****

**2**

|  |
| --- |
| **[insert name of Group]** |

Note from Bishop’s Stortford and District Scouting: *this policy has been drafted to make all volunteers adults in the Group or Section aware of their obligations under the new General Data Protection Regulation (GDPR) from 25 May 2018. This* provides practical guidance for volunteers to keep personal data safe – it is not a document for parents or youth members. The District does not know how data is looked after in the Group and this template should be a guide. The broad text is recommended and where there are [ brackets ] you need to insert your relevant Group information. It is recommended you do not stray too far from the text as when the regulations change, the District will send out changes to this template. If you have questions email the District Commissioner, Greg [here](mailto:gregjmstewart@hotmail.co.uk).

**Data Security Policy for Group Volunteers**

Introduction

Information security is about what you and the Scout Group should do to make sure that all personal data **i**s kept safe and it is very important that you get this right. Most data protection fines result from information security breaches.

This Group policy need to be read alongside the Scout Group’s **Data Protection Policy for Volunteers** which gives you an overview of you and the Group’s obligations for data protection. You also need to read and understand the Group’s Privacy Notices for Parents [🡺 *insert any other polices of the Group that should be read e.g. use of images]*.

This policy is for all volunteers and Young Leaders (which includes Group Executive Members and Occasional Helpers) when handling Personal Data. If you have any questions or concerns about your obligations with this policy they should be referred to [🡺 *insert role (not name) of person responsible for the Group data Protection*].

Be cautious!

Data security breaches can happen in different ways. Examples of breaches which get media coverage include:

* + - Personal Data taken after a website was hacked;
    - an unencrypted laptop being stolen after being left in a car;
    - sending a confidential emails to the wrong recipient;
    - leaving confidential documents on a doorstep; and
    - using carbon copy (cc) rather than blind carbon copy (bcc) to send emails to multiple recipients.

These give you a good idea of the type of things that can go wrong. Try and think about what problems might arise in your Section and what you can do to manage the risks. Talk to your Section Leader or Group Scout Leader if you have ideas about improving practices in the Group or Section.

You must **immediately** report all security breaches, incidents and weaknesses to the Group Scout Leader or *[🡺 insert role (not name) of person responsible for the Group data Protection].*

You must **immediately** tell *[🡺 insert role (not name) of person responsible for the Group data Protection]* if you see anything which might mean that there has been a security breach. You must give all of the information you can.

If it is outside normal meeting times then please report it - do not wait - report immediately no matter what time of day. All of the following are examples of a security breach:

* + - you accidently send an email with personal data to the wrong recipient;
    - you cannot find papers which contain Personal Data; or
    - any device (such as a laptop or a smartphone) used to access or store Personal Data has been lost or stolen or you suspect that the security of a device has been compromised.

In certain situations the Scout Group must report information security breaches to the Information Commissioner's Office (the data protection regulator). You may also have to let those know whose information has been compromised, all within strict timescales. This is another reason why it is vital that you report breaches **immediately**.

Always focus on privacy

We should be thinking about data protection and privacy whenever handling any Personal Data. From May 2018, we are required to carry out an assessment of the privacy implications of using Personal Data. These assessments must be help the Scout Group to demonstrate the measures needed to prevent information security breaches from taking place, especially if we are ever involved in an investigation by the Information Commissioner’s Office.

Special Category Data

Data protection is about protecting information about individuals. Something as simple as a person's name or their hobbies count as their Personal Data. However, some Personal Data is so sensitive that we need to be extra careful. This is called Special Category Data - you must be extra careful when handling this. Special Category Data is:

* + - information concerning safeguarding matters;
    - information about serious medical conditions and information about Special Needs;
    - information about allegations made against someone (whether or not the allegation is a criminal offence and whether it has been proved);
    - bank details (for example about parents and volunteers);
    - information about an individual's ethnic or racial origin;
    - political views;
    - religious beliefs or other beliefs of a similar nature;
    - trade union membership;
    - physical or mental health or condition;
    - genetic information;
    - sexual orientation;
    - information relating to actual or alleged criminal activity; and
    - biometric information.

Limit the amount of Personal Data held

Try to keep a minimum amount of Personal Data on young people and adults helps keep data safe.

Using IT and computers

Many data protection breaches occur as a result of basic mistakes when using computers. Here are some suggestions to avoid problems:

* + Lock device screens: Your phone, computer or tablet should be locked when not in use, even if you are away only for a short time.
  + Private cloud storage: You should avoid using private cloud storage or private file sharing accounts to store or share Scouting documents. Documents should be kept in Group cloud accounts such as Google docs or a Scout Dropbox account.
  + Portable media: Portable media devices (such as USB drives, portable hard drives, DVDs) should be kept to a minimum – avoid it if possible. If you have to use one it must be encrypted.
  + Disposal of equipment: Laptops, printers, phones, and DVDs must always be disposed of in a secure way so that data cannot be retrieved. Seek advice on how to do this safely,

Passwords

Your password should be difficult to guess and must be long, for example, you could use a song lyric or a memorable phrase e.g. *standbyyourman(1966)* Your password should not be disclosed to anyone else. You could also base your password on something memorable that no-one else would know. For example the name of your first pet and your dad’s year of birth. You should not use information which other people might know or be able to find out such as your address or your birthday. Passwords should not be written down.

