Scouts

1st Ince and Elton

Data Protection and Security Policy

Ref number:	1STIEGP06	Date of issue:	08/06/2025	Prepared by:	Ashley Proctor
Page:	Page 1 of 16	Revision number:	4.2	Approved by:	Group Trustee Board

Data Protection and Security Policy

1. Purpose

This policy sets out how the Group collects, uses, stores, and protects personal data in line with the General Data Protection Regulation (GDPR), Data Protection Act 2018, and relevant Scout Association policies.

2. Scope

This policy applies to all members, leaders, volunteers, and anyone handling personal data on behalf of the Group, including digital systems, paper records, CCTV, and online platforms.

3. Key Principles

We commit to upholding the following data protection principles:

- Lawfulness, fairness, and transparency
- Purpose limitation
- Data minimisation
- Accuracy
- Storage limitation
- Integrity and confidentiality
- Accountability

4. Types of Data We Hold

We process the following categories of data:

- Member contact details, medical and dietary needs
- Attendance, activity records, and badge progress
- Emergency contact and safeguarding data
- Financial records, donations, and Gift Aid
- Website registrations and communication mailing lists

5. Data Storage and Retention

Data is stored securely using:

- Online Scout Manager (OSM) for youth records
- Scout Association systems (e.g. My Membership) for adult volunteers
- Secure digital storage (SharePoint, encrypted devices)

- Paper records (locked cabinets in HQ)

Retention periods vary based on data type:

- Youth records: 2 years post-membership
- Safeguarding: Indefinitely
- Financial: 7–10 years
- Event forms: Destroyed after event unless incident occurs
- Insurance & H&S: Varies by statutory guidance

6. IT and Email Security

- Devices used for Group purposes must be running a supported Operating System, have latest security updates and patches install, have functioning and up to date antivirus protection and preferably disk encryption (especially if saving personal data locally).
- Passwords must be strong and changed if you suspect that it's been breached.
- Personal data must not be stored on unencrypted USBs or personal cloud accounts.
- Group emails should use official addresses (e.g. @1stinceandelton.org.uk).

7. Website and Cookies

Our website (1stinceandelton.org.uk):

- Collects anonymised usage data via Google Analytics
- Uses cookies to support functionality and user experience
- Hosts forums and shop services that require user registration
- Does not share data with third parties without consent

A public privacy notice and cookie policy is available on the website.

8. CCTV

CCTV is used at HQ for safety and security. It:

- Covers entry/exit points and communal areas only.
- Does not record sound or cover private areas (e.g. toilets).
- Is monitored only by authorised personnel.
- Records are retained for up to 14 days and then overwritten.
- Requests for access must be made via dataprotection@1stinceandelton.org.uk.

9. Data Subject Rights

Individuals may:

- Request access to data held about them (Subject Access Request)
- Request correction or erasure of data
- Object to or restrict processing

All requests should be made in writing to dataprotection@1stinceandelton.org.uk.

10. Breach Notification

In the event of a data breach:

- The Data Protection Lead must be informed immediately
- The Group will assess the risk and notify the ICO if required within 72 hours
- Affected individuals will be informed where there is a high risk to their rights

11. Volunteer Responsibilities

All adults must:

- Complete data protection awareness training (annually or as needed)
- Handle personal data responsibly and only share it on a need-to-know basis
- Store documents securely and report any concerns without delay

12. Review

This policy will be reviewed every three years or sooner if required.

13. Appendix

Here you'll find copies of supplementary documents that expand the detail of a number of points in this document.

- Data Privacy Notice
- CCTV Policy

Data Protection and Security Policy

Data Privacy Notice

Our Privacy and Fair Processing Notice describes the categories of personal data we process and for what purposes. We are committed to collecting and using such data fairly and in accordance with the requirements of the General Data Protection Regulations (GDPR).

Who are we?

Our Scout Group, 1st Ince and Elton, is a youth charity. Our mission is to actively engage and support young people in their personal development, empowering them to make a positive contribution to society. We are incorporated by royal charter and are regulated as a member of the UK The Scout Association, (see www.scouts.org.uk for more information.).

