Contents

[Guide Dogs Data Protection and Information Security Training for volunteers 2](#_Toc151650756)

[About this training 2](#_Toc151650757)

[Section 1 – Information Security 2](#_Toc151650758)

[What is information security? 2](#_Toc151650759)

[Everyone is responsible for protecting personal information 3](#_Toc151650760)

[Reporting an incident 3](#_Toc151650761)

[Data breaches – situations to watch out for 4](#_Toc151650762)

[Good practice guidance 5](#_Toc151650763)

[Use unique, strong passwords 6](#_Toc151650764)

[Viruses and malware 6](#_Toc151650765)

[Social networks 7](#_Toc151650766)

[What to do if you have been hacked 8](#_Toc151650767)

[Section 2 – Data and the Law 9](#_Toc151650768)

[What is personal data? 9](#_Toc151650769)

[What is sensitive or ‘special category data’? 9](#_Toc151650770)

[Some terminology for the handling of data 9](#_Toc151650771)

[Data protection laws setting best practice 10](#_Toc151650772)

[Data Protection Principles 10](#_Toc151650773)

[Breach notifications 12](#_Toc151650774)

[Data Protection Impact Assessments (DPIAs) 12](#_Toc151650775)

[Having a data protection culture 13](#_Toc151650776)

[Section 3 - Data Breaches 14](#_Toc151650777)

[Potential impact 14](#_Toc151650778)

[Data security – top tips 14](#_Toc151650779)

[Subject access requests (SARs) 15](#_Toc151650780)

[Further information and questions 15](#_Toc151650781)

[Assessment questions 16](#_Toc151650782)

[End of document 16](#_Toc151650783)

# Guide Dogs Data Protection and Information Security Training for volunteers

This document is the alternative format of the ‘Data Protection and Information Security’ training for volunteers. It is also available as eLearning and a prerecorded webinar – please visit the [‘Data protection training’ section](https://www.guidedogs.org.uk/vip/resources/data-protection-training/) on the Volunteer Information Point (VIP) for details.

## About this training

Keeping the information and data of our supporters, service users and volunteers safe is a high priority for everyone at Guide Dogs.

This training is designed to support volunteers whose role involves handling data regularly to understand the essentials, feel confident about the dos and don’ts and know what to do if something goes wrong. By completing this training, you will also be helping Guide Dogs meet its legal obligations around data protection.

This document should take around 20 minutes to read through, and there will be a short assessment at the end to complete to confirm your comprehension.

This course is divided into three sections:

1. Information Security
2. Data and the Law
3. Data breaches

## Section 1 – Information Security

### What is information security?

Information security for us, means keeping all information we hold at Guide Dogs, secure and ensure it is being used in the correct way, and against criminal activity such as theft. It applies to all data held either electronically (on databases, computers or on mobile devices) and also on paper, such as a service user’s address you have written down for collecting their guide dog.

### Everyone is responsible for protecting personal information

All staff and volunteers have a responsibility to look after personal information at Guide Dogs. Sometimes it can be very sensitive and private information that we need to take extra care with, or to ensure that it is kept confidential.

For example: a service user’s health details or simply a mobile telephone number or email address.

We process information on our service users, supporters, staff, and volunteers, and that includes your personal information too.

### Reporting an incident

If you are ever concerned data is not being handled correctly, or if there is an actual incident then please report it immediately to your volunteer manager or any other member of staff you work with. You can also contact our Data Protection Team directly DataProtectionOfficer@guidedogs.org.uk

The sooner we know about it, the sooner we can support you and take action. Even if you are not completely sure it is a breach, it is always better to let us know.

There are many situations when a data breach might happen, and we will go through some examples that might be related to your volunteering role but can also be helpful in your personal life too*.*

### Data breaches – situations to watch out for

#### Using mobile devices in a public space

Be careful when speaking on your phone in a public space in case personal/confidential information can be overheard. This can also apply to being inside, around other people, or perhaps on your own but near an open window with passers-by.

#### Protecting your mobile device

Protecting your device is really important, and you can do this by:

* Using secure passwords and carrying out regular back-ups.
* Storing your mobile device in a safe place, do not leave on a table or in plain sight, left open and unlocked. Be careful no-one can look over your shoulder to view it.
* Do not have your device set to automatically connect to public Wi-Fi networks because these are not secure, and don’t leave Bluetooth auto-discovery on.
* Only download apps from official sources.

#### Sending emails

Data incidents involving the sending of emails are one of the most common causes of data incidents. Sending an email to the wrong person is an easy mistake to make and sharing the wrong information with the wrong person can lead to embarrassing or even very serious results.

Take extra care when sending emails. Before pressing ‘send’, take time to pause, check the recipients are correct and double check the content of the email and attachments.

