5th Dorking (URC) Scout Group
Data Protection

Adopted by the Group Executive Committee on: 9th July 2015

The Data Protection Act 1998 governs the collection, recording, storage, use and disclosure of personal data, whether such data is held electronically or in manual form. Young people have the same rights as adults under the Act, and the impact on Scouting is addressed below.
This is a general overview of the main ways in which data protection may be relevant to scouting. It is not intended as a detailed account and more information can be found from the Information Commission Office (ICO) the independent governmental authority responsible for overseeing and regulating data protection. Further explanation/assistance can also be obtained by contacting the Legal Service Department at The Scout Association (TSA) Headquarters.

Contents:

1. What is data protection?

Data protection aims to protect an individual's rights to privacy by regulating how organisations obtain, store and use their personal data. So, data protection rules provide individuals with certain rights whilst also imposing certain duties and obligations on organisations. Young people and adults have the same data protection rights under the law.

a) The Law and regulation

Data protection is governed by the Data Protection Act 1998 ("DPA") which is overseen and regulated by the ICO. Amongst other matters, the ICO:
i) keeps a central record of those organisations that are formally registered with it;
ii) provides further Guidance regarding particular issues e.g. marketing, fundraising etc. Interpretations and summaries of the law as well as downloadable which can all be found on the ICO websitewww.ico.gov.uk; and
iii) enforces the law through fines and prosecutions where applicable

b) What records are subject to data protection?

The rules apply particularly to computer or automated records (including email) but also apply to manual records kept in such a way that specific information about a particular individual can easily be retrieved e.g. manual records filed by the name or role etc.
Examples of automated records include:

- Computer files- files stored on hard file or USB memory sticks, CD Roms, DVD's, hard disks, back-up files
- Audio/Video-CCTV, webcam images,
- Digitalised images- scanned photos, digital camera

Examples of manual records include:

- Files – on employees, volunteers, young people
- Index systems – names, addresses, other details
- Microfiche records- containing personal data

A mere passing reference to an individual is not necessarily classed as personal data e.g. the Minutes of a meeting will not be considered personal data about those attending in general. However, if an individual was specifically discussed and is identifiable from such discussion in the Minutes, then the Minutes will be 'personal data' about that individual.

2. What is personal data?

This is any information held about a living individual who can be identified from the information itself or other information also held. Names, addresses or specific roles are obvious ways of identifying individuals but they can also be identified in photos or CCTV images.
There are special rules applying to 'Sensitive Personal Data' where extra care must be taken when handling or disclosing it to third parties. (See further under Part II)

Sensitive personal data

Personal data becomes 'sensitive' if it includes information about:
a) Racial or ethnic origin;
b) Political opinions;

c) Religious beliefs;
d) Trade union membership;
e) Physical or mental health; or
f) Sexual life;
g) Commission of offences or alleged offences.

3. What are the rules?

The law states that when processing any personal data the Data Controller must apply 8 basic 'Data Protection Principles'.

a) What is 'Processing'?

Processing has a wide meaning and includes all aspects of handling personal data e.g. from obtaining, recording, retaining (incl. editing and revising it), storing, sharing it to archiving and destroying it.

b) What is a Data Controller?

A Data Controller can be either individuals, organisations or other incorporated or unincorporated bodies of persons who determine what personal data is held, why it is held and how it is processed
Data Controllers are responsible for ensuring compliance with data protection. An organisation can also designate a Data Protection Officer ("DPO") to ensure compliance on its behalf but the Data Controller remains ultimately responsible.
The DPA also refers to a data processor who processes personal data on behalf of the data controller e.g. usually an external company or business. Although Scout units are unlikely to use a data processor, however, if and when they do it is important to ensure a proper agreement is in place specifying the Data Controller's instructions and that the processing complies with the DPA. This is because the Data Controller remains ultimately responsible for what the data processer does with the data.

c) What are the 8 basic principles?