Every year we hold an annual general meeting where members of the group trustee board, are elected, any parent of a youth member can decide to be in the trustee board at the AGM and every parent has the right to attend the Annual General Meeting.

We are based at **1st Ince and Elton Scout HQ, School Lane, Elton, Chester, CH2 4LT**.

Our Group Trustee Board is the data controller for the information we collect from you. Any personal data that we collect will only be in relation to the work we do with our members and through our relationship with supporters, donors and funders.

Your personal data – what is it?

Personal data relates to a living individual who can be identified from that data. Identification can be by the information alone or in conjunction with any other information in our Scout Group's (the data controller's), possession or likely to come into such possession. The processing of personal data is governed by the General Data Protection Regulation (the "GDPR").

How we gather personal information

The majority of the personal information we hold, is provided to us directly by yourself or by parents/legal guardian in either paper form or via our online membership systems, in the case of an adult member, data may also be provided by third party reference agencies, such as the Disclosure and Barring Service (DBS).

Where a member is under the age of 18, this information will only be obtained from a parent/guardian and cannot be provided by the young person.

How do we process your personal data?

Data Protection and Security Policy

We comply with our obligations under the "GDPR" by keeping personal data up to date; by storing and destroying it securely; by not collecting or retaining excessive amounts of data; by protecting personal data from loss, misuse, unauthorised access and disclosure and by ensuring that appropriate technical measures are in place to protect personal data.

We process the data to have the ability to contact the member, parents and guardians, to inform them of meetings, events that the group itself may be running or attending.

We use personal data for the following purposes: -

- we collect personal and medical information for the protection of that person whilst in the care of the Scout Group
- we collect religious data to respect a person's beliefs with regards to activities, food and holidays
- To enable us to provide a voluntary service for the benefit of the public in a particular geographical area as specified in our constitution
- To administer membership records
- To fundraise and promote the interests of the Scout Group
- To manage our volunteers
- To maintain our own accounts and records (including the processing of gift aid applications);
- To inform you of news, events, activities and services running at 1st Ince and Elton Scout Group.

What is the legal basis for processing your/your child(ren)'s personal data?

We only use your personal information where that is permitted by the laws that protect your privacy rights. We only use personal information where:

a) We need to use the information to comply with our legal obligations
b) We need to use the information to contact with you, regarding meetings, events, collection of membership fee's etc, (i.e. for the day to day running of the group)
c) it is fair to use the personal information in your interests, where there is no disadvantage to you – this can include where it is in our interests to contact you about products or services within scouting.
d) The processing is necessary for the persons legitimate interests or the legitimate interests of our Scout Group unless there is a good reason to protect the individual's personal data which overrides those legitimate interests.

How we store personal data

We are committed to the protection of your personal information.

We generally store personal information in one of two secure digital online database systems, where access to that data is restricted and controlled.

My Membership: - is the online membership system of The Scout Association, this system is used for the collection and storage of Adult personal data.

Online Scout Manager is an online membership system run by Online Youth Manager Ltd, this is a secure membership database where we store the personal information of Adults and Youth members for the day to day running of the group.

Printed records and Event data

Paper is still used within the sections to capture and retain some data for example the following: -

- New joiners form.
- New joiners waiting lists.
- Health and contact records update forms.
- Gift Aid Collection forms.
- Events consent from parents.
- Events coordination with event organisers.
- Award notifications/nominations

In the case of Joining forms, Health and contact update forms, this information is securely held by the leader and transferred to our secure digital systems as soon as possible before the paper form is destroyed.

Gift Aid collection forms, will be securely held by the Groups Treasurer to aid in the collection of Gift Aid for monthly membership fees, we have a legal obligation to retain this information for 7 years after our last claim.

Events

As a member of 1st Ince and Elton Scout Group it is hoped you will take up the opportunity to attend events and camps, where is necessary to fulfil our legal obligations we will be required to potentially have a less secure means to access personal information, such as printouts of personal contacts and medical information, (including specific event contact forms), rather than relying on secure digital systems, as often the events are held where internet and digital access will not be available. We will minimise the use of paper to only what is required for the event/camp.