#### Auto complete slip ups

Some email software has a helpful ‘auto complete’ function in the To: box that fills in the rest of an email addresses you have used recently once you start typing. A great feature, but it can sometimes inadvertently auto complete the address of someone you didn’t intend to send the email to.

For example, you want to send an email to Linda Jackson, but as you start typing Linda it auto completes the address of Linda Smith who you sent an email to earlier.

Make sure you check that you have the right person in the To: box before you press send.

#### Replying-to-all by accident

Email software often has both a ‘Reply’ and a ‘Reply to all’ button which are easy to mix up. ‘Reply’ will go to the person who authored the email, but ‘Reply to all’ will go to all of the people who were copied into the email.

Be careful which one you choose when writing replies, and always double check the recipient list and remove names where necessary before sending.

#### Forwarding long email chains

When forwarding emails, check the content of the earlier emails included in the thread. Make sure the previous chain of emails are appropriate for the recipient to see. Remove or delete emails and/or content that is not appropriate to pass on or start a new email.

#### Forgetting to use BCC:

This is one of the most common mistakes made at Guide Dogs as well as other organisations who report data breaches to the Information Commissioner’s Office.

When you send an email to a group of people using their personal email addresses, the recipients may not be happy for their contact details to be shared with the other recipients, especially if they are not known to them.

In these cases, you must use the BCC: (blind carbon copy) box and not the To: or the CC: (carbon copy) boxes. This will ensure the recipients in the BCC: box will get your email but won’t be able to see the email addresses of the other recipients.

Always take some extra time to double check all the above before hitting the send button.

### Good practice guidance

If you handle data in paper copy – then just remember, do not leave pieces of paper, post-it notes, open calendars or notebooks lying around where other people can see them. Make sure everything is securely stored at the end of each day or if you are stepping away from your workspace.

We discourage the use of memory ‘USB’ sticks at Guide Dogs, but if you are authorised to use one then make sure it has a password to open it, and do not leave it plugged into your device when you’re not around.

When you have finished for the day, close down the applications you were working in, and shut down your computer. Don’t forget to lock it too, if you leave it unattended however briefly, if other people are about and they could view it.

### Use unique, strong passwords

Creating strong passwords is extremely important when it comes to information security. A compromised password can result in theft of personal information or even your own identity. So, keep the following tips in mind:

* Use different passwords for your different accounts.
* Don’t use passwords that are simple or easy to work out e.g., pet names.
* One way to create passwords is to abbreviate a phrase that might not make sense to someone else. Take the first letter of each word. Mix in some symbols, such as ampersand ‘&’.
* Protect your passwords, do not share or write them down.
* Be cautious entering passwords using another person’s device.
* Only use machines you trust.

### Viruses and malware

A virus is a malicious piece of computer code that can infect your computer or devices and corrupt or destroy information on it. Malware is software designed to disrupt, damage, or gain unauthorised access to a computer system e.g., trojans.

The most common source of infection by viruses and malware is through email. Here’s some tips on spotting suspicious emails that may potentially contain viruses or malware.

#### Spoofed or forged email headers

Spoofing or forging email headers is where cyber criminals try to make it look like the email has come from a trusted source, so that the person thinks they are legitimate in their request.

For example, the criminal may know you normally communicate with “John Doe” and spoof their name to trick you into think their email is legitimate.

Real email = "John Doe" <jd23950@gmail.com>

Spoofed email = "John Doe" <johndoe.cmu.edu@scammersite.net>

Double check that both the sender’s displayed name and the email address match what you would expect.

#### Check email contents before opening attachments

Another way to check if the email is genuine is to look out for spelling or grammar mistakes in the contents, as this might be a sign that it is not genuine.

Do make sure you are happy the sender is genuine, and that you trust them before opening any attachments, especially zip files, as these could release a virus, trojans or other malware.

If you have any concerns at all, do not open it.

### Social networks

Another area we need to be careful with is social networking sites, such as Facebook (Meta), Twitter (now called X), and Instagram. They are great for communicating and staying connected; however, we must be very careful not to post personal or confidential information on them.

**WhatsApp** – although encrypted, the issue is that the data can sit with the telephone number as well as on the device (even if the sim card is taken out but the details have been saved to the device). If the phone is passed on to another person, they too have access to the WhatsApp group, and all their phone numbers – so it is good to remind people of the coffee and catch-up event, but do not use it to share personal information.

Social engineeringis where you are deceived or manipulated into doing something, or providing information so criminals can gain access to your computer. This could be by phone, email, or mail.

Phishing is an example of this, where the person is tricked into giving information such as bank details.

The criminal could even take over an organisation’s account. You might think it is from a Guide Dogs employee, so you think it is ok to share sensitive information.

