Scouts

1st Ince and Elton

Data Protection and IT Security Policy

Ref number:	1STIEGP12	Date of issue:	12/06/2018	Prepared by:	Ashley Proctor
Page:	Page 1 of 8	Revision number:	002	Approved by:	Group Exec Committee

Data Protection and IT Security Policy

This Data Protection and IT Security policy applies to all operations of 1st Ince and Elton Scout Group.

The policy is designed to ensure that 1st Ince and Elton Scout Group complies with its obligations under the Data Protection Act/General Data Protection Regulation (GDPR), and conforms to the following eight data protection principles:

1. Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless:
    a. at least one of the conditions in Schedule 2 is met, and
    b. in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met.
2. Personal data shall be obtained only for one or more specified and lawful purposes and shall not be further processed in any manner incompatible with that purpose or those purposes.
3. Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.
4. Personal data shall be accurate and, where necessary, kept up to date.
5. Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.
6. Personal data shall be processed in accordance with the rights of data subjects under the Act.
7. Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.
8. Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

The personal data we hold

Data description	Personal data included	Stored using	Retention policy	Responsible officer
Information about our members	Contact information, badge records, activity records	Online Scout Manager	Retained whilst a current member. A subset of data is retained	Section Leader
	(Includes sensitive data, as defined)	by UK Scout Association	2 years after membership ceases to support continuity should the person reapply for membership	
Information about Safeguarding incidents	Contact information and information regarding the nature of any allegation, the status and outcome of the investigation	Paper, County Email and Electronic Files	Indefinitely	Group Scout Leader
Information about accidents and near misses	Contact details and nature of accident		3 years after end of investigation	Group Scout Leader
Information about our event attendees	Contact details, next of kin information, medical conditions and special diets. *(Includes sensitive data, as defined)*	Paper forms (which may also be stored in Online Scout Manager)	Destroyed after event, unless medical incident and then kept for 3 years.	Event Leader
Information about general enquirers	Contact information and nature of enquiry, which may contain personal data	Email System	Indefinitely	Group Scout Leader or Group Secretary
Information about complainants	Contact information and nature of complaint, which may contain personal data	Email System	Indefinitely	Group Scout Leader or Group Secretary

Information about people registered for our website	Contact Information	Wordpress, Invision Community (Forums)	Indefinitely, unless the individual requests removal	Website Manager
Information about people registered to our mailing lists	Contact information	Mailchimp (3rd party system)	Indefinitely, unless the individual requests removal	Website Manager
Bank details of our members family members and our suppliers	sort-code and account number	Not stored, other than by 3rd party merchant (e.g. Bank or Paypal)	Merchant's policy	

For completeness, we also hold the following information which is not categorised as Personal Data but has the following retention policies applied:

Data description	**Retention policy**	**Responsible officer**
Finance – purchase ledgers, record of payments made, invoices, bank paying in counterfoils, bank statements, remittance advices, correspondence regarding donations, bank reconciliation.	7 years	Group Treasurer
Finance – Receipt cash book and sales ledger	10 years	Group Treasurer
Finance - Fixed assets register	Indefinitely	Group Treasurer Group Quartermaster
Finance – Deed of covenant/Gift aid declaration and legacies	6 years after last payment made	Group Treasurer
Buildings – Deeds of title	Indefinitely	Group Secretary
Buildings – Leases	15 years after expiry	Group Secretary
Buildings – Documentation regarding plant and machinery	Until 1 year after disposal	Group Secretary
Buildings – records of major refurbishments, warranties, planning consent, health & safety files.	13 years after completion of project	Group Secretary
Trustee's minutes	Indefinitely	Group Secretary
Annual accounts and annual reports	Indefinitely	Group Secretary

Investment and insurance policy records	7 years after disposal	Group Treasurer
Insurance policies	Indefinitely	Group Secretary
Employer's Liability insurance certificate	40 years	Group Secretary
Health and safety records	3 years	Group Secretary
Contract with customers, suppliers or agents, licensing agreements, rental/ hire purchase agreements, indemnities and guarantees and other agreements or contracts	6 years after expiry or termination	Group Secretary

Our Security Policies

The following security policies will apply to the storing of personal data as outlined in this policy. These security policies are mandatory.

Overarching policies

- **Need to know** – We only give people access to the data that they need to carry out their role. If people change roles, we review access accordingly.
- **Passwords** – We use systems that force complex password complexity. Change regularly or set once and keep until you think the password has been compromised.
- **Commercially available software** – where possible we use third party software to store personal data (either installed on our IT network or provided as software-as-a-service), where the software is regularly testing and patched for security vulnerabilities.
- **Volunteers** – We ensure our volunteers are made aware of their data protection obligations.
- **Transporting data** – We only transport data using physical media if absolutely necessary and then using encrypted media only.
- **Education** – We will run a regular awareness session for volunteers about their obligations under this policy and general IT Security awareness.
- **We keep people informed** – we tell people why we are collecting their data and how we use it, at the point in time we collect it.

Physical storage

- **Limiting storage** – We limit the amount of personal data we physical store to the absolute minimum. Only those with a need to know will have access to the data.
- **Locked** – Physical documents with personal data will be store in a locked cabinet. This is located in the Scout HQ.

