Key message	Answers
Consent	• Consent is obtaining permission to use the data of an individual. It must be clear about what data will be used and for what purpose. • Only share a volunteer's personal data you have consent for. • If unsure about consent, email dataprotection@girlguiding.org.uk or talk to your commissioner.
Responsibility	• Data protection is all our responsibility – we all have a role to play in keeping the data we access safe and secure. • It does not have to be scary or complicated, and most of it is common sense. • Data protection has always been a requirement of organisations. The EU has been working on updating data protection legislation for four years and the result is GDPR. Its purpose was to bring data protection into the 21st century as it was last updated in 1995.
Special category data (sensitive data)	• Special category data includes information on an individual's religion, race, ethnic origin, health, etc.
Personal data	• Personal data is anything that can be used to identify an individual – for example, personal information, such as name, date of birth, email address and also location data.
Principles (of data protection)	• In collecting and handling data, participants must ensure: ○ The data is handled lawfully, fairly and transparently. ○ The data is used only for the purpose it was given. ○ They use the minimum amount of data needed. ○ The data is kept up to date and accurate. ○ They only keep data that is actively needed. ○ The data is disposed of/destroyed securely when no longer needed. ○ The data is handled in line with the rights of the individual.

Key message	Answers
Privacy notice	• Girlguiding's Privacy notice states what data is collected and for what purposes it is used. • For example, we use the legal basis of legitimate interest to collect and store personal information to allow people to participate in guiding. (If members want to participate in guiding, we need to use their data. We don't ask for consent to do this.) • However, if we take photos, we will ask for consent before we will use a photo of an individual.
Sharing data	• Data should only be shared with people or organisations that we have stated we will share data with when we collect the data. • If we need to share data with an additional party or for a new purpose, we will need consent to do so. • Personal data can be shared without consent if it is in the public interest or it is vital in the interests of the individual to do so. Girlguiding will consider sharing data with the police or other authorities if it is required to assist in the prevention or detection of a crime.
Breach	• A data breach is an incident or omission that results in a loss, theft, deletion, unauthorised sharing or unauthorised access to personal data. Here are some examples: ○ Emailing personal data to the wrong person, leaving unit health forms on the bus, posting personal information onto social media without permission, or letting someone else use your GO account or password. Identify if it is a breach and report it as soon as possible (or within 48 hours at the latest). If in doubt, report it.
Individual rights	Data protection legislation gives individuals a number of rights over the personal data we hold and use about them. These six rights are: 1. The right to be provided with copies of the data we hold about them through a Right of Access Request, previously known as a SAR. 2. The right to have the data we hold about them corrected if they believe it is wrong.

Key message	Answers
	3. The right to have the data we hold about them deleted, if certain conditions apply. 4. The right to ask us to temporarily stop using the data we hold about them. 5. The right to question how we use the data we hold about them. 6. The right to be provided with copies of the data we hold about them in a format that can be used by another organisation, if certain conditions apply. There are some circumstances when the rights above do not need to be adhered to, for example, for national security or to prevent or detect a crime.
Retention of data	• Data should only be retained (kept for) as long as it is needed. • Be aware of the retention times for data in Girlguiding and follow them. Some data may be needed for much longer (safeguarding, finances). • Ensure data is securely and safely destroyed.
Collecting data	• Keep completed forms in a secure place. • Where possible, transfer the information from a form, email or phone call into GO as soon as you can. • When the form is no longer needed, destroy it (shred it or tear it up, so it can’t be put back together). • Use official forms on the membership section of the Girlguiding website. • Make sure no one can overhear you on the phone. • Always explain who you are and why you’re collecting the information. • Only ask for, and record, the information you really need. • Make sure you’ve collected information accurately. • Keep any personal information you collect in a secure place.
Destroying data	• Destroy data no longer needed, securely and safely. • Securely destroying **hard data** means: shredding or tearing it up, so that it can’t be put back together and read.

Key message	Answers
	- Securely destroying **soft/electronic data** means: ensuring the data has been erased permanently from anywhere where it exists. Be aware that electronic data may be saved in several places, so just pressing 'delete' may not be enough – you need to consider where it might be and ensure it is erased. For example, when downloading a document, make participants aware that it may be saved to their downloads folder automatically. When deleting documents, they will also need to empty their computer trash folder and consider where else data may be backed up to automatically, such as an iCloud linked to their phone account. They need to be extra careful when disposing of hardware (like a hard drive) and must ensure the data is encrypted.
Archiving data	- If there is personal data you need to archive you need to make sure you can locate it if you need to and it is kept safe. - If you are adding personal data to your unit's historic archive, you need to make sure that you are not storing too much personal data, for example, a person's address or phone number. These details need to be removed before adding to an archive.
Up to date	- The law requires us to keep the personal data we use up to date. To do this, it will mean that as a leader you need to make sure the data you have on GO for your leaders and your girls is checked at regular intervals to make sure it's up to date. - If there is an emergency and the phone number we have on GO for a parent/carer is out of date, this would have very serious consequences. - We also have to make sure that any distribution lists we use for sending emails to parents/carers are kept up to date. Receiving an email from an organisation that you have left three months ago is really annoying and will probably result in a complaint, but this failure to keep the data up to date is a breach of the Data Protection Act 2018 and could result in a sanction.
Disposing of data	- When participants have finished with personal data, they need to securely delete it. If it's electronic, they should delete it from their PC, and remember to check the default download folder, too. - If they have printed it, they should tear it up so that it can't be put back together and read.

Key message	Answers
Downloading data	• They should only download the quantity of personal data that they need for the specific purpose they need it for. • When they have finished with the personal data, they should securely delete it. If it's electronic, they should delete it from their PC, and remember to check the default download folder, too. • If they have printed it, they should tear it up so it can't be put back together and read. This also ensures that they don't use the same data in three months' time, when it could be out of date if there has been a change.

Printing and preparation notes:

Print double-sided, 1 per trainer.