
Tuition
extra

CCTV Policy

Head of Tuition Service: Lydia Blench

Head of Maypole Farm: James Pickles

Approved: 01 October 2024

Signed: Ruth Minhall

Position: CEO

Last reviewed: September 2023

Next review: Sept 2025

Contents

1. CCTV STANDARD AND THE LAW

1.1 Closed Circuit Television 'CCTV' and its use is governed by the Data Protection Act 2018 (DPA) and the General Data Protection Regulation 2016 (GDPR). The Service have a legal duty to comply with the relevant Data Protection Legislation. This Policy is to ensure CCTV within the Service is controlled appropriately to facilitate the Service's legal obligations, best practice and to reduce risk of information loss. The CCTV Policy should be read in conjunction with the Service's additional policies.

1.2 The Service is the body that makes the decisions concerning CCTV, for example, who has responsibility for the control of the images, i.e. deciding what is to be recorded, how the images should be used and to whom they may be disclosed. The Service is the data controller and is legally responsible for compliance with the GDPR and DPA. This Policy is not intended to replace procedures already in place within the Service that relate to the physical operation and use of the system.

1.3 With regard to the decision as to how the images are used and to whom they may be disclosed, this delegated responsibility lies with the governing body, SLT and the Service's DPO. Certain staff members are identified as authorised personnel, in certain circumstances, regarding the use and control of the equipment and viewing the live or recorded images (see clause 3.1 (f)). This ensures that the sharing of personal data is kept to a minimum within the service.

1.4 CCTV can record personal data and sound in the form of a person's face and may indicate 'special category' personal data, such as a person's ethnic origin or physical disability. This means that live or recorded images and monitor screens should not be viewed by any unauthorised third party without a lawful basis i.e. the person(s) that appear and are identifiable from the footage.

1.5 As an organisation frequented by members of the public, including staff, pupils, parents/carers, visitors and contractors, the Service is required to place CCTV monitors in a secure environment where those members of the public are not able to see images.

1.6 All authorised operators and employees with access to images are aware of the procedures that need to be followed when accessing the recorded images. All operators are trained by the appropriate person in their responsibilities under the ICO's CCTV Code of Practice. All authorised employees are aware of the restrictions in relation to access to, and disclosure of, recorded images within this CCTV Policy. The CCTV Policy must be read by any person/employee/contractor who will process personal data belonging to the Controller, the Service. The Service will make this CCTV Policy a public facing document.

2. WHY THE SERVICE USES CCTV

1.1 The Service uses CCTV for the purpose of a public task duty, the management and security of the site, monitoring health and safety and safeguarding of the pupils, parents, visitors and employees on site. By using CCTV, the Service can monitor occurrences on site and also the security of the buildings and grounds. The Service may use CCTV for "crime prevention" and it would be acceptable to disclose images to law enforcement agencies if failure to do so would be likely to prejudice the prevention and detection of crime. The footage may also be used as evidence during internal

disciplinary proceedings or complaints where specific issues have been raised and corroborative evidence is necessary.

3. HOW THE SERVICE USES CCTV

3.1 When installing CCTV there are several issues to be taken into consideration, such as:

a) Where to position the cameras?
b) Where to position the monitors?
c) Who will operate the cameras?
d) Who will handle requests for access to the images?
e) How do we record who sees the images and for what purpose?
f) Who do we authorise to access the images and for what purpose?

A. The person or body responsible for the management of the Service's premises, under the guidance of the Data Protection Officer (DPO) will be responsible for identifying the most suitable place to locate the cameras. The cameras will not process data that may be deemed as 'excessive', such as capturing public areas outside the scope of the Service, or where there is a reasonable expectation of privacy such as toilets or staffrooms, as this goes beyond what is proportionate and necessary to fulfil the purpose for processing the personal data.
B. Along with the external considerations, the Service's management of premises will identify the most appropriate housing for the monitors, ensuring security and privacy. In maintained services this may be the Local Authority. This will take into account the cabling and technical accessories of the equipment. This will be undertaken in compliance with data protection legislation, British Standards and consideration of the advice taken from the Service's DPO. This would need to take into account capturing the best view of buildings for the purposes of security and high risk areas around the Service. The cameras must be of such quality to satisfy the purposes of installing the CCTV.
C. The CCTV system is owned and operated by the service, and its deployment is determined by the Service's management team. Installation should be carried by an industry-approved installer. The Service's authorised personnel is responsible for ensuring that the cameras are working correctly and consistently and will be responsible for ensuring they are maintained. This may mean retaining the services of a specialist CCTV service company who would also be considered as authorised personnel.
D. Subject Access Requests are dealt with in clause 10.
E. A record of access and disclosure will be kept for disclosure of images in accordance with clause 6.
F. Access to recorded images is restricted to authorised personnel only.

3.2 The Service takes a privacy by design approach and will conduct a Data Protection Impact Assessment (DPIA) with guidance from the Service's DPO in accordance with GDPR, as they are systematically monitoring and capturing 'vulnerable' data

subjects, such as children. The Service will also ensure a GDPR compliant agreement is in place with any organisation where personal data/CCTV footage is processed on behalf of the Service.