Volunteer equipment

- **Virus –** A virus scanning service must be installed on all devices and regularly checked.
- **Encryption** – All devices are disk encrypted with disk encryption (by default, most mobile devices running iOS or Android will automatically encrypt if a passcode has been set on the device). If a device is not encrypted, then it should not be used to download personal data under any circumstances.
- **Removable storage –** Removal devices that will contain personal data should be encrypted using Bitlocker or similar encryption.

Volunteer emails

- **Restriction** - Our volunteers should use the Scout Groups 'official' email addresses (ending in @1stinceandelton.org.uk) as their primary method for receiving, storing and sending of Scouting related emails, and always when they are transmitting personal data.
- **Virus, Malware and Phishing protection** – All emails will be scanned for virus, malware and phishing.
- **IT security -** We rely upon the IT security provisions of our preferred cloud platform which provide an adequate level of security for our needs.

Third parties

- **Third party processing** – Other than the Scout Association (Compass) and Online Youth Manager Ltd (Online Scout Manager), we limit the use of third parties to process personal data collected by 1st Ince and Elton Scout Group and only do so where we have the express permission of the Group Executive Committee.
- **Third party compliance** – We ensure third parties we contract with to store personal data comply with the principles of this policy, have an information security policy in place and ideally hold an information security standard (such as ISO 27001).
- **Limiting exports** – When exporting data from third party systems (e.g. Compass, Online Scout Manager), we only export the data we need for the purpose we need it for.

Consent

Where we do not have a lawful basis to hold or process data, we will seek the express consent of individuals to hold data about them. This will be by specific and unambiguous statements that must be opted-into on any forms (electronic or otherwise) and systems. In some circumstances due to the organisation of the Scouts, we ask our members to ensure they have express consent for the data they are submitting to us.

For example:

"I consent to my name, date of birth, t-shirt size and information about my special diet to be used for the purposes of administering the event by ensuring that the correct security wristband is assigned, t-shirt ordered and meal options provided. We will not use this data for any other purpose than this event, except in aggregate to provide statistics for historical reference. We will delete this data one year after the event ends."

Data Subject Access Requests

Should a member of 1st Ince and Elton Scout Group or a member of the public request a copy of any personal information which 1st Ince and Elton Scout Group holds, then the following process should be followed:

- The individual should write to our Data Protection Lead (dataprotection@1stinceandelton.org.uk) outlining the personal data they are seeking to obtain.
- Our Data Protection Lead will acknowledge the request by email.
- Our Data Protection Lead will seek to verify the identity of the individual and that they are lawfully entitled to request a copy of the personal data. This may involve asking for information such as a membership number, date of birth, address, or documentary evidence.
- Our Data Protection Lead will collate the data requested, noting that we cannot provide data held by other organisations such as the Scout Association, Online Scout Manager, the Scout District. The data should be carefully analysed to ensure it does not refer to any other individuals, in which case it should be redacted.
- Within 30 days of the receiving the request, our Data Protection Lead will provide the data to the individual. This will normally be by email.
- There will be an administration charge of / There will be nocharge.

For more information about our legal obligations, refer to the ICO website.

Right to erasure (Right to be forgotten)

Should a member of 1st Ince and Elton Scout Group or a member of the public wish for their personal information to be erased, then the following process should be followed:

- The individual should write to our Data Protection Lead (dataprotection@1stinceandelton.org.uk) outlining the personal data they are seeking to erase.
- Our Data Protection Lead will consult the Group Chair and Group Scout Leader to decide as to whether the request should be processed. Guidance from the ICO should be followed. Whilst 1st Ince and Elton Scout Group will not seek to refuse the request unreasonably, it has several

statutory obligations to comply with and uses personal data as part of its vetting and safeguarding procedures.

- If it is deemed that the data shall be deleted, then our Data Protection Lead will confirm to the individual the timescales involved and instruct the necessary responsible officer to delete it.

Correcting inaccurate personal data

Should a member of 1st Ince and Elton Scout Group or a member of the public believe that information that we hold about them is inaccurate, they should write to our Data Protection Lead (dataprotection@1stinceandelton.org.uk) outlining the inaccuracy. Our Data Protection Lead and/or The Group Secretary will then seek to correct the data and confirm back to the individual.

Reporting a breach

A breach is defined as any event which "leads to the destruction, loss, alteration, unauthorised disclosure of, or access to, personal data". If a breach occurs, our Data Protection Lead will be immediately informed (dataprotection@1stinceandelton.org.uk).

Our Data Protection Lead (in consultation with the Group Chair and Group Scout Leader) will need to consider if the breach is likely to "result in discrimination, damage to reputation, financial loss, loss of confidentiality or any other significant economic or social disadvantage". If it does, the ICO should be informed within 72 hours of the breach occurring.

If the breach results in a high risk to the rights of the individuals involved, they should also be informed directly.

Group Website

The Group shares a summary about the data it holds and how it processes it on its website at (www.1stinceandelton.org.uk). The website also provides information on how to submit a data subject access request and right to be forgotten request.