We will ensure:

a) Transfer of paper is secure, such as physical hand to hand transfer or registered post.
b) Paper forms are securely destroyed after use.
c) Secure destruction will be through a shredding machine or securely burned.
d) Always keeping the paper records secure, especially when in transit.

e) If transferred to somebody, we will audit that they return them when the event is complete.

Awards

Sometimes we may nominate a member for national award, (such as Chief Scout Awards or Duke of Edinburgh award), such nominations would require we provide contact details to the awarding organisation, this is most often done online or sometimes on paper via registered post.

CCTV

We use captured CCTV footage and images at our Scout HQ so that we can perform our duty protecting both our visitor's and our property. We may use the footage to support third-party organisations such as The Police, Solicitors and Insurance companies who may request data in support of Criminal or Civil action. All footage is either stored on a password protected recorder in a locked cabinet or on our secure cloud storage on Microsoft 365.

Photography

The law on image use and GDPR needs further clarification, the position of the 1st Ince and Elton Scout Group is:

Photographs/images (which can be classed as personal information) of you or your child(ren) may be taken during activities and be used within a Scouting context and publicity material, for example, Scouting publications and the media. Images may be published to official Scout websites and scouting affiliated social media and our public display boards in our Scout HQ (but will never identify individuals in line with Scout Association guidelines). We ask for consent to take such photographs and are diligent in avoiding taking photographs of any individual where the consent of a parent/guardian has not been given.

Under GDPR, storing data by consent is only permitted if people can easily and effectively withdraw consent. If we publish a photograph or image in any public forum (such as a website or social media) we no longer have control over that photograph in so far as it can be downloaded and reproduced elsewhere (without our knowledge), so a withdrawal of consent once a picture has been published cannot be effective.

In the event that consent for photographs to be taken is withdrawn, the Group will undertake to publish further no photographs of the youth members concerned and will delete any images already taken from any sites and social media over which it has control. It may not be possible to remove all images and photographs from the historical record online or elsewhere.

Please note that as many Scouting events happen in the open air and in publicly accessible spaces, it is not possible to guarantee that photographs are not taken by people unconnected with the group.

Data Protection and Security Policy

1st Ince and Elton Scout Group may store an image of youth members and/or their parents/guardians on the Online Scout Manager (OSM) membership database as part of the personal information stored there.

Sharing and transferring personal Information

We will only normally share personal information within our Scout Group leaders and trustee members.

However, there may be occasions where we may need to share your information with others outside our Scout Group in order to meet or enforce a legal obligation, this may include – Mersey Weaver District Scouts, Cheshire Scout County (known as Cheshire Scouts), The Scout Association and its insurance subsidiary "Unity", local authority service and law enforcement. In these instances, we will only share your personal information to the extent needed for those purpose and where there is a legitimate reason to do so.

If you move from 1st Ince and Elton Scout Group, to another Scout Group or Explorer Scout Unit we will ask you before we transfer your personal information to them.

We will never sell your personal information to any third party for the purposes of marketing.

Your personal data will be treated as strictly confidential. We will take steps to anonymise the data we provide (i.e. collective reporting on gender, ethnicity, age, etc.). If identifiable data is to be shared we will seek your consent.

Third Party Data Processors

1st Ince and Elton Scout Group, employs the services of the following third-party data processors: -

- The Scout Association via its adult membership system "My Learning" which is used to record the personal information of leaders, adults and parents who have undergone a Disclosure and Barring Service (DBS) check.
- Atlantic Data which is the vendor that The Scout Association uses to handle requesting of Disclosure and Barring Service (DBS) checks.
- Online Youth Manager Ltd (Online Scout Manager) which is used to record the personal information, badge records, event and attendance records etc, we have a data processing agreement in place with online youth manager, more information is available at https://www.onlinescoutmanager.co.uk/security.php
- Microsoft occasionally used for secure transfer of limited personal information for events via the Microsoft 365 platform.