Emails

When sending emails, take care to make sure that the recipients are correct.

Emails to multiple recipients: A blind carbon copy (bcc) function must be used when sending emails to multiple email recipients (more than 2) so that names and email address are not visible to other recipients. This includes email to parents, Leaders and young people. People may not want their email address seen by others and by letting other people know you would be in breach of regulations.

If the email contains Special Category Data, get someone to double check that you have entered the email address correctly before pressing send.

Encryption: Emails containing Special Category Data must be encrypted. For example, encryption should be used when sending details of a complaint or health matter. If you need help encrypting a file please ask *[🡺 insert role (not name) of person responsible for the Group data Protection]*. If you need to give someone the "password" or "key" to unlock an encrypted email or document then this should be provided via a different means e.g. after emailing the encrypted documents you could call the recipient with the password.

[🡺 *the following point is strongly recommended* ]Private email addresses: You must not use a private email address for Scouting related work. You must only use an email address provided to you from the Scout Group. This is because if you leave or were ill, the GSL could gain access to the information. To comply with the law, we also need access to all emails and related documents if a Subject Access Request is made. If this information is held in a private account - Scouting does not have legal control of the data.

Paper files

These are as important to protect as digital data.

Keep under lock and key:You must ensure that any papers containing Personal Data are kept under lock and key in a secure location at home or at the meeting place and that they are never left unattended.

Disposal: Personal Data should **never** be placed in the general waste. Paper records containing Personal Data should be disposed of by securely shredding. If you don’t have a shredder as the GSL where you can use one.

Printing:When printing documents at the meeting place or perhaps at work, make sure that you collect everything from the printer immediately, otherwise there is a risk that confidential information could be read or collated by someone else.

Post: You also need to be extra careful when sending items in the post. Confidential materials should be sent by registered post and it must be marked “Private and Confidential” and contain a return to sender address

Keeping data at home or away from home

You might need to take Personal Data out of your home or Scout HQ site for various reasons. This does not breach data protection law as long as safeguards are in place to protect Personal Data.

Take the minimum:A leader organising a hike might need to take with them information about Scouts medical conditions (for example allergies and medication). If only eight out twenty Scouts are attending the trip, then the Leader should only take the medical information about the eight Scouts.

Data on the move:You should not work on documents containing any Personal Data whilst travelling if there is a risk of unauthorised disclosure. For example, if working on a laptop on a train, you should ensure that no one else can see the screen. Never leave any device unattended.

Paper records:If you need to take hard copy (i.e. paper) records out with you then you should make sure that they are kept secure. For example:

* + - documents should be kept in a locked case. They should also be kept somewhere secure in addition to being kept in a locked case if left unattended (e.g. overnight);
    - if travelling by car, you must keep the documents out of sight. Possessions left on car seats are vulnerable to theft;
    - if you have a choice between leaving documents in a vehicle and taking them with you (e.g. to a meeting) then you should take them with you and keep them on your person in a locked case. However, there may be specific circumstances when you consider that it would be safer to leave them in a locked case in the vehicle out of plain sight.

Public Wi-Fi: Public Wi-Fi is not secure so try not to use it for Scouting data.

Your personal devices and Scouting

You may use your personal device (such as your laptop or smartphone) for Scouting but this must be secure and encrypted.

Security: appropriate security measures should always be taken. Use firewalls and anti-virus software and should be kept up to date.

Friends and family: You must take steps to ensure that others who use your device (for example, friends and family) cannot access anything Scouting related e.g. you should not share the login details with others and you should log out of a Scout account once you have finished. You must also make sure that your devices are not configured in a way that would allow someone else access to Scouting related documents and information.

Breach of this policy

Any volunteer who deliberately or recklessly discloses Personal Data held by Scouting without proper authority is guilty of a criminal offence and gross misconduct and would be subject to the consequences of the rules of the organisation. Treat Data Protection as you would Safeguarding matters – confidentially, carefully and most seriously.

Date policy AGREED:

Next REVIEW date:

**Data Security Policy for Group Volunteers**

I confirm that I have read and understood the contents of the Group Data Security Policy:

|  |  |
| --- | --- |
| Name of volunteer: |  |

|  |  |
| --- | --- |
| Signed |  |

|  |  |
| --- | --- |
| Date |  |