BLACK PENNY CONSULTING

scouts be prepared . . .

The GDPR toolkit

Data Security Best Practices…

Version 1.0 – March 2018

Contents

Data

When it comes to the protection of data there are some common best practices that can help maintain strong processes.

As part of local scouting, Sensitive Personal Data (also known as special category data) is gathered, processed and transferred frequently. For example:

- New joiner details, be that Adult Volunteer or a Young Person.
- Processing of this data for the purposes of events, awards, moving on.
- Annual reviews of this data through census or further data gathering to update medical records.
- Management of safeguarding incidents where data needs to be transferred to 3rd parties for assistance.

Consideration needs to be made when collecting, managing and transferring the data required to operate local Scouting.

This can be broken down into simple questions to ask yourself:

What?

What data am I collecting on the Adult Volunteers and Young Members? Do I know the details I am asking the individuals to give me? This could be details such as:

- Name
- Address
- E-mail address
- Date of Birth

These data types are known as Personal Data, this becomes Sensitive Personal Data when you add information such as:

- Race
- Ethnic origin
- Religion
- Health

Why?

Why am I collecting the data? Can I determine a reason for this data collection and use, and does that align with the lawful purposes as defined by the GDPR? For example:

- The collection of Young People's medical records is necessary for the protection of that Young Person whilst in the care of the Scout Group.
- The collection of Young People's religion is necessary to respect their beliefs with regards to activities, food and holidays.
- The collection of Adult Volunteers data is necessary for the purposes of disclosure checks and safeguarding.

If I can't justify the reason behind the gathering or use of a certain type of Personal or Sensitive Personal Data, then I shouldn't. This guidance will come from the Executive Committee.

How?

There are many means by which you can gather and use data, this is explored further in this guide, however the key question is; how am I collecting the data and how am I using it? The consideration needs to be whether you can demonstrate that you know this information and it has been well thought through as the best way to achieve this.

When?

When should I delete the data I hold? Whilst the use of the data is required for the provision of local Scouting operations, the longer-term retention needs to be justified. For example:

- The Young Person's awards records are retained for a defined period when they leave in case they wanted to return and continue.
- Adult Volunteer data is retained for a defined period post leaving for the purposes of ongoing handover of the appointment.
- Gift aid data needs to be retained for 7 years to meet audit requirements by HMRC.

If justification cannot be made for the retention of data, then it should be securely deleted at the point it is no longer required.

Guidance will be provided by the Executive Committee on the types of data you can capture and for how long.

Who?

Who can access the data? This access could be via memberships systems, paper records or via email. In all cases the access to this data needs to be minimised to only who needs it and, if possible, only the subset of data they need, for example:

- The Group Scout Leader and Section Leader will require access to data for the Young People and Adult Volunteers in their group.

- Adult Volunteers may require access to the data of the Young People but potentially not to the other Adult Volunteers in their Scout Group.

If any of the above are in doubt, then please refer to the Executive Committee for guidance. The questions above should be asked to assist in the protection of personal and sensitive personal data, in the case of local Scouting, this is young people's data and duty of care should be considered.

Where

Where do I store the data I have for local Scouting? There are many places this data can be stored, and these will normally be chosen based on ease of use or what you are used to using. Consideration needs to be made for the decision as to where the data is stored such as:

- Is the storage system secure and safe?
- Who needs access to the system and can we easily collaborate?
- Can I trace access to the storage location and minimise where necessary?
- Is there a reputable system available today that I can use, such as?
    - Secure cloud storage.
    - Online membership system.

All of the above questions help in constructing an appropriate Privacy Policy and subsequent Privacy Notices where you are capturing data.

Data Media Guidance

Today's technology age means that there are many tools available to us all when it comes to the management of our day to day jobs and activities.

