Policy Document:

CCTV.

Policy Document:

CCTV.

1. Introduction

1.1. The purpose of this Policy is to regulate the management, operation and use of the closed circuit television (CCTV) system at The Meadows Day Care Centre, hereafter referred to as 'the centre'.

1.2. The system may comprise of a number of fixed, or mobile cameras, with or without built-in microphones, located around the centre site. All cameras are monitored from the centres office, remotely accessed via the internet or smartphone applications and are only available to selected senior staff and selected members of the committee.

1.3. This policy follows GDPR guidelines.

1.4. The policy will be subject to review annually to include consultation as appropriate with interested parties.

1.5. The CCTV system is owned by the centre.

2. Objectives of the CCTV scheme

2.1. To protect the centres buildings and their assets.

2.2. To increase personal safety and reduce the fear of crime.

2.3. To support the Police in a bid to deter and detect crime.

2.4. To assist in identifying, apprehending and prosecuting offenders.

2.5. To protect members of the public and private property.

2.6. To assist in managing the centre.

2.7. To assist in staff training and staff disciplinary procedures if appropriate.

2.8. To assist in other matters as seen an appropriate use by the management.

3. Statement of intent

3.1. The CCTV Scheme will be registered with the Information Commissioner under the terms of GDPR and will seek to comply with the requirements both of the Data Protection Act and the Commissioner's Code of Practice.

3.2. The centre will treat the system and all information, documents and recordings obtained and used as data which are protected by GDPR.

3.3. Cameras will be used to monitor activities within the centre, its grounds and other public areas to identify criminal activity actually occurring, anticipated, or perceived, and for the purpose of securing the safety and wellbeing of the centre, together with its visitors.

3.4. Staff have been instructed that static cameras are not to focus on private homes, gardens and other areas of private property.

3.5. Unless an immediate response to events is required, staff must not direct cameras at an individual, their property or a specific group of individuals.

3.6. Materials or knowledge secured as a result of CCTV will not be used for any commercial purpose. Recordings will only be released to the media for use in the investigation of a specific crime and with the written authority of the police. Recordings will never be released to the media for purposes of entertainment.

3.7. The planning and design has endeavoured to ensure that the Scheme will give maximum effectiveness and efficiency but it is not possible to guarantee that the system will cover or detect every single incident taking place in the areas of coverage.

3.8. Warning signs, as required by the Code of Practice of the Information Commissioner have been placed at all access routes to areas covered by the centre CCTV.

4. Operation of the system

4.1. The Scheme will be administered and managed by the centres Management Team, in accordance with the principles and objectives expressed in the code.

4.2. The day-to-day management will be the responsibility of the centres Management Team.

4.3. The CCTV system will be located within the centres office and accessed from the centres office, remotely accessed via the internet or smartphone applications where it will be password protected to allow access only by the Management Team.

4.4. The CCTV system will be operated 24 hours each day, every day of the year.

5. Equipment Monitoring

5.1. The Management Team will check and confirm the efficiency of the system daily on weekdays during term time and in particular that the equipment is properly recording and that cameras are functional.

5.2. Unless an immediate response to events is required, staff operating the CCTV equipment must not direct cameras at an individual or a specific group of individuals.

5.3. Visitors and other contractors wishing to gain access to the CCTV equipment will only be able to with the correct password

5.4. The password must only be given to authorised vetted persons approved by the Management Team and a log kept of all access granted.

5.5. Other administrative functions will include maintaining hard disc space, filing and maintaining occurrence and system maintenance logs.

5.6. Emergency procedures will be used in appropriate cases to call the Emergency Services.

6. Liaison

6.1. Liaison meetings may be held with all bodies involved in the support of the system.

7. Monitoring procedures

7.1. Camera surveillance may be maintained at all times.

7.2. A monitor may be installed in the Main Office to which pictures will be continuously recorded.

7.3. A PC connected to the network may be connected to the NVR/DVR equipment, where access to camera surveillance and recordings will be password protected.

7.4. A remote PC or smartphone may be connected to the NVR/DVR via the internet, where access to camera surveillance and recordings will be password protected.

7.5. If covert surveillance is planned, it can only be undertaken by the police after providing sufficient need and with authorisation of the Management Team.

