

# Data protection:

## Frequently asked questions

Depending on the nature of your volunteer role with Lymphoma Action, you may have access to or come into contact with the personal data of people who attend our services and events, as well as that of other Lymphoma Action volunteers and staff. You are expected to follow the instructions and guidance shared with you in the course of your induction, training and volunteering.

We don't want you to be worried about data protection, important though it is. Please ask if you don't understand something, and let us know straightaway if something goes wrong, so we can put it right.

### Frequently asked questions

This resource is designed to supplement your volunteer induction and training, to help you understand data protection and apply the policy and processes in your volunteer role.

These FAQs are not exhaustive, so if you have questions that are not included here or you need more information, please get in touch with your volunteer manager or the Volunteering Team.

Please find quick links to our FAQs sections below, to help you find the answers you're looking for:

- [What is personal data?](#)
- [What is data protection and why does it matter?](#)
  - [Seven key principles of GDPR](#)
- [What is a data breach?](#)
  - [What should I do if I think data security has been breached?](#)
  - [What should I do to avoid a data breach?](#)
  - [How would I know that I'd been involved in a data breach?](#)
- [How do volunteers safely 'process' personal data?](#)
  - [How should I store personal data?](#)
  - [How can I use personal data?](#)
  - [When should I delete or destroy personal data?](#)
  - [How should I delete or destroy personal data?](#)

## What is personal data?

Personal data covers any information that can identify an individual and includes their name, address, email and phone numbers, date of birth and any other information that could lead to them being identified – either on its own or in combination.

Some personal data comes into a **special category** because it is very sensitive. It includes any information about physical or mental health, including whether someone is affected by lymphoma. So, the fact that someone attends a Lymphoma Action support service is special category personal data because anyone could assume something about their health status from knowing this.

Other special categories of personal data are racial or ethnic origin, sexual orientation, political opinions, religious or philosophical beliefs, trade union membership, sex life, genetic data and biometric data obtained as means of identifying someone.

## What is data protection and why does it matter?

To give greater protection to everyone's personal data, the GDPR (General Data Protection Regulation) was introduced in 2018 and is part of UK law. It gives everyone greater rights to decide who holds their personal information and how it is used.

GDPR also places greater requirements on the people and organisations that collect and use personal data - Lymphoma Action has a legal obligation and responsibility to protect the personal and sensitive information of all individuals we interact with. This duty extends to all of our volunteers.

You have probably heard news stories about personal data being misused, including by some charities. This is why GDPR matters - not only to greatly protect the personal information of others, but also to protect the reputation of Lymphoma Action and to make sure we don't incur any financial penalties as a result of any data breaches.

## Seven key principles of GDPR

The following principles share in brief terms what good data protection practice looks like and set out how personal data should be processed:

1. Lawfully, fairly and in a transparent manner.
2. Collected for specified, explicit and legitimate purposes and not used in any other way.
3. Adequate, relevant, and limited to what is necessary for the purpose it has been collected.
4. Accurate and, where necessary, kept up to date.
5. Kept for no longer than is necessary.
6. Ensure appropriate security of personal data to avoid data breaches.
7. An accountability and responsibility to demonstrate compliance.

## What is a data breach?

A data breach is when any personal data is disclosed, lost, destroyed, corrupted; a person or organisation accesses or obtains personal data, or passes it on, without authorisation. It also covers the misuse of data.

A data breach can happen in many ways, including accidentally or deliberately sending it to another person or organisation, or them deliberately obtaining the data, for example by hacking into a computer. Breaches from misuse are often using data in ways the person whose data it is, has not been told about beforehand, or that they haven't agreed to. For example, sending them information about something they didn't consent to, or wish to receive.

## How would I know that I'd been involved in a data breach?

You might not know immediately, for example, if your computer or phone has been hacked or the system you are using is breached.

If you've forgotten to 'Bcc' attendees to emails, you might not realise until later or an individual contacts you, or Lymphoma Action contacts you about a breach we've been told about.

If you aren't sure but only suspect there may have been a breach, always report it.

## What should I do if I think data security has been breached?

You **must** notify your volunteer manager, or the Volunteering Development Manager in their absence, immediately by sending an email or leaving a phone message for them to pick up as soon as they are available, making sure you include all the details you have about the breach.

The charity needs to follow the GDPR legal processes. This includes **not** contacting the person/people whose data has been breached or the person/people or organisation to which the data has been sent.

If you think that the breach is a result of your computer or phone having been hacked, use a different device to contact Lymphoma Action. Once you have done this, please do not do anything else until your volunteer manager or another member of Lymphoma Action staff discusses any additional action that needs to be taken.

You may feel anxious about what has happened – **please try not to worry**. As a volunteer you are an authorised person of Lymphoma Action, which means you are not personally liable if you have followed our policy and processes. The focus is on finding out what went wrong and putting it right.

## What should I do to avoid a data breach?

As a general guide, take the following precautions, depending on how you store and use the personal data for your volunteer role. In all cases, you must delete all personal data you have access to, whether on an electronic device or paper, when asked to do this by Lymphoma Action. (See [‘how do volunteers safely ‘process’ personal data?’](#)).

### For electronic devices

- Password protect your devices
- Have adequate security programmes installed and keep these updated
- Don’t share devices with others and/or keep personal data for Lymphoma Action in password protected accounts that sharers don’t have access to.
- Do not copy or back up personal data to external sources. If you accidentally delete someone’s details, you can obtain them again by contacting your volunteer manager.
- If you need advice about any of this, do ask your volunteer manager, as the charity’s digital team might be able to answer your question or explain what is required.

### For paper copies

Some volunteer roles may need to store some personal data on paper, for example, a list of registered workshop attendees.

- Keep all paper copies in a locked file or drawer at home before and after the event.
- Speak with your volunteer manager if you need a lockable file.
- Do not leave registers or information out for others to see or take during the event – securely store this away once you have finished using it.

## How do volunteers safely ‘process’ personal data?

### How should I store personal data?

You can store personal data digitally or on paper, or both, as required for your volunteer role. If data has been sent to you digitally, try to avoid printing this out unless absolutely necessary to keep the number of records of personal data to a minimum. For example, only store data on one computer or phone and only in one place on each.

Please also refer to [‘what should I do to avoid a data breach?’](#)

### How can I use personal data?

You must **only** use the personal data you have access to as required for your volunteer role, which will be covered during your induction, training and ongoing support.

**Never** use personal data for any other reason without specific permission from your volunteer manager or other member of Lymphoma Action staff.

## When should I delete or destroy personal data?

You should only delete or destroy personal data when told to do so by your volunteer manager or another member of Lymphoma Action staff. You must securely delete or destroy the information as soon as possible (see [‘how should I delete or destroy personal data?’](#)).

In most cases, this will be as soon as you have finished using the data for the purpose of your volunteer role and activity.

## How should I delete or destroy personal data?

This depends on how the data has been stored and used, whether digitally or on paper.

### Digital

All the relevant personal data must be deleted from digital devices and systems. They must also be deleted from your ‘recycle bin’ or ‘deleted items’.

### Paper

You will need to destroy all paper records that include the individual’s name or contact details. Paper records must be destroyed by shredder or by cutting up into small pieces.

If you don’t have the means to do this, please speak to your volunteer manager.



**volunteering@lymphoma-action.org.uk**



**01296 619415**