Automated decision making

1st Ince and Elton Scout Group does not have any automated decision-making systems.

Transfers outside the UK

1st Ince and Elton Scout Group will not transfer your personal information outside of the UK, with the exception where an Event is taking place outside of the UK and it is necessary to provide personal information to comply with our legal obligations, although generally such an event will have its own data collection form which will be securely held and disposed of after the event.

How do we protect personal data?

We take appropriate measures to ensure that the information discussed to us is kept secure, accurate and up to date and kept only for as long as necessary for the purpose for which it is used.

How long do we keep your personal data?

We will retain your personal information, throughout the time you/your child(ren) are a member of 1st Ince and Elton Scout Group.

When you/your child(ren) leave 1st Ince and Elton Scout Group, we will retain your information for a period of up to two years from the date you left the group, however this will be in a limited form (Initials, badge and attendance records) and is only held to help us fulfil our legal obligations for insurance and legal claims.

We will also keep any Gift Aid Claim information for the statutory 7 years as required by HMRC (which may be beyond age 21)

Your rights and your personal data

You have the right to object to how we process your personal information. You also have the right to access, correct, sometimes delete and restrict the personal information we use. In addition, you have a right to complain to us and to the data protection regulator.

Unless subject to an exemption under the GDPR, you have the following rights with respect to your personal data: -

- **The right to be informed** – you have a right to know how your data will be used by our Scout Group.
- **The right to access your personal data** – you can ask us to share with you the data they have about you!
- **The right to rectification** – this just means you can update your data if it's inaccurate or if something is missing. You can view and edit your personal information directly on our online membership systems Online Scout Manager and Compass.

- **The right to erasure** – this means that you have the right to request that we delete any personal data they have about you. There are some exceptions, for example, some information can be held for legal reasons.
- **The right to restrict processing** – if you think there's something wrong with the data being held about you, or you aren't sure if we are complying to rules, you can restrict any further use of your data until the problem is resolved.
- **The right to data portability** – this means that if you ask us we will have to share your data with you in a way that can be read digitally – such as a pdf. This makes it easier to share information with others.
- **The right to object** – you can object to the ways your data is being used. This should make it easier to avoid unwanted marketing communications and spam from third parties.
- **Rights in relation to automated decision making and profiling** – this protects you in cases where decision are being made about you based entirely on automated processes rather than a human input.

Please contact your child(ren)'s leader, our Group Lead Volunteer or our Data Protection Lead for more information, in the first instance.

Whether or not you exercise your rights is up to you – the main thing to remember is that they're there if you need them.

Further processing

If we wish to use your personal data for a new purpose, not covered by this Data Protection Notice, then we will provide you with a new notice explaining this new use prior to commencing the processing and setting out the relevant purposes and processing conditions. Where and whenever necessary, we will seek your prior consent to the new processing.

Contact Details

To exercise all relevant rights, queries of complaints please in the first instance contact our Data Protection Lead at 1st Ince and Elton Scout Group, 28 Lime Grove, Elton, Chester, CH2 4PX or email dataprotection@1stinceandelton.org.uk.

You can contact the Information Commissioners Office on 0303 123 1113 or via email https://ico.org.uk/global/contact-us/email/ or at the Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire. SK9 5AF.

CCTV Policy

Introduction

Data Protection and Security Policy

1st Ince and Elton Scout Group has installed a closed-circuit television (CCTV) system at its HQ building (the system) to provide a safe and secure environment for the young people, adult volunteers, visitors and to protect the Group's property.

This document sets out the accepted use and management of the CCTV system and the images captured to ensure the Group complies with the General Data Protection Regulation (GDPR), the Data Protection Act (DPA) 2018, the Human Rights Act 1998 (HRA), the Surveillance Camera Code of Practice issued under the (POFA Code) and other relevant legislation.

Purpose

The Group has installed a CCTV system covering the HQ building.