3.3 Any changes to CCTV monitoring will be subject to a Data Protection Impact Assessment (DPIA) in which the Service's DPO will provide advice.

3.4 The use of CCTV recording involving audio recording between members of the public is highly intrusive and unlikely to be justified. The appropriate personnel should choose a system without this facility if possible. If CCTV system are equipped with a sound recording facility these should be disabled.

3.5 In the exceptional circumstances where audio recording is justified and this has been agreed with the DPO, it must be limited to that which is necessary to achieve the purposes specified in paragraph 4, appropriate signage and notification must make it clear that audio recording is or may be carried out.

OBJECTIVES OF THE CCTV SYSTEM

4.1 To protect pupils, staff and visitors.

4.2 To increase personal safety and reduce the fear of crime.
4.3 To protect the service buildings and assets.
4.4 Without prejudice, to protect the personal property of pupils, staff and visitors.
4.5 To support the police in preventing and detecting crime.
4.6 To assist in identifying, apprehending and prosecuting offenders.
4.7 To assist in managing the Service.

5.0 STORING AND VIEWING IMAGES

5.1 When conducting a viewing, either of live images or recorded playback, the viewing should take place in a secure office and only those persons who are authorised and/or who appear on the footage, should be present where relevant. Staff should ensure that no part of the footage can be seen through a window in a door or a window looking into the office from an external area. The office door should be completely closed for the duration of the viewing and for any discussions about the footage that may follow.

5.2 In general, CCTV footage should be kept for a maximum of 30 days, unless an incident has occurred on Service premises and the footage is to be kept for a purpose. CCTV footage is stored securely in a lockable office / on the Service's password protected software system. If an incident has occurred, the footage in question should be stored securely in a way that maintains the integrity of the images pending further action. Once the action/investigation has been concluded, a review of the retention of the footage should be exercised and secure, permanent disposal of the footage should occur where there is no longer a valid lawful basis to keep the images.

5.3 The Service has developed a form called the "CCTV Disclosure Record" and it must be completed on every occasion that footage is viewed or disclosed to a third party. The form should be forwarded to the Data Protection Officer as and when a valid request for CCTV footage is made. The form can be located on the Service's internal shared drive. The record will include the following:

5.3.1 the purpose of any searches and whether the search was successful or not

5.3.2 who carried out the search

5.3.3 persons present (particularly when reviewing).

5.3.4 date, start and end time of the incident.

5.3.5 date and time of the review

5.3.6 any other relevant information

6.0 DISCLOSURE OF IMAGES

6.1 The Service will ensure that any disclosure of images is in a controlled manner and that the disclosure is consistent with their data mapping and privacy notice in regards to CCTV. Any disclosure should be clearly documented by the Service as outlined in clause 5.3.

6.2 There will be no disclosure of recorded data to third parties without a lawful basis. It is acceptable for the Service to disclose images to law enforcement agencies for the purpose of prevention and detection of crime. These requests should be:

- be provided in writing (WA170) where possible
- signed by authorised officers
- make reference to the name and section of the legislation that entitles them to receive the information.

6.3 The Service will document in their DPIA how personal information will be shared. In the case of a disclosure request from law enforcement or a valid subject access request, the recording pertaining to the request will be downloaded onto a portable device and securely stored in a locked room until collection. The process will remain the same when disclosing in regard to insurance purposes. The file will be encrypted or password protected where possible. Alternatively, the recording will be sent in a password protected document via email. Staff will ensure passwords are given to the authorised recipient separately from the email containing the recording, ensuring that the original copy of the recording is kept at the Service for only as long as is necessary for the purpose of retaining the recording.

- If the immediate viewing of a recording is necessary, this will be governed by clause 5 above.
- In cases where disclosure is requested by a third party who does not appear on the footage, extreme caution should be taken and the DPO referred to. Where this is a parent on behalf of a pupil, the Subject Access Guidance should be followed. Where

technology permits, images of third parties should be blurred and unidentifiable if a disclosure request does not pertain to them.

- The data may be used within the service's discipline and complaints procedures as required, and will be subject to the usual confidentiality requirements of those procedures.

7.0 AUTHORISED PERSONNEL AND CIRCUMSTANCES

7.1 The persons authorised to operate the equipment and view the monitors are appropriate personnel. The appropriate personnel will have received training in the operation of the particular systems used by the Service. However, there may be occasions that will require contractors to view the monitors during the recording of live images and also images that have been recorded previously. It is important to remember that the viewing of all images from a CCTV system must be controlled and consistent with the purpose for which the system was installed. On a routine basis, this means that teaching and support staff cannot request to access footage.

7.2 On occasion the Service may receive a request to carry out covert monitoring on behalf of the Police, which must be requested with evidence of the Police's RIPA authorisation for this surveillance. If this is not possible due to sensitivity issues.

Appropriate personnel will allow third parties to view live and recorded images for maintenance purposes and in compliance with the objectives of the CCTV objectives set out in paragraph 4.

7.3 The Service's DPO may be involved in any circumstances where the Service feels advice is necessary. Where the Service is unsure of whether to seek advice from the DPO, for the avoidance of doubt advice should be sought.