The 8 basic principles address fairness, lawfulness, relevance, excessiveness, accuracy, up-to-datedness and security. Thus, when processing personal data, the Data Controller must ensure that the data is:

- Processed fairly and lawfully;
- Obtained for a specified and lawful purpose;
- Adequate, relevant and not excessive for purpose;
- Accurate and up-to-date;
- Kept only for as long as required;
- Processed in accordance with the data subjects rights;
- Be kept secure proportionately to the level of harm that could result if unauthorised access occurs;
- Not transmitted outside the European Economic Area (EEA) without consent from the data subject.

For a more detailed explanation of these principles please see the ICO website

4. How does data protection apply to Scouting?

4.1 Does data protection apply to our Scout Groups?

Data protection law applies in full to all Scout Units as it does to any form of organisation including public authorities, companies, businesses and other charities. Scout Units are created and operate as independent charities and are likely to collect and store personal data about members and, in many cases, other individuals involved with the unit. Scout Units must adhere to the DPA when using the Association's Membership System "Compass". Please see POR, Chapter 14
The rules do not apply to individuals collecting information solely for their domestic and household affairs e.g. address book or solely for research, journalistic, artistic or literary purposes

a) Does our Scout Group have to register with the ICO?

As smaller 'not-for-profit' organisations, Scout Units do not have to register provided they do not hold personal data about anyone other than members or potential beneficiaries. However, they are still subject to the rules of the DPA. As a larger organisation, TSA Headquarters is registered as a Data Controller with the ICO.

b) Who within our Scout Group is responsible for Data Protection?

Each Scout Unit is a Data Controller and, therefore, overall responsibility for compliance with data protection will lie with the Executive Committees of each Unit who, as the Managing/ Charity Trustees, are jointly responsible for all the affairs of the Unit.

c) How does data protection usually arise within a Scout Group?

As Scout Units are subject to data protection rules in full, the issue could arise in many different ways. However, it usually arises in two main ways which are:

(i) How personal data must be "processed" in general; and
(ii) When individuals make a "Subject Access Request" ("SAR") i.e. a request for disclosure of all their personal data.
These two areas are explained further.

4.2. How personal data must be processed

Our Scout Group must apply the 8 basic Data Protection Principles when processing Personal Data and the following are some basic essentials to be applied:

(a) When obtaining personal data

- have legitimate grounds for collecting and using it in the first place
- be transparent about the purpose for which it is collected and who it will or may be shared with by providing privacy notices when collecting it
- ensure you have consent from the individual. For many immediate purposes, consent can be implied as the individual will know why they are providing it. However, you need to explain what else you might use the information
- ensure that the source is clear

(b) When retaining personal data

- only hold and retain data sufficient for the intended purpose
- take reasonable steps to ensure accuracy as to facts and consider any challenges to this (personal data is not 'inaccurate' if it faithfully represents someone's opinion. In these circumstances, if challenged, the data would not have to be 'corrected' but a note added to it recording that the data subject disagrees)
- update, edit and revise it regularly in accordance with the purpose it was collected e.g. changes to names, addresses, contact details, medical needs etc
- review how long it should be retained in accordance with the purpose it was collected
- give individuals access to their personal data

(c) When storing personal data

- ensure secure system policies of storage, including encryption where necessary, and access in order to prevent accidental loss, alteration or breaches of security
- be clear about who is responsible for ensuring information security
- swiftly and effectively respond to any breach of security including reporting this to the ICO.

(d) When sharing personal data

- Personal data must always be processed fairly, handled for intended purpose and only in ways that an individual would reasonably expect. This means that a data controller should not share personal data without legitimate reason.
- Sharing personal data within scouting.

