Scouts

1st Ince and Elton

1st Ince and Elton HQ CCTV Policy

Ref number:	1STIEGP14	Date of issue:	19/01/2022	Prepared by:	Ashley Proctor
Page:	Page 1 of 6	Revision number:	002	Approved by:	Group Exec Committee

CCTV Policy

Introduction

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 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 Executive Committee including the Group Scout Leader.

The Group Executive Committee 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. Each site's NVR is located in a locked cupboard 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 Executive Committee 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 Executive Committee 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 Executive Committee are the only person(s) who are permitted to authorise disclosure of images to external third parties such as law enforcement agencies.