The purposes of the Group using CCTV systems include:

- To assist in the prevention or detection of crime or equivalent malpractice.
- To assist in the identification and prosecution of offenders.
- To monitor the security of the Group's premises.
- To ensure that health and safety rules and procedures are being complied with.
- To assist with the identification of unauthorized actions or unsafe working practices that might result in disciplinary proceedings being instituted against volunteers and to assist in providing relevant evidence.

The system will be provided and operated in a way that is consistent with an individual's right to privacy.

The system will not be used to provide images to the world-wide web for entertainment purposes, record sound or disclose to third parties (unless disclosed to the police or other legally authorised body in response to any criminal activity discovered).

Covert recording, or automated recognition (e.g., ANPR) will not take place. Duties to comply with the requirements of DPA rest with the Responsible Person. This term is defined in the FSO and might apply to one or more people depending upon the nature of the issue concerned. Any employer will be a Responsible Person.

Scope and Applicability

Responsibilities

The CCTV system is owned and operated by 1st Ince and Elton Scout Group.

Authority for use of the CCTV and responsibility for CCTV use lies with the charity trustees otherwise known as the Group Trustee Board including the Group Lead Volunteer.

The Group Trustee Board are responsible for the day-to-day operation of the CCTV systems and compliance with this policy.

Overview of the System

The CCTV system runs 24 hours a day, 7 days a week.

The CCTV system is managed locally and remotely by the nominated individuals.

The CCTV system comprises of fixed position cameras; monitors; digital recorders; remote monitoring applications; and public information signs.

Cameras are located at strategic points throughout the Group's premises. The Group has positioned the cameras so that they only cover communal or public areas on the premises, and they have been sited so that they provide clear images. No camera focuses, or will focus, on toilets. All cameras are also clearly visible.

Images are restricted to those entering/exiting the premises or in the immediate vicinity of the buildings to assist in the prevention and detection of crime or equivalent malpractice, as well as prosecution of offenders. Cameras have been positioned to prevent focusing on any surrounding private residential gardens and windows into residential buildings.

CCTV signs are prominently placed around the premises to inform young people, adult volunteers, visitors and members of the public that a CCTV installation is in use.

Although every effort has been made to ensure maximum effectiveness of the CCTV system it is not possible to guarantee that the system will detect every incident taking place within the area of coverage.

Operating Standards

System Access

The CCTV cameras are connected via a private hard wired ethernet network directly plugged into a dedicated on-site network recorder. The cameras are on a dedicated sub-net. The data signal between cameras and NVR is digitally encrypted and requires a password to un-encode and view the camera feed. Access to recorded images is restricted to the operators of the CCTV system.

Operators of the system require an account name and password to access the Cameras and NVR management interface and/or images. The NVR is located in a locked cabinet to which only authorised personnel have access to the keys.

There are no monitors permanently connected to the NVR for live viewing or viewing recordings.

Live footage can also be viewed remotely by authorised persons using Hik-Connect app or via VPN.

Only authorised personnel can view recorded footage. When viewing recordings, personnel should ensure that it cannot be viewed by unauthorised persons.

It is expected that those accessing the system do so for the purposes of the outlined above only.

When recordings are viewed, a log shall be retained setting out the following:

- Person(s) reviewing recorded footage.
- time, date, and location of footage being reviewed; and purpose of reviewing the recordings.

Operator training

1st Ince and Elton Scout Group will ensure that all volunteers handling CCTV images or recordings are trained in the operation and administration of the CCTV system and on the impact of the Data Protection Act 1998 with regard to that system.

Processing of Recorded Images

CCTV images will be displayed only to persons authorised to view them or to persons who otherwise have a right of access to them. Where authorised persons access or monitor CCTV images on workstation desktops, they must ensure that images are not visible to unauthorised persons for example by minimising screens when not in use or when unauthorised persons are present. Workstation screens must always be locked when unattended. Images and video footage must not be stored locally on machines.