- It is reasonable for members to expect their data to be shared within their particular sections for practical, legitimate purpose and on a need-to-know basis.
- Email communication - Please note that extra care should be taken when using email which, once sent, can easily be shared beyond your control. Therefore, you should always consider the contents of email communications carefully to ensure that if they contain personal data, especially of a confidential or sensitive nature (whether your own or another's), they are sent with caution and to only those who will safeguard that personal data and not share it with anyone without legitimate reasons. It is good practice to make your intentions clear in the email itself and, where necessary, mark clearly as 'Strictly Confidential' or 'Sensitive' or 'Intended for recipient/s only and not to be shared' etc.
- Sensitive personal data - You must also ensure that extra special care is taken with this which, as highlighted earlier, requires explicit consent of the individual for you to obtain it and therefore whether such consent has been obtained from the subject should be checked e.g. through the AA Form or directly from the subject by some other means.

(e) When deleting, destroying or archiving personal data

- delete or destroy when no longer required securely
- archive securely where retention is justified

(f) What are the special rules for processing 'sensitive personal data'?

- All the above rules are also applicable when processing sensitive personal data but an additional rule applies to sensitive personal data which may only be held with the explicit consent of the data subject i.e. where sensitive personal data is to be processed, you must ensure that individuals have given explicit consent for this to happen. The DPA does not define the method of obtaining explicit consent, however, the best method is to obtain such consent in writing requiring the individual to

e.g. tick a box or sign a declaration etc, agreeing that their sensitive personal data may be processed.

- In order to ensure consistency the Association's Membership System "Compass" requires users to confirm that permission has been given to hold the information. This confirmation is given via a pop-up box within Compass itself.

4.3 Data controllers must not:

use personal data in ways which have an unjustifiable adverse effect on the individual;
transfer personal data to a country or territory outside the European Economic Area (EEA) unless first ensuring that country or territory also ensures a like level of protection for the processing of personal data

5. How to deal with subject access requests (SARs)

(a) What is a SAR?

One of the main rights which the Data Protection Act gives to individuals is the right to access their personal information. An individual can make a request in writing to an organisation for a copy of any personal information held about them. This is known as a Subject Access Request (SAR).
Following a request, a data subject is entitled to a copy of personal data being held or being processed about them (with only a few exemptions possible). The data controller may charge a standard fee to the data subject (a maximum of £10) As the Association is a charitable organisation, in order to cover some of its administrative costs, Headquarters charges £10 for providing an SAR. It is recommended that scout units, which all also operate as charities, also charge the £10 fee in order to assist towards their administrative costs.
You must comply with the SAR within 40 calendar days of receiving the said cheque. Remember the 40 days starts ticking on receipt of the cheque (and not when it is cleared by the bank)

(b) What can the Subject do following receipt of their personal data?

Subjects can:

- ask to have inaccurate data rectified, erased or destroyed
- ask that data be stopped from being processed if it is unnecessary or causing unjustified damage or distress.
- ask the ICO whether the Act has been contravened.
- If necessary, apply to court to exercise their rights and may receive compensation if damages are suffered due to any contravention of the Act.

For a more detailed account check out 'how to respond to Subject Access Requests' and also the ICO website.

5th Dorking (URC) Scout Group – How we meet our obligations

1. The group is obliged to appoint a data controller.
2. The Group Executive has formally minuted the appointment of **Rob Jones** to the position. A change must be shown the Group Executive Meeting minutes.
3. The group is obliged to store/ maintain records that are relevant, necessary, transparent (for use) and secure etc. The group executive are satisfied that it meets these obligations by:
    a. Appointing a Data Controller that has oversight on all process involving data security.
    b. Collecting information transparently via application forms etc where the purpose is clearly relevant (ie no covert data collection).
    c. Stores records securely only within approved systems (Group level – Online Scout Manager (OSM), and not on personal laptops etc, Compass for the Scout Association).
    d. Controls access to personal records by:
        i. a "scheme of access": passwords issued to named individuals, generic access accounts are not used;
        ii. access rights issued only to those individual who have a valid need and:
            1. either a warrant holder, or
            2. an appropriate level of training that is recognised by the Scout Association/Group.
    e. Data kept on approved systems is reviewed at least annually and personal records older that two years are removed/ deleted.
    f. Personal data will not be released to third parties without written consent. (For the avoidance of doubt, and as far as there may be a valid need, the Scout Association and other Scout groups are not seen as a third parties).