8. **Recording procedures**

8.1. The CCTV system will utilise a hard drive, which will provide a continuous recording medium. Once the hard drive is full, the system will go back to the start and record over the oldest records, wiping them out.

8.2. To capture a particular event as a permanent record the CCTV operator will be able to copy an event off the hard drive onto a suitable media storage via PC. Either after transferring the images from the NVR/DVR to a USB flash drive and then to the PC, or directly using software via network or internet access.

8.3. In order to maintain and preserve the integrity of the media storage used to record events from the hard drive and the facility to use them in any future proceedings, the following procedures for their use and retention must be strictly adhered to:

(i) Each storage device must be identified by a unique mark.

(ii) Before using each storage device must be cleaned of any previous recording.

(iii) The controller shall register the date and time on each storage device, including reference.

(iv) A storage device required for evidential purposes must be sealed, witnessed, signed by the controller, dated and stored in a separate, secure, evidence tape store. If a device is not copied for the police before it is sealed, a copy may be made at a later date providing that it is then resealed, witnessed, signed by the controller, dated and returned to the evidence tape store.

(v) If the device is archived the reference must be noted.

8.4. Devices may be viewed by the Police for the prevention and detection of crime.

8.5. A record will be maintained of the release of storage device to the Police or other authorised applicants. A register will be available for this purpose.

8.6. Viewing of media by the Police must be recorded in writing and in a log book. Requests by the Police can only be actioned under section 29 of the Data Protection Act 1998.

8.7. Should a storage device be required as evidence, a copy may be released to the Police under the procedures described in paragraph 8.1 (iv) of this Code. Disks will only be released to the Police on the clear understanding that the device remains the property of the centre, and both the device and information contained on it are to be treated in accordance with this code. The centre also retains the right to refuse permission for the Police to pass to any other person the device or any part of the information contained thereon. On occasions when a Court requires the release of an original device this will be produced from the secure evidence device store, complete in its sealed bag.

8.8. The Police may require the centre to retain the stored device for possible use as evidence in the future. Such devices will be properly indexed and properly and securely stored until they are needed by the Police.

8.9. Applications received from outside bodies (e.g. solicitors) to view or release devices will be referred to the Management Team. In these circumstances devices will normally be released where satisfactory documentary evidence is produced showing that they are required for legal proceedings, a subject access request, or in response to a Court Order. A fee can be charged in such circumstances: £10 for subject access requests; a sum not exceeding the cost of materials in other cases.

9. **Breaches of the code (including breaches of security)**

9.1. Any breach of the Code of Practice by centre staff will be initially investigated by the Management Team, in order for them to take the appropriate disciplinary action.

9.2. Any serious breach of the Code of Practice will be immediately investigated and an independent investigation carried out to make recommendations on how to remedy the breach.

10. **Assessment of the scheme and code of practice**

10.1. Performance monitoring, including random operating checks, may be carried out by the Management Team.

11. **Complaints**

11.1. Any complaints about the centre's CCTV system should be addressed to the Chairman.

11.2. Complaints will be investigated in accordance with Section 9 of this Code.

12. **Access by the Data Subject**

12.1. GDPR provides Data Subjects (individuals to whom "personal data" relate) with a right to data held about themselves, including those obtained by CCTV.

12.2. Requests for Data Subject Access should be made in writing providing dates, times and if requested a photograph of the person(s) concerned.

13. **Public information**

13.1. Copies of this Code of Practice will be available to the public from the Centre Office.

Summary of Key Points

- This Code of Practice will be reviewed annually.
- The CCTV system is owned and operated by the centre.
- The CCTV system will and can be accessed out of centre hours via remote internet access.
- Access to the CCTV system will be password protected and not open to visitors except by prior arrangement and good reason.

- Liaison meetings may be held with the Police and other bodies.
- Recording devices will be used properly indexed, stored and destroyed after appropriate use.
- Devices may only be viewed by Centre Officers and the Police.
- Devices required as evidence will be properly recorded witnessed and packaged before copies are released to the Police.
- Devices will not be made available to the media for commercial or entertainment.
- Devices will be disposed of securely by incineration or shredding.
- Any breaches of this code will be investigated by the Management Team. An independent investigation will be carried out for serious breaches.

Breaches of the code and remedies will be reported to the Chairman.