Quality of Recorded Images

Images produced by the recording equipment must be as clear as possible so that they are effective for the purpose for which they are intended. The standards to be met in line with the codes of practice referred to in the introduction of these procedures are set out below:

- recording features such as the location of the camera and/or date and time reference must be accurate and maintained.
- cameras must only be situated so that they will capture images relevant to the purposes for which the system has been established.
- consideration must be given to the physical conditions in which the cameras are located, i.e., additional lighting or infrared equipment may need to be installed in poorly lit areas.
- cameras must be properly maintained and serviced to ensure that clear images are recorded, and a log of all maintenance activities kept; and
- as far as practical, cameras must be protected from vandalism in order to ensure that they remain in working order. Methods used may vary from positioning at height to enclosure of the camera unit within a vandal resistant casing.

Retention and disposal

As the network video recording (NVR) system records digital images, any CCTV images that are held on the NVR are deleted and historical data is overwritten in chronologically order to produce an approximate 14 – 21-day rotation of data retention and, in any event, are not held for more than 31 days.

Provided that there is no legitimate reason for retaining the CCTV images (such as for use in legal proceedings), the images will be erased following the expiration of the retention period.

All retained CCTV images will be stored securely on the 1st Ince and Elton SharePoint system and not on personal computers or storage.

Images that are stored on, or transferred on to, removable media such as USB drives/CDs are erased or destroyed once the purpose of the recording is no longer relevant. In normal circumstances, this will be a period of one month. However, where a law enforcement agency is investigating a crime, images may need to be retained for a longer period.

Data Protection

The Group has carried out a Data Protection Impact Assessment (DPIA), as provided and recommended by The Surveillance Camera Commissioner. This has been used to check and demonstrate that the processing of personal data by the CCTV System is compliant with the GDPR and DPA. Copies can be requested from: dataprotection@1stinceandelton.org.uk.

CCTV digital images, if they show a recognisable person, are personal data and are covered by the GDPR and data privacy legislation. This policy is associated with the Groups Data Privacy Policy.

The Group is required to register its processing of personal data via the CCTV System with the Information Commissioner's Office (ICO). The Groups ICO notification registration number is ZB291118, renewed annually in January.

Access to images

Access to images will be restricted to specifically authorised persons and in line with the purpose of the system and the GDPR and data privacy legislation.

Individuals

The GDPR and data privacy legislation gives individuals the right to access personal information about themselves, including CCTV images.

All requests for access to a copy of CCTV material should be made to dataprotection@1stinceandelton.org.uk.

Requests for access to CCTV images must include:

- The date and time the images were recorded
- Information to identify the individual, if necessary
- The location of the CCTV camera
- Proof of Identity.

The Group will respond promptly and at the latest within 30 calendar days of receiving the request. All requests must be accompanied with sufficient information to identify the images requested.

The Group will always check the identity of the person making the request before processing it.

The Group Trustee Board will first determine whether disclosure of their images will reveal third party information as they have no right to access CCTV images relating to other people. In this case, the images of third parties may need to be obscured if it would otherwise involve an unfair intrusion into their privacy.

If the Group is unable to comply with their request because access could prejudice the prevention or detection of crime or the apprehension or prosecution of offenders, the individual will be advised accordingly.

The Group Trustee Board are the only person(s) who are permitted to authorise disclosure of images to external third parties such as law enforcement agencies.

All requests for disclosure and access to images will be documented, including the date of the disclosure, to whom the images have been provided and the reasons why they are required. If disclosure is denied, the reason will be recorded.

Third parties

Disclosure of images to other third parties will only be made in accordance with the purposes for which the system is used and will be limited to:

- The police and other law enforcement agencies, where the images recorded could assist in the prevention or detection of a crime or the identification and prosecution of an offender or the identification of a victim or witness.
- Prosecution agencies, such as the Crown Prosecution Service.
- Relevant legal representatives.
- Line managers involved with disciplinary and performance management processes.
- Individuals whose images have been recorded and retained (unless disclosure would prejudice the prevention or detection of crime or the apprehension or prosecution of offenders).

The Group Trustee Board are the only person(s) who are permitted to authorise disclosure of images to external third parties such as law enforcement agencies.