### What to do if you have been hacked

If you think your device may have been infected with a virus or malware, or you think you may have been hacked, even if you’re not completely sure, change your password immediately, and report it to your volunteer manager or other staff member, or the Data Protection Team by emailing DataProtectionOfficer@guidedogs.org.uk

The sooner we know, the sooner we can take steps to stop any further harm from happening.

## Section 2 – Data and the Law

Understanding some aspects of the law around data protection will help you know how to look after personal information properly, and make sure it is protected.

The legislation is there to make sure organisations behave responsibly.

Unprotected data could lead to a serious breach of a person’s rights, causing them physical, emotional, or financial harm. It can also lead to risks of a penalty from the regulatory body (the Information Commissioner’s Office) and reputational damage to Guide Dogs.

### What is personal data?

Personal data is any piece of information that can identify or give information about an individual, such as name, address, age, phone number.

Personal data is separated into two categories: personal data and sensitive personal data.

### What is sensitive or ‘special category data’?

Sensitive personal data, also known as ‘special category data’, requires extra privacy and protection safeguards. Sensitive personal data could include information about a person’s racial or ethnic origin, political opinions, religious beliefs, health (physical and mental), sex life, sexual orientation, trade union membership, and genetic / biometric data such as fingerprints. We only collect this type of data when absolutely necessary.

### Some terminology for the handling of data

Here is some terminology you might come across in relation to data protection:

1. **The Data Controller** is the organisation that controls the data and decides what will happen with it. (e.g. Guide Dogs is the data controller for its employees’ data)
2. **The Data Processor** is a third party who processes data on the Controller’s behalf (e.g. outsourcing payroll to another company. A data controller can also be a data processor)
3. **The Data Subject** – is the living individual to whom the personal data belongs, such as yourself as a Guide Dogs volunteer, or any other person Guide Dogs holds data about.

### Data protection laws setting best practice

The EU’s General Data Protection Regulation (GDPR) sets the standard for data protection laws across the world. It was incorporated into our national law with the Data Protection Act 2018 and has been retained in UK law as the ‘UK GDPR’, since the UK is no longer a member of the EU.

These laws cover personal data processed either electronically, including in the Cloud and also any paper-based information that is stored in an organised manner.

Data protection laws can be rather complex, but the good news is that the Data Protection Team is here to support you with any questions you might have.

### Data Protection Principles

The UK GDPR’s seven data protection principles lay the foundation for how we must look after personal information. They are...

#### Principle 1) Lawfulness, Fairness and Transparency

**Lawful** - means we collect and use information in a lawful way (for example a person has given their consent for their photo to be taken at a fundraising event, or if an individual attending a community Fundraising event has requested to be contacted or sent information about volunteering.)

**Fairness** - it is fair to individuals (the Data Subjects), and it does not cause them any detriment.

**Transparency** – we let people know what is happening to their data, and it is a reasonable expectation. (Providing notices at point ofcollection e.g. collecting name and vehicle registration to enable free parking at ‘picnic in the park’ and tell people that details will be destroyed after the event).

#### Principle 2) Purpose Limitation

This means we only use it for the reason we collected it. We cannot then use it for something else.

For example: If you collect email addresses to confirm and send out details of an event to the attendees, you cannot then use the email addresses to send them information about other events.

#### Principle 3) Data Minimisation

This means we only collect the information we need and nothing more.

For example: If you invite people to leave their contact details to receive information about volunteering with Guide Dogs, you should only collect their email / telephone number. It would not be appropriate to ask for people’s gender, or date of birth for this purpose.

#### Principle 4) Accuracy

We keep the information we hold accurate and up to date.

For example: Guide Dogs needs to keepvolunteers’ contact details up to datein order to keep in contactwith them about their role.

#### Principle 5) Storage Limitation

We only keep the information for as long as we need it. We cannot keep it ‘just in case’.

For example: When a volunteer leaves Guide Dogs we keep some of their personal details on file for a defined period but then anonymise it, as after a certain point we no longer have a need to retain it.

#### Principle 6) Integrity and Confidentiality

This means we keep the information secure and would not share it with others when we are not meant to share it.

For example: When Puppy Raiser volunteer Sam tells her volunteer manager that she has to go into hospital for a hip replacement, her volunteer manager does not then tell all the other local volunteers, despite knowing that they would like to wish Sam well. (Sam may not want others to know about the operation).

Similarly, if the other volunteers did find out about the operation and wanted to send Sam some flowers, her volunteer manager cannot give them her home address unless Sam consents to this.

At Guide Dogs we do not sell data to third parties.

