Scenarios	Answers
Scenario 1 You're a Guide leader, and you normally collect and use a generic Activity/Event Notification and Consent form at the start of each year to cover all smaller events, such as visits to the park, for your unit. You do this because it saves on time and ensures it's easy to find in one place. Is this practice OK to ensure you are compliant with GDPR?	**Scenario 1: Answer** Leaders should not be collecting a consent form for the whole year. Instead, at Girlguiding, we advise that you use one on a termly basis. You'll need to list all the planned activities and dates for the term ahead and keep the data up to date. You can do this by emailing each parent/carer separately, asking whether the information has changed. When the events are over, the leader should securely destroy all the data unless there is a reason to keep it (for example an incident/accident took place).
Scenario 2 A unit has a camping trip coming up, and you and the other leaders want to capture some good photos of the girls. You may even video a few girls on the trip to use afterwards to promote the unit and attract new volunteers to sign up. What should you and the leaders do to ensure you are compliant with GDPR?	**Scenario 2: Answer** The leaders must ensure they have gathered consent from all the girls they wish to photograph or video and be explicitly clear about how they will use the content gathered. If the girls are under 14, the consent will need to be gathered from the girls' named primary contact. If the leaders later want to use the content for another purpose, they will need to gather consent again specifying this new use. The same rules apply to using photos or videos of volunteers.

Scenario 3 The actions of a leader in your unit have led to a breach in data. Will she be held responsible for the breach? And what does this mean?	**Scenario 3: Answer** We understand that sometimes things go wrong. If the leader shared data inappropriately or deliberately – for example, by not following policies and procedures, or selling data on, then that is a breach of the Volunteer Code of Conduct, which may affect their membership. However, if it was a genuine accident – for example, something got stolen or they sent an email by mistake to the wrong person – then we, at Girlguiding, will do our best to help them. Our Data Protection team will be able to advise them once the breach has been reported.
Scenario 4 You're a busy leader, and well into your 30-minute drive home from Rainbows when you remember that you absent-mindedly left the unit register (with girls' names and emergency contact details) in the church hall in the unit equipment box. You return to the church to retrieve it and notice that the hall is now filled with another evening community group meeting. What should you do? Is this a breach and do you need to report it?	**Scenario 4: Answer** Yes, you need to report it – ideally, straight away but no longer than 48 hours after the breach. Contact our Data Protection team, who'll be able to help you, at dataprotection@girlguiding.org.uk. Though it's unlikely anyone opened your box, it was left in a space open to the public, and unattended and accessible, for a considerable amount of time.

Scenario 5 A Brownie slipped and fell on a weekend event and has minor grazing. She had first-aid treatment at the time and is fine now. The unit leader has all the event paperwork, including the completed Notification of Incident/Accident form. What should the leader now do with the paperwork to ensure she is compliant with GDPR?	**Scenario 5: Answer** The leader should scan or copy the form and send the original to Girlguiding HQ. Once HQ has confirmed they have received it, the unit leader should securely destroy her copy. 'Securely destroy' means to shred or tear up into pieces, so it cannot be put back together and read.
Scenario 6 The venue where your unit meets doesn't have Wi-Fi and, therefore, you're unable to access GO while there. What information do you take to the meeting? And how should you handle it safely?	**Scenario 6: Answer** As you know, you still need to access certain information for your meeting. This may include an attendance register, health form or emergency contact list. You can have them as password protected files on your laptop or tablet. If you don't have a portable device, you can have paper documents. If using paper copies, make sure that the information is up to date (by regularly asking parents/carers for any changes) and is kept safe during the meeting. 'Keeping it safe' means keeping it away from those who should not see it, so might mean keeping it zipped up in your bag, so that others are unable to access it without you knowing. After the meeting, keep it in a secure place in your home and don't leave it in your car, etc.