This situation exists within local Scouting and in most cases, you will opt to use the tooling you are familiar with or makes your operation as easy as possible. The below guidance draws out these technologies and gives advice on the security measures that should be considered:

Paper

Whilst not strictly a technology, paper is still widely used to capture and retain data. This is the case within Scouting and as such needs to be considered, for example paper-based records could exist for the following:

- New joiners form
- New joiners waiting lists
- Events consent from parents
- Annual health records updates
- Events coordination with events companies
- Award notifications/nominations

The following should be considered when using paper:

- Not digitally searchable – not easy to find specific information
- If lost or damaged it's not recoverable
- Not easy to transfer
- Prone to error or misinterpretation
- Requires physical storage and security

In some cases, paper-based records are justified or the only means of data capture, where this is the case then duty of care needs to be considered, such as:

- Minimise the use of paper to only what is required.
- Transfer of paper is secure, such as physical hand to hand transfer or registered post.
- Paper forms are securely destroyed post use if possible.
- Secure destruction should be through a shredding machine.
- Keep the paper records secure always, especially when in transit, consider using:
    - A lockable brief case.
    - A lockable filing cabinet if long term stored.
    - If transferred to somebody, audit that they return them when complete.

Paper should be considered a last resort for data gathering/storage or transfer.

Digital forms

Digital forms offer the ability to capture data in a digital means via a website link. The form is presented to the person entering the details as designed by yourself.

The following should be considered when using web forms/online surveys:

- Digital forms can be from your own website, online survey tool or a membership database.
- Digital forms are widely used and accepted as means for gathering data.
- They need to be carefully created to capture only the data required and offer a clear capture flow.
- Digital forms reduce mistakes of data capture.

Where web forms or digital surveys are being used the following best practices should be considered:

- The presentation of the form is easy to understand and follow.
- The form itself is using a secure transfer mechanism, the link to it should start with 'HTTPS://'.
- You understand how the data is used after the form is completed, is it emailed to yourself, is it retained in the website?
- If the detail is emailed to yourself post it being completed this email should be treated with care and deleted when not required any further.
- If the data is retained on the website, then ensure access to this website is protected by a strong username and password and the access to it is limited to only those that require the data.
- Delete any data that is not needed from the locations it is stored.

Digital forms are a good way to gather accurate data in a secure way.

E-Mail

The most common communication tool used today is e-mail. This can be either personal or corporate e-mail from a large variety of providers. E-mail is used commonly to transfer all types of data and can be used to either transfer forms with information in or the data directly in the body of the e-mail itself.

The following should be considered when using e-mail to gather or transfer data:

- E-mails are sent in clear text, this means that if they are intercepted the contents can be read.
- Most e-mail systems retain lots of copies of the data sent and received, for example in:
    - Inbox folder
    - Sent items folder
    - Deleted folder
- It is easy to mistype an e-mail address or select an incorrect pre-populated address.
- The security of an e-mail system varies depending on the service provided.
- E-mails can be stored locally on your laptop/desktop.

Where e-mail is being used the following best practices should be considered:

- Free e-mail services generally lack a level of security appropriate for sending lots of sensitive personal data.
- Review the e-mail service you have; good service add-ons include:
    - Anti-virus scanning
    - Anti-malware scanning
    - Encrypted e-mail
- Delete e-mails when they are no longer required, especially if they contain data-based attachments, this should be from the folders highlighted above.
- Add a delay to the sending of your e-mails by 2 minutes. Most email clients allow this as a 'Rule', any mis-typed email can then be stopped before it leaves.
- Don't store your e-mails locally on your laptop/desktop to minimise the data you store, guidance can be found here: https://social.technet.microsoft.com/Forums/office/en-US/d630dc5e-22b5-40ec-85f6-5e369384be4c/how-to-set-outlook-to-online-mode?forum=outlook.
- Minimise the use of e-mail to what is necessary when it comes to gathering or transferring data.
- Take care when replying to all in the email chain, you may not want all email participants to be part of any on-going communications.
- If you are looking to send an email to multiple individuals and don't want everybody to see the email addresses on the distribution list, then simply add all of their email addresses to the 'BCC' field. You can then add your own email address in the 'TO' field, this will mask all addresses except yours.

