter of thanks and Susan is very annoyed that she has not received any contact from Barnardo's and tells several of her friends so our reputation is damaged
- The donation cannot be processed with gift aid or set up as a record on Salesforce
- Susan's data is in Gloria's coat pocket where it could get misused or sit undiscovered for a long time. The loss or misuse of this data constitutes a breach.
- If someone makes a donation their personal contact details should be kept secure (e.g. in a locked cash tin) until the donation and enquiry can be processed. All personal data should then be shredded or destroyed.

How to keep yourself and data safe

Risks: Workplace

The workplace contains many information risks. **You can avoid making mistakes by:**

- Avoiding putting passwords on post-it notes on your desk
- Not sharing passwords
- Not letting someone into the offices without a pass
- Not having a messy desk: if your desk is a mess you could accidentally leave sensitive information on display and then not notice if it went missing.
- Not leaving sensitive information lying around. When you are finished with whiteboards, flipcharts and meeting rooms you should make sure that all the information is removed.
- Locking your computer. This protects the information and safeguards you from blame if the computer is misused while you are away.
- Protecting and disposing of information correctly.

If in doubt, speak to your supervisor or line manager.

Risks: On the move

Technology means you can now keep in touch with your colleagues and supporters more easily when you are away from the office.

However, before you take information out of the shop or office, ask yourself:

- What information am I taking?
- Am I allowed to take it?
- Do I know what Barnardo's guidance is on carrying information?
- Is the information stored securely?

When working outside traditional office space, for instance in a shop, café or on the train home, information immediately becomes more vulnerable. So, take extra care to avoid unnecessary risks.

- Check before you leave: have you left anything behind? In particular documents, flash drives or your laptop?
- Work tidily and with care. Ensure no information is on display.
- Make sure your laptop screen is not visible to others. The same applies to your mobile phone/smartphone or other mobile devices.
- Avoid discussing anything sensitive where people might overhear. Pay attention to who is around you.
- Make sure you remove your pass when you leave work.

Always report lost or missing information immediately to your line manager. The consequences of trying to hide a loss can be far worse.

Risks: Home

You might feel that your own home is the most secure environment of all. **However, you still need to consider the risks:**

- **Document disposal**: Don't throw sensitive or confidential documents into the bin. Dispose of paper documents just as securely as you would in the office, i.e. shred them or take them to an appropriate office hub and put them in confidential waste.
- **Documents lying around**: Get into the habit of keeping information discreet. Don't just leave things lying around for others to see.
- **Mobile phone**: When dealing with sensitive information over the phone, be aware of who might overhear, purposely or not.
- **Protecting information**: Sensitive business should not be conducted using personal laptops or home computers unless using some kind of mobile device management (seek advice from IT).
- **Insecure networks**: Web-based email accounts are particularly risky. Avoid using personal email addresses to send confidential company information. Connect to the business network via appropriate desktop tool within OKTA.

Social networking

Social networking is a great way to connect with people, share media and exchange information and ideas. **But be aware of the risks.**

- Your personal information may be easily available to others
- You may expose sensitive company information
- You may lose control of your photos once they are on the internet
- Sites may be used to spread malware and malicious applications

Don't discuss work issues on personal social media sites, you can never be sure who will read the information and what they will use it for.

It is fine to say on something like your LinkedIn profile that you volunteer for Barnardo's, but please check with your manager before going into more detail about what you do.

Keep your professional and personal information separate.

Don't underestimate the power of 240 characters. The speed at which information can spread virally online means you very quickly lose control over anything you post.

Case study 5

Jason is at his desk and is tweeting about his current project. Although the project is a high-profile company one, he is tweeting that: “nobody seems to know what they’re doing round here”.

One of Jason’s friends finds this tweet amusing. He re-tweets and puts it in context. He has 3,000 followers so the message spreads quickly.

Jason deletes the tweet, but the information has spread and has already been picked up by the media. This is not a data breach, however, there is reputational damage to the organisation and Jason’s position needs to be evaluated by his manager.

Risks: Taking Photos

Photographs and videos are vital elements that enhance the work of Barnardo’s, however, photographs can also be personal data, and we have to protect our service users, celebrities and employees.

Please remember:

- Don’t use your personal devices (i.e. phones and tablets) to take pictures or videos on behalf of Barnardo’s or when attending events.

If you need advice about this, email **dpo@barnardos.org.uk**

FAQs

Q Do we have a Data Protection Officer (DPO) and how can they be contacted?

A The designated DPO for Barnardo's is Martine King. She can be contacted via dpo@barnardos.org.uk

Q A breach has been brought to my attention, what shall I do immediately?

A If a breach has been identified, this should first be brought to the attention of your supervisor/ line manager, or in their absence you should make contact with the Data Protection Manager (DPM) for your team.

Q What's the difference between a data breach and a breach of confidentiality?

A A breach of confidentiality happens when you tell someone something that you shouldn't. A data breach is the physical destruction, loss, alteration or disclosure of data without permission.

Q I think that I may have found a data protection problem or vulnerability in our processes – what should I do?

A All suspected issues should be raised with your supervisor or line manager immediately so that they can be assessed and the relevant corrective action applied.

Q How quickly do we need to report a breach?

A Under the UK GDPR legislation we have 72 hours to raise the matter with the ICO, so you need to act immediately.

Q I still have a few queries around Data Protection and Information Security and our processes, who do I contact?

A Please send through any additional queries to dpo@barnardos.org.uk

Q Why do I need to complete the acknowledgement slip at the back of this guide?

A Barnardo's needs to be able to demonstrate that employees and volunteers have a certain level of understanding of data protection when audited. Signing and returning your form demonstrates that everyone has had visibility and instruction. The acknowledgement slips will allow us to achieve these objectives and will be stored by the People team for our records.

Checklist

The following are checks that we would encourage everyone to make:

✔ Make sure you are aware that personal data always needs protection

✔ Make sure you've read the Data Protection and Information Security Policies

✔ Make sure you are recording customer's data and wishes accurately

✔ Make sure you are never sending personal data through insecure methods

✔ Make sure you tell your supervisor or line manger if anyone raises any objections to data processing or requests erasure of data

✔ Be alert for anything suspicious that could highlight a data breach and report it to your supervisor or line manager or in their absence, your Data Protection Manager.

Barnardo’s Data Protection Awareness Acknowledgement

Please complete the acknowledgement below and return to your line manager, for delivery to the People team.

I can confirm that I have read the Barnardo’s Data Protection Booklet.
I commit to complying with its requirements:

Name:

Employee/Volunteer ID/Reference (if appropriate):

Department/Service/Shop:

Region/Area:

Name of Line Manager:

Signature:

Date: DD/MM/YYYY

www.barnardos.org.uk

Barnardo House,
Tanners Lane,
Barkingside,
Essex IG6 1QG

Believe in children
Barnardo's

Barnardo's Registered Charity Nos. 216250 and SC037605 23258dos22