Scenario 7 You are a commissioner concerned about whether all of your volunteers are following data protection good practice guidelines. As a commissioner, how can you ensure your volunteers are compliant with GDPR? And, are commissioners responsible if the volunteers they support don't comply with GDPR?	**Scenario 7: Answer** All volunteers are expected to keep up to date on Girlguiding's policies and procedures. It's part of their membership conditions – they must follow the Volunteer Code of Conduct. Keep reminding them of their responsibilities and that they must follow the checklist on the GDPR webpages, so that they're always up to date. Commissioners are responsible for ensuring that the volunteers they support know about the data protection guidance and know that they must comply with Girlguiding's Managing Information policy and the data protection procedures. As long as you've done this, you won't be held responsible for your volunteers not complying with GDPR. All volunteers agree to the Girlguiding Volunteer Code of Conduct, which stipulates that they must adhere to all Girlguiding's policies and procedures, including data protection. If a volunteer doesn't do this, they may have a disciplinary action taken against them. A commissioner wouldn't face disciplinary action for a volunteer's non-compliance, unless they've been negligent in their responsibility to support volunteers to know about data protection procedures or have been non-compliant themselves.
Scenario 8 As a leader, you're trying to ensure you don't have any data you aren't actively using and want to securely destroy all unneeded data. You're also concerned about destroying any needed data or destroying records of the unit's history. You want to keep records of the first meetings you had and some photos from across the years, which you don't have permission for. You can't even remember who all the girls were, so can't contact them to ask for their consent.	**Scenario 8: Answer** Archives, by definition, involve the long-term storage of documents and items that record an organisation's history. As a result, archives should only contain the selected information that constitutes a summary of an organisation's history – it's not an excuse to be able to retain everything. Ensure data is depersonalised by minimising the personal data it contains – for example, by deleting names, dates of birth, addresses, phone numbers and so on, so an individual cannot be identified. You may keep photos/videos, but ensure there are no names attached to them. Ensure there's a visible and transparent process applied to retaining this data, which can allow the purpose of maintaining the archive to be achieved, while ensuring an individual's rights and freedoms are protected. Note: all financial data must be kept for the financial year it was collected, plus six years. Records of gift aid must be kept for the year of last donation, plus six years.

What can you keep in terms of retaining old meeting information? What should you keep?	If unsure, contact the Data Protection team at Girlguiding HQ.
Scenario 9 You belong to several unofficial Facebook groups for guiding, where you chat and share details on events and good offers related to guiding with members, parents/carers and other volunteers. You also use WhatsApp with other leaders and parents/carers to discuss guiding activities. Is it OK to still be using these social media platforms like this? If yes, why? And what should you be aware of? If not, why?	**Scenario 9: Answer** For WhatsApp you need to contact the individuals and ask them to join the group – in effect gaining their consent. Do this by email, as their reply will be your evidence of consent. They'll then be able to leave at any time, if they wish to do so. For Facebook, individuals have to opt in anyway to be a part of the group, so – again – they're giving consent. When using any social media platform, please don't share any personal information (for example, photos, which you don't have permission to use for that purpose). Note: according to Girlguiding's Managing Information policy, you can't have a social media group for members under the age of 14, including closed or secret Facebook groups. If you want to contact Guides or younger girls, you would need to go through their parents/carers.
Scenario 10 A disclosure has been made to a volunteer and they have taken notes on what was said. The volunteer has called and relayed this information to a staff member at Girlguiding HQ. What should the volunteer now do with the notes?	**Scenario 10: Answer** The following guidelines should be adhered to: 1. Scan/copy the notes. (If this is not possible, try to scan through the country/region office. If this is not possible, post the originals securely (for example, signed for) to Girlguiding HQ, along with a completed notification form. 2. Password protect the documents and email them to safeguarding@girlguiding.org.uk. 3. Girlguiding HQ will confirm receipt of the notes. 4. Once the Safeguarding team has confirmed they have received them, the copy the volunteer has should be securely destroyed. 'Securely destroy' means shredding or tearing up the data, so it will not be possible to reassemble the information, or deleting from anywhere it may be held electronically. This is a data security requirement, as well as prevention of retaining duplicated information.