Additionally, e-mail mass mailers may be used to communicate with the local scouting community, this is required for updates, events and other operational means. When looking at a service like this you should consider the following:

- Is the service with a reputable provider?
- Is the data set I am providing minimised to only what is required?
- Does the data get stored with the provider, if so can I delete it when finished with?

E-mail is an effective way to communicate but can lead to lots of data across lots of folders. 85% of all reported data breaches in the UK come from e-mail to the wrong recipient.

Laptop/Desktop/Tablet

Laptops/desktops/tablets are common place in most households as well as in peoples place of work. As Adult Volunteers within The Movement you will probably have access to or be using this type of technology to manage the operations for local Scouting.

Security of laptops/desktops/tablets is key when gathering/storing or transferring data, the security already in place for the physical device could vary depending on if this is company or personal asset and your line of work.

The following should be considered when using a laptop/desktop to gather, store or transfer data:

- Is the laptop/desktop a shared resource?
- Who owns the laptop/desktop and is ultimately responsible for it?
- How is the laptop/desktop/tablet to be used?
    - Transient, data comes in and out but is not stored on it.
    - Data is stored locally.

Where a laptop/desktop is being used the following best practices should be considered:

- The laptop/desktop is protected by a username and strong password, strong is defined as:
    - Consists of at least eight characters.
    - Combination of letters, numbers and symbols (@, #, $, %, etc.).
    - Contains letters in both uppercase and lowercase.
- The laptop/desktop includes hard disk encryption – Check your operating system provider and google for options of hard disk encryption.
- Software packages such as anti-virus and anti-malware are included.
- Software on the laptop/desktop is up to date.
- Implement a digital password safe to store all passwords you must remember, there are many free tools available.
- Storage of data locally is minimised to only what is required.

Laptops especially are very useful for mobile management of local scouting, but the mobile element introduces a loss or theft risk. Reduce the exposure by considering the measures above.

Consent

Consent is a lawful means by which you can capture, process or transfer data. For local Scouting most of the reasons you have for data ownership are already justified based on the obligations you undertake as part of your role, for example:

- The collection of Young People's medical records is necessary for the protection of that Young Person whilst in the care of the Scout Group.
- The collection of Young People's religion is necessary to respect their beliefs with regards to activities, food and holidays.

Consent is different though, this should be used sparingly as consent can be removed as quickly as given and requires a significant amount of transparency on what you are requiring and why, as well as an ability to provide evidence that consent has been given in the first place.

Situations where consent may be required could be as follows, these are purely examples to highlight the point:

- An event facility requests the parents contact details to advertise their facility.
- The Scout Group would like to send parents details on a local fund-raising event.

In these cases, if you feel the activity warrants consent then this should be clearly presented to the person consenting at the point at which you gather their personal data, or as a separate form for completion, in both cases you need to consider the following, this is known as a privacy notice:

- Is the reason I want the consent, justified?
- Is the consent notice (privacy notice) clear and transparent as to the justification above?
- Do I give clear opt-in check boxes for ticking?
- Can I store the evidence of consent once I have gained it?
- Can I easily remove the consent if requested to do so?

Further guidance on privacy notices is available here: https://ico.org.uk/for-organisations/guide-to-data-protection/privacy-notices-transparency-and-control/privacy-notices-under-the-eu-general-data-protection-regulation/.

In addition, TSA are adding privacy notices to the most commonly used example forms that will be available from the TSA website.

In most cases consent is being asked for from the parent responsible for the Young Person. This is also true when gaining consent for nights away from the parents however this is consent for the attendance of the Young Person and not the on-going use of their data, this is very different.

Where consent is required by a data subject under the age of 18, parental consent must be obtained and cannot be provided by the young person.

As part of local Scouting, photography is common place to record events and publicise activities. As a photograph is considered Personal Data and isn't really justified via another lawful basis, consent

should be used, especially if the photograph is publicised with the individuals name. This consent should be captured at the time the data is collected, such as the attendance form for the event.

Further guidance on consent is available here: https://ico.org.uk/about-the-ico/ico-and-stakeholder-consultations/gdpr-consent-guidance/.