Understanding your responsibilities for data protection

Guidance for Staff and Volunteers

February 2024

Contents

Introduction

Employees and volunteers have a shared responsibility to follow the rules of the UK GDPR, part of the Data Protection Act 2018 (the Act). This guidance will help you to comply with the requirements of the Act.

When anyone gives and trusts us with their personal information, it is our responsibility to treat this information in a way that lives up to their expectations and complies with all our legal obligations.

We must treat personal information properly. A serious breach of data protection law could result in criminal prosecution and a fine. It would also seriously damage our reputation. Individuals as well as organisations can be fined and prosecuted when they are judged to have breached the law.

Generally, a useful way of thinking about data protection is to treat people's personal information in the same way that you would expect your own information to be treated.

Data Protection Terms and Definitions

Data protection law applies to how we process people's personal information. The key terms that we need to understand are:

Controller – We are a Controller as we collect personal information and decide how will be used.

Principles – These are the rules that we must follow when processing personal information

Processing - This is what we do with personal information. It includes how we collect, record, store, share and use personal information

Personal information – This includes any information that could be used to identify a person and includes special category personal data

Personal data - This is information about people and held in computer systems, mobile devices, laptops, tablets, memory sticks, or in manual records such in paper files and note books. Types of personal data might include but is not limited to, name, address, date of birth, bank account details, interests

It also includes opinions about a person. For example, notes on how you think someone has behaved, performed or appears

Special category personal data – this is information about a person's health, religion, political opinion, trade union membership, race or ethnic origin, sexuality

A **data subject -** this is the person whose personal information is being processed. For example, a person that uses a foodbank, a donor, employee, or volunteer

A **privacy notice** – this is a short notice when we collect personal information from people to inform them how their personal information will be used.

A **privacy policy** – this is how we inform people about how their personal information will be used. Our privacy policy is provided on our website

Data processor – this is an organisation that we use to process personal information on our behalf. For example, a software provider like Microsoft or Google

Information Commissioner's Office (ICO) - this is the government body responsible for enforcing data protection law in the UK

The Data Protection Rules

Personal information must be:

	collected and processed in a fair, lawful and transparent way
	used only for the reasons it was collected
	relevant and not excessive
	kept accurate and up to date, and corrected or deleted if there are mistakes
	kept for no longer than it is needed
	kept safe to protect it from being lost, stolen or used inappropriately
	processed in accordance with people's rights

Compliance Guidance

Personal data must be processed fairly, lawfully and in a transparent manner

- ✓ Be clear and open with people about how their personal information will be used
- ✓ Include a written or verbal Privacy Notice when collecting personal information. This should describe:
    - who the controller is: For example, the food bank

- the purpose for which the personal information will be used. For example, to process a donation, to provide food
- if the personal information will be shared with any other organisations. For example, the Trussell Trust

See the separate guidance on Privacy Notices for more information about this

- ✓ Only use personal information in a way that people would reasonably expect
- ✓ Think about the impact of your processing – don't do anything that could have a negative effect on the people whose personal information you are using
- ✓ Obtain the explicit recorded consent of a person if you are collecting their sensitive (special category) personal data. For example, health or medical information
- ✓ Obtain prior recorded consent from people before publishing photographs or film footage of them (see resource 5.2.R10).

Personal information should be used only for specific and legitimate purposes

- ✓ Only use personal information for the purpose that was described in the privacy notice when collecting it. For example, if the privacy notice states that the information collected will only be used to process a donation, that is all it can be used for.

Personal information must be adequate, relevant and not excessive

- ✓ Collect just the right amount of information for the purpose required and described in the privacy notice – no more, no less
- ✓ If a person gives you more information that you need to know, for example in an email or phone conversation, only record the relevant information
- ✓ Data protection law does not allow for personal information to be kept because 'it might become useful' at some point in the future.

Personal information must be accurate and up to date, with errors corrected or deleted as soon as possible

- ✓ Regularly check that the personal information you hold in computer and paper records is accurate
- ✓ Do not use personal information if you have doubts about its accuracy
- ✓ Remind people to notify you of any changes in their personal information
- ✓ Amend relevant electronic and manual records as soon as possible if someone informs you of a change in their information

Personal information should be kept only for as long as it is needed

- ✓ We must have a valid reason for keeping personal information

- ✓ A data controller must document how long it will keep different types of records and personal information for in a Personal Data Retention Policy and Schedule
- ✓ Know where to locate the Personal Data Retention Policy and Schedule and follow it
- ✓ When personal information is no longer required it must be destroyed or disposed of securely, for example, by shredding it.
- ✓ Delete emails containing personal information once no longer needed

Personal information must be kept safely to prevent it from being lost, damaged or stolen