Scenario 11 You're a leader and there's a parental dispute. A Guide's father, who is estranged from his wife and not the Guide's named primary contact adult, calls you asking for details of where his daughter is on a residential. What should you do?	**Scenario 11: Answer** At unit level, we cannot share personal data with an individual who is not the named primary contact recorded on GO, or an individual the named primary contact has named as an authorised emergency contact. This is to ensure the safety of the child. In this situation, the father has the right to be told this information. However, we need to be sure he is entitled to receive it. This cautious approach is to always ensure that we consider what is in the best interests of the child. Without a child arrangements order, one parent is not at liberty to block the other parent's access (Children Act 1989). The father will need to contact Girlguiding HQ and be prepared to prove his identity and his parental responsibility, in other words providing a copy of the child's birth certificate with his name on the certificate, or by providing a copy of a child arrangements order.
Scenario 12 You have been asked to supply any historic (past) potential safeguarding cases you are aware of. What is the process for handing over this data? And, are there any special considerations you need to make?	**Scenario 12: Answer** We, at Girlguiding, state in our *Privacy notice*: We will share personal data when it is in the public's interest to do so. A safeguarding investigation/case is a situation in which, if doing so has the purpose of protecting a child or vulnerable person, or is for the purposes of detecting or preventing a crime, Girlguiding can and will share personal data. The Safeguarding team will provide details of the process required to send any historic (past) potential safeguarding cases to Girlguiding HQ for all levels.
Scenario 13 You're stepping down from your volunteer role and have been involved in a	**Scenario 13: Answer** If the safeguarding case is still active, you will need to make sure that you provide all the necessary information to allow the new volunteer to carry on in the role/case. In other words, you should

safeguarding case. What steps should you take in relation to data protection and handing over the case you have been involved in?	notify the Safeguarding, Complaints and Compliance teams of the change, and agree the handover information and notes. If the case is closed and there is a restriction on a member of the unit/region, this information will need to be passed on to the new volunteer in a handover meeting. Or it could be given to the appropriate commissioner, who is overseeing the handover. If the case is closed and no action was taken or was necessary, the case details do not need to be passed on as there is no reason for sharing this information. However, we ask you to check with the Safeguarding team before you destroy the material, in case they don't have a copy.
Scenario 14 As a leader, you keep a downloaded list of parents'/carers' email addresses, so that when you're arranging an event, for example, you can email those directly who are not part of the Facebook group you use to post event updates. Is it OK to have this list of email addresses? If yes, why and what should you be aware of? If not, why?	**Scenario 14: Answer** No. You shouldn't be using lists outside GO, unless it's a group address book that is kept up to date in your email account. It's acceptable to save their email addresses in an email address book – you don't need permission for that. However, when emailing a group of parents/carers, always make sure you blind copy (BCC) them into the email and never share personal data. When a girl leaves your unit, remember to remove her parents'/carers' email address from your email address book.
Scenario 15 As a volunteer, you have regularly been sending out e-newsletters to parents/carers and volunteers, which contain information on offers available to members, information about local events	**Scenario 15: Answer** It is OK to continue to email information about guiding activities to parents/carers and volunteers (and members aged 14 and over). However, for anything related to marketing or fundraising (for example, sharing details of a special offer or writing about a fundraising event), you must ensure you have permission to do this. Consent must be evidenced, meaning you have to be able to prove you have it. An email, a ticked box on a form or a text message is evidence. However, you must