#### Principle 7) Accountability

Being accountable means that we take responsibility for what we do with personal information, and how we comply with all the data protection principles. We need to be able to demonstrate this compliance such as having a Data Protection Officer, having the Data Protection Team to support everyone at Guide Dogs including volunteers, as well as implementing policies and procedures.

Keeping a record that you have completed this data protection training also helps demonstrate our compliance, because everyone at Guide Dogs has a responsibility to protect information.

### Breach notifications

We have already looked at some examples of when breaches might occur.

For more serious incidents we may need to report to The Information Commissioner’s office, but we only have 72 hours from the moment the incident was first identified to Guide Dogs.

It is for this reason we say the Data Protection Team must be notified of any incidents without delay (so if you come across anything, please tell a member of staff or Data Protection Team as soon as possible).

### Data Protection Impact Assessments (DPIAs)

These are assessments Guide Dogs carries out to help us identify any risks to personal information when using a new or changing an existing system or process. It’s unlikely you will be involved in DPIAs, but it is helpful to be familiar with the term in case you come across it.

## Having a data protection culture

Having a culture where thinking about using personal data I forms part of what we do and how we develop processes this, enables us to protect people’s information. If we think about it when we first plan a new project, or when planning a fundraising event, or when sharing contact details with fellow volunteers it Ensures that data protection forms the foundation of all our processes.

We should always be thinking ‘how am I going to do this and make sure I look after the information.’ The more we consider what we do with personal information, the more likely we will remain compliant.

It is helpful to think about any personal data as if it is your own. Would you expect Guide Dogs to process your data in this way and if you feel uncomfortable or unsure at all – then please raise your concerns with your Volunteer Manager or the Data Protection Team.

## Section 3 - Data Breaches

We need to comply with these seven data protection principles to help avoid a data breach.

### Potential impact

Whenever any of us collect and use people’s personal information, such as sending an email to a group of supporters or writing down a service user’s address so that we can collect their dog, there is a risk that something can go wrong and we should consider the potential impacts.

* **The impact on individuals** – we have already looked at potential risk of emotional, physical and financial harm.
* **The impact on Guide Dogs** – can potentially be very damaging and can include penalties issued by the ICO such as large fines, reputational damage, and even criminal proceedings for the really serious cases.

You may have heard of an incident in 2023 where the Police Service Northern Ireland had a data breach. Details of police officers were accidentally shared publicly (the wrong spreadsheet was uploaded to a website), potentially putting many people at a high risk of harm.

### Data security – top tips

To help prevent a breach from happening, we should all follow best practice so that protecting information becomes second nature.

Top tips include:

* Securely disposing of documents with personal information rather than throwing them in a bin - shredding.
* Securely locking away devices, laptops, and paper-based personal data – not left on desks when not in use.
* Encrypting USB sticks if authorised to use them.
* Locking computers when you leave from your desk.
* Not discussing or repeating personal information if unauthorised people can hear your conversation.
* Not putting any personal information in messages or message apps such as WhatsApp.

We just need to take a sensible approach and following this best practice will help protect you too while you volunteer for us.

## Subject access requests (SARs)

We would just like to end our training, with a quick look at subject access requests (SARs). It is unlikely you will come across these as volunteers, however, it is helpful for you to know what they are – just in case.

Any person (the Data Subject) has the right to ask Guide Dogs for a copy of the information that we hold about them. They can make the request to anyone at Guide Dogs – staff or volunteer. It can be verbal or in writing, and it might be for all or only a part of their personal data.

We only have one calendar month by law to respond to the request. So, if anyone does ever approach you, perhaps a service user for example or a supporter, and they say they would like a copy of information that Guide Dogs has on them, then please tell your volunteer manager, or other staff you work closely with, or the Data Protection Team straight away.

If you are not completely sure whether what you have been asked amounts to an SAR, then please do contact us and we can help.

## Further information and questions

Contact the Data Protection Team at DataProtectionOfficer@guidedogs.org.uk if you have any questions or concerns.

For information on Guide Dogs policies and procedures visit the ‘Resources’ section of the Volunteer Information Point (VIP):

<https://www.guidedogs.org.uk/vip/resources/>

For further information on data protection and cyber security, there are a range of resources available online including the websites below:

Information Commissioner’s Office <https://ico.org.uk>

National Cyber Security Centre <https://www.ncsc.gov.uk/collection/top-tips-for-staying-secure-online>

## Assessment questions

Thank you for completing this training. We hope you found it informative or a helpful refresher. You’re now ready to complete the assessment questions. We won’t be able to mark the training as completed until you have done the assessment.

If you have access to the internet, please use the following link to access the assessment questions <https://forms.office.com/e/Ai84rMFivZ>

If you don’t have access to the internet, please contact your volunteer manager who will go through the assessment questions with you and fill in the answers on your behalf.

# End of document