Scouts
Chester and District

DATA PROTECTION

How you can help to keep personal data safe

1. Know the personal data you are holding as part of your involvement in the Scouts (young people, adults, third parties)

2. Know all the places you might have people's data (laptop/desktop, mobile, Compass, Online Scout Manager, Google Drive, Microsoft One Drive, Dropbox, Office 365, YouTube, paper forms in your home/workplace/car…)

3. Know the various collection methods (for example, paper form, web form, e-mail, OSM, Compass, social media, other…)

4. Know and justify the purpose(s) for which you are collecting and storing the personal data

5. Collect and process the personal data with the full knowledge and consent of the people involved

6. Download or print personal data where it is necessary – but not otherwise

7. Know how long the data will be in use

8. Know all parties to whom you transfer personal data (The Scout Association, other leaders in the Group, event organisers, social media, YouTube, WhatsApp, cloud storage providers…)

9. Know who has access to the personal data – only allow access to those who need it (for example, the First Aider at camp will have access to health data of camp attendees but not every adult volunteer at camp)

10. Keep personal data on a device that is password protected and do not share passwords

11. Securely destroy personal data you no longer need

12. If you lose any personal data or share it wrongly, inform your Executive Committee

Personal data is information about a person that will identify them. Examples:

- Name
- Address
- E-mail address
- Phone number
- Date of Birth
- Images of persons (photographs and videos)

In the Scouts, we regularly collect, process and transfer **Sensitive Personal Data** (also known as special category data) such as race, religion/faith and health. For example:

- Membership, both adult volunteers and young people.
- Camps and other events
- Awards, moving on between Sections
- Census
- Health and medical records
- Management of safeguarding incidents

Click *here* to access the latest information from UKHQ

There is *mandatory learning* on the GDPR. This is done online and validated by a Training Adviser either as part of Module 1 (for new leaders) or separately for existing ones. If you have any problems with validation, consult your Local Training Manager

We prepare young people with skills for life

Processing personal data – collection and use

Processing personal data on paper or electronically

- Keep until no longer needed. If you cannot justify retaining the data, then it should be securely deleted as soon as it is no longer required.
- There are special rules for financial records

Examples of personal data

- Membership records including badge records of young persons.
- Financial records according to the data retention period
- Permission forms for events
- Contact lists (In Touch procedure) and directories (paper or electronic)
- Registers (paper or electronic)
- Health data and other sensitive data to support Scout activities
- Any other document or file containing personal data

Processing personal data by capturing images – photographs and video

- Only publish photographs and video clips of adult volunteers and young people, produced during Scout activities, on social media, web sites and other publications if consent has been given
- There is a specimen form of consent in our social media guidance, which can be used at the same time as other information is obtained relating to the member concerned. You can download a Word version to help with setting up the consent form on your computer

Processing personal data by phone or email

- Take care not to be overheard when you are on the phone
- Make it clear who you are and why you are collecting the personal data
- Only ask for personal data that is accurate and is relevant to your purpose(s)
- Keep/transfer the collected personal data in a secure place as soon as possible
- Minimise the use of email to the absolute necessary when collecting or transferring personal data.
- Take care when replying to all in the email chain and ensure only intended recipients are part of any on-going communications
- BCC email addresses when sending emails to multiple recipients to avoid sharing the email address of an individual unless it is for a specific Scout purpose and consent to do so has been given

Although email is an effective way to communicate, a mistyped email address is a common mistake and results in disclosure to an unintended recipient

Where can you find personal data relevant to Scouting?

- At home (paper files in cupboards/attic/other rooms/sheds/garages)
- Scout meeting place (paper files in filing cabinets, car boot, cupboards)
- Online storage systems (Dropbox, Google Drive, OneDrive …)
- Current and old laptops, desktops, tablets, mobile phones or other devices
- Photographs and video clips of Scouting members in all your devices, storage facilities and those shared on social media
- CDs, discs, memory sticks that you may have used to store personal data in relation to Scouting
- Email accounts

Secure data storage and destruction of personal data

(Secure data storage means keeping the personal data in your care in a secure place where unauthorised access is blocked. It is also vital to destroy personal data properly when no longer needed)

For paper records

- Only print data if necessary. Paper should be the last resort for collection, storage or transfer of data
- Ensure transfer of paper is secure, such as physical hand-to-hand transfer or signed-for post to the intended recipient(s)
- Destroy paper records securely after the purpose is completed. This means shredding into pieces so that these cannot be put back together prior to binning it

For non-paper records

- Ensure that a safe and secure storage system is being used
    - Secure cloud storage
    - Online membership system
    - Strong password-protected, virus-free electronic devices

- Ensure that applications used on devices do not have access to personal data stored.

> Some applications require access to personal data stored in a device as a condition of using the app. This includes WhatsApp, which transfers the phone book on a mobile phone containing all contact information, including those who have not given consent

- Check the terms and conditions and privacy notice of your intended cloud storage provider, email provider, web server, online survey tool etc to ensure that the personal data in your care is not compromised

Some cloud-based storage providers such as Google claim a worldwide licence to further process any content including personal/sensitive personal data received through using Google services including Gmail, Google Docs, and Google Forms

Google is a US based company and any personal data going through Google is a transfer to a third party out of the EU, and raises the question of whether there is a justified, legitimate reason to do so. Google specifically states in its EU User Policy that EU Users must obtain consent to any data collection, sharing and usage of Google's services

- Limit access to personal data to those whose Scout role entitles them to see it
- Do not download personal data onto shared computers or work computers where other people could access the data
- Restrict access to personal data on Scout web sites by using a strong username and password
- Where using digital forms or online surveys to capture personal data, ensure that there are secure transfer mechanisms. For example, the link should start with https://
- Delete personal data when no longer required. This means deleting it and emptying the recycling bin
- Destroy CDs by scratching or breaking them before throwing them in the bin
- Check that there is no more personal data in your electronic device if you later sell/discard it

The choice we make in our personal life to share photographs and other personal information about ourselves and family or friends in the course of our personal activities does not apply in our Scouting roles, where the data protection principles come into play.

6 June 2018

Note for Executive Committees

It is vital that the Executive Committee, as data controller, supports volunteers and helps them with any questions or concerns they may have.

In addition to going through the above guidance and checklists:

- Support your volunteers with anything that may be linked to data protection and safeguarding
- Check Scout buildings for any records, either paper or electronic, that contain personal data
- Do a Data Protection Impact Assessment where the processing is likely to result in high risk to individuals, (unlikely in most Groups and Districts) for example:
  - Where a new technology is being deployed
  - Where a profiling operation is likely to significantly affect individuals or
  - Where there is processing on a large scale of the special categories of data.
- Check that your third party processors (OSM, etc) comply with their obligations under the relevant legislation. You can use the GDPR Third Party Processor Checklist Template, which is part of the ***GDPR Toolkit***
- Securely destroy contact lists for training, camps or other events/activities that have passed.
- Securely destroy personal data of young persons, adults and third parties once the purpose for collection has ended, including those on emails, paper copies and/or stored in your computer, laptop or any other device
- Securely destroy records that hold personal information no longer needed, For example: contact details, photographs and video clips used as evidence for training purposes etc

6 June 2018