and other information on what the unit is doing over the coming weeks. Is this OK? If yes, why and what should you be aware of? If not, why?	provide clear information for what a person is consenting to, to make sure the consent is valid (for example, 'Do you want to receive information on special offers and fundraising events?'). You should be able to pull off an 'opt-in' list from GO of those who have selected to receive this type of communication. Note: you can share marketing and fundraising information by hard copy (for example, through the post or handing out leaflets) without special permission. But, if asked, you would need to stop sending it.
Scenario 16 A leader in your unit has shared that they have heard you should be shredding forms and information you are not actively using to ensure you are GDPR compliant. They are concerned about what your unit should be doing and want to get it right. They are particularly concerned about what parts of the new starter form should be disposed of and when. What advice could you give them to clarify what needs to be done and by when, to ensure your unit is GDPR compliant?	**Scenario 16: Answer** Many of our Girlguiding forms, when completed, have personal data for a specific reason – for example, an event. Once that specific reason is over, the form can be securely destroyed unless there was an accident, in which case email it to insurancesupport@girlguiding.org.uk, or a safeguarding concern, in which case send it to safeguarding@girlguiding.org.uk. A good example might be the new starter form. Pages one to two should be given to the parent/carer; pages three to five include personal information that needs to be added to GO. Once this has happened, they can be destroyed. Don't forget to log any medical issues onto GO. The gift aid form is valid for six years, plus the year of the last donation, so please keep that with your unit's finance records. For more information on data retention see the Girlguiding GDPR webpages. Note: the new starter forms will be changing and you'll be able to keep the part of the form that includes the parents'/carers' signatures and gift aid as a detachable section. Note: information collected on the older new starter forms that isn't collected on GO, such as parents'/carers' volunteering options, school, ethnicity and so on, will not be collected on the new forms.

Scenario 17 As a volunteer, you know you should not be keeping all data from the various forms you use, old registers, photos of events taken and so on. But you're also aware some information must be kept or shared with Girlguiding HQ, such as financial records or safeguarding case notes. What should you be: 1) sending to Girlguiding Trading Service for safekeeping, 2) keeping in a safe place locally, or 3) securely destroying?	**Scenario 17: Answer** There are three actions to take with data you have: 1. **Send to us at Girlguiding, care of our Trading Service in Altrincham:** • Any health forms for activities and residentials, which have already taken place and where there was an accident or safeguarding incident (for the girl/s involve in the accident/incident). • Consent forms for activities and residentials, which have already taken place and where there was an accident or safeguarding incident (for the girl/s involve in the accident/incident). • Any paperwork/electronic records relating to safeguarding concerns you might have dealt with, which you reported at the time to district, division, county, country/region or Girlguiding HQ. • Any paperwork/electronic records, where you've noted any safeguarding concern associated with either a unit or previous role within Girlguiding, for example an activity form. • Any paperwork/electronic records that you decided not to report at the time, as you weren't sure or it wasn't appropriate to do so. All of this information will be kept on file but there may be cases where we need to follow up further. 2. **Keep in a safe place:** • Current records. Keep these until they are no longer needed, for example when a girl leaves a unit, or the event has taken place. • Financial records from the last six years, plus year of their creation (or year of last donation for gift aid forms). • Other documents that you're currently using.

	Or 3. **Securely destroy:** • Any other health forms for activities and residentials, which have already taken place without any accidents or safeguarding incidents. • Consent forms for activities and residentials, which have already taken place without any accidents or safeguarding incidents. • Old unit starting forms. • Current starting forms after you've updated GO. KEEP current gift aid forms. • Financial records older than six years, plus the year of their creation, including old gift aid forms. • Paper registers. • Six/Patrol registers no longer used. • Old electronic registers or spreadsheets. • Emergency contact lists, either paper or electronic. • Any documents, either electronic or paper, which list personal information or contact details. • County/local directories. • Old booking forms/order forms. • Any non-safeguarding records/paperwork passed on by a previous leader or volunteer. If you're not sure whether to keep or destroy a document you find, contact the Data Protection team at Girlguiding, on 020 7834 6242, extension 3060.

Printing and preparation notes:
Print double-sided, 1x trainer.