- ✓ Use a password to log in to your computer so that others cannot access the personal information you hold, and do not share your password with anyone
- ✓ Lock desks and cupboards used to store personal information, and keep the keys secure
- ✓ Use Royal Mail registered post to send large volumes of paper containing personal information or sensitive personal data or deliver by hand.
- ✓ If you need to send an email containing personal information, or attach a file which includes personal information to an email, password protect the email or document, and send the password in a separate email or text message
- ✓ Double check that you have attached the correct file before sending an email
- ✓ Double check that the email is addressed to the correct recipient
- ✓ Always use the bcc field (not the cc field) when sending an email to more than one person so that the recipients' email addresses are not visible to each other - unless consent to share email addresses has previously been obtained
- ✓ Delete emails containing personal information when no longer required or move to a secure folder if still required
- ✓ Take special care when travelling with computers, laptops, tablets, smart phones and paper records containing personal information
- ✓ Do not leave laptops and paper documents or files unattended and visible in your car
- ✓ Make sure papers or screens containing personal information are not visible to others in meetings, on trains, and even in your own home
- ✓ Do not download documents containing sensitive personal information to your desktop or mobile devices, such as hard disks and memory sticks

Sharing Personal Information

- ✓ You can sometimes share personal data without consent, if you have a good reason to do so. For example, someone's life is at risk.

- ✓ There are some cases where the impact on an individual might override your interests in sharing their information, in which case you might need to ask for their consent. For example, when sharing sensitive or "special category" data about a person.

- ✓ If we need to share personal information with other organisations, for example, we must include this information the privacy notice

- ✓ Where data is shared with another organisation on an ongoing or repeated basis it is good practice to have a data sharing agreement. For example, with referral agencies or the Trussell Trust

When deciding whether to share personal information you should consider the following:

1. Identify the objective that the sharing is meant to achieve
2. Consider the potential benefits and risks of sharing the information
3. Assess the likely results of not sharing the information

You should only share the specific personal data needed to achieve your objectives. For instance, you might need to share somebody's current name and address, but not other information you hold about them

Personal Data Breach – What to do

Personal data breaches occur when personal information is lost, destroyed or shared without consent, or if someone accesses the personal information or passes it on without consent. This can be deliberate or by accident. It includes sending personal information to the wrong person and electronic devices such as laptops and telephones containing personal information being lost or stolen. We must act quickly if there is an issue

- ✓ If you think there may have been a data protection breach or there has been a near miss, please let the Data Protection Lead know immediately: info@redbridgefoodbank.org / 020 8518 0056
- ✓ Data controllers must keep a record of all personal data breaches
- ✓ Serious breaches must be reported to the ICO within 72 hours of being discovered

Data Subject Rights

Data protection legislation gives rights to people. The rights that are most relevant to us are:

- **The right to be informed** – we do this by including appropriate privacy notice information when collecting personal information
- **The right of access** – if asked we must give people a copy of their personal information which we hold
- **The right to object to processing** – if someone objects to the processing of their personal information we must consider whether we can stop the processing and provide them with an explanation if not.
- **The right to not receive direct marketing -** if a person changes their mind about receiving direct marketing (which includes any newsletters) we must stop sending people direct marketing messages
- **The right to rectification** – we must correct any inaccurate or incomplete personal information when asked
- **The right to erasure** – we must delete or remove some personal information if asked

Data Subject Rights – How to respond

The right of access

A person has the right to view their personal information which hold.

- ✓ When asked we must provide this information within 30 days.
- ✓ The information provided must not include anyone else's personal information unless we have their consent.
- ✓ Assume that anything you record about a person could be seen by that person.
- ✓ Record facts and opinion that you would be able to defend if challenged
- ✓ If someone asks to see their personal information, contact the Data Protection Lead info@redbridgefoodbank.org / 020 8518 0056.

The right to object to processing

People have the right to object to us processing their personal information. If someone requests this, explain to them why we process their personal information and the consequences of not processing it. For example, we may not be able to provide a food parcel if we do not have a record of who we have given it to. If the person still objects to the processing, take a note of their contact details and pass to the Data Protection Lead info@redbridgefoodbank.org / 020 8518 0056.

The right to not receive direct marketing

People have the absolute right to prevent their personal information being processed for direct marketing purposes.

The definition of 'direct marketing' by the Information Commissioner's Office includes an organisation communicating its aims and objectives by email, e-newsletter, telephone, text message or post. This includes information about our campaigns, events and fundraising activities.

- ✓ You must only contact a person with a direct marketing message by electronic means (email, text message) if they have already opted in to receiving these communications
- ✓ Every direct marketing message you send by email and text message must include an unsubscribe function so that the recipient has a choice to opt out of further communications from the group
- ✓ A person must not be contacted again if they unsubscribe or request not to receive further direct marketing messages

- ✓ If someone contacts you to say that they no longer wish to receive direct marketing messages by post or phone call, you must remove their name from or suppress it in your group mailing list
- ✓ A person must not be contacted again if they have requested not to receive further direct marketing messages

The right to erasure

The right to erasure is also known as 'the right to be forgotten'. People have the right to request the deletion or the removal of their personal information where there is no compelling reason for its continued processing.

- ✓ If you have given a person's personal information to someone else, you must contact each recipient of that information and ask them to erase the personal data in question. For example, to delete information from the DCS you should contact Network Services at the Trussell Trust
- ✓ If it is not possible to delete someone's personal information then consider how you can restrict further processing of the data in future. For example by adding their basic details to a suppression list.
- ✓ If you receive a right to erasure request and you're unsure how to handle it, please get in touch with the Data Protection Lead info@redbridgefoodbank.org / 020 8518 0056.