8. BREACHES

8.1 A 'personal data breach' means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

8.2 Any breach of security will be initially investigated by the Service's appropriate personnel, in order to discuss this further with the Service's DPO, governing body and Senior Leadership Team. The Service's DPO may initiate communications to the ICO, within the 72 hour period, in cases where the breach could lead to or has led to a risk of harm. The Service's DPO may extend the communications to those affected by the breach, in order to provide them with the details in regards to the breach of their personal information and how they can take precautions from further consequences of the breach.

8.3 The Service may take the appropriate disciplinary action in the relevant circumstances. A breach of this policy will be governed by the Service's existing policies and procedures. Any serious breach of the CCTV Policy may be concluded to be a form of gross misconduct. It will be immediately investigated and an independent investigation carried out to make recommendations on how to remedy the breach. This investigation will involve the input of the Service's DPO.

8.4 A breach of security in relation to CCTV footage will be actioned in line with the Service's Breach Procedure.

** Where a criminal offence has been committed on Service premises, the Service is not under any duty to release the footage to or allow it to be viewed by the subject, their family or friends. Any unauthorised disclosure of the footage may prejudice any subsequent police enquiry. The footage should be downloaded onto disk/memory stick/email attachments and given directly to the police as evidence, following the production by the police of a valid request for disclosure. When an incident occurs on Service premises during evenings and weekends, it would be necessary to contact the Site Services Manager or appropriate person.*

This means that on those occasions the Site Services Manager or appropriate person would be an authorised person in order to view footage and in an emergency, disclose it to the police. On receipt of a 'routine' subject access request by an individual, the Site Services Manager or appropriate person should ask the requestor to complete a 'Subject Access Request' form available on the Service's website and send it to the Service's email address.

If the Site Services Manager or appropriate person receives a request from the police, but it is not an emergency, the request should be directed to the Service's email address to be dealt with during normal office hours.

9. CCTV and GDPR

9.1 In order to comply with the right to be informed, significant signage is found in prominent positions in all areas where CCTV cameras operate to inform staff, students and the general public that they are entering an area where their images are being recorded either as still or video footage. Employee, parent, pupil and visitor privacy notices include the information that the service uses CCTV cameras. Visitors must have the knowledge of who to contact to make an enquiry regarding the system where this is not obvious.

9.2 The right for individuals to request access to their data can be exercised using a subject access request template on the service's website.

9.3 The right to object/restrict processing may be possible in certain circumstances. However, this will be considered on a case-by-case basis.

9.4. The right to rectification will apply where possible.

9.5 The right to data portability is not applicable as CCTV is filmed under the public task duty. Automated decision making is not included in this process.

9.6 Data minimisation is exercised with the automated deletion of CCTV footage after 30 days, unless an exemption to the rule applies. For example a police investigation is ongoing.

9.7 The right to erasure is considered where the personal data is no longer necessary in relation to the purposes for which it was processed.

9.8 All rights can be exercised by individuals contacting the Service or the named DPO.

10. SUBJECT ACCESS REQUESTS

10.1 Individuals have the right to request access to CCTV footage relating to themselves under the GDPR and DPA. The Subject Access and ICO guidance will be followed.

10.2 All requests should be made in writing to the Service. Individuals submitting requests for access will be asked to provide sufficient information to enable the footage relating to them to be identified. For example, date, time and location.

10.4 The Service will respond to a request within one calendar month of receiving a valid request.

10.5 Where a Subject Access Request includes footage of another individual not included in the request, the service must either use 'blurring' to distort the images to only the relevant individual or gain consent to disclose third party personal data from those individuals not involved in the request.

10.6 The Service reserves the right to refuse access to CCTV footage where this would prejudice the legal rights of other individuals or jeopardise an ongoing investigation.

10.7 Wherever possible, the Service will notify the requester if an exemption or limitation to their request applies, such as, but not limited to:

- **10.7.1** A claim to legal professional privilege in legal proceedings
- **10.7.2** The request will infringe on a third party's rights and freedoms
- **10.7.3** Any other exemption to the right of access as stated in the GDPR and DPA.

10.8 The Service understands that individuals have further individual rights under the GDPR and DPA and will seek DPO advice where necessary.

11.0 FREEDOM OF INFORMATION

11.1 The Service may receive requests under the Freedom of Information Act 2000 (FOI). A response must be provided within 20 working days, beginning from the next working date after receipt of the request.

11.2 If individuals are capable of being identified from the CCTV images, personal data is unlikely to be disclosed in response to an FOI request as Data Protection Legislation will apply and the rights of the individual will need to be considered.

12.0 APPEALS

12.1 There is a Service 'Subject Access Procedure' that should be followed in the event that an individual is refused access to CCTV images and they are not satisfied with this outcome or the reasons why access has been refused. The appeal procedure document will be provided to the requester in the final response from the Service to the individual making the Subject Access Request.

13.0 COMPLAINTS

13.1 Complaints and enquiries about the operation of CCTV within the service should be addressed through the Service's complaints procedure. Where necessary, the Service's Data Protection Officer will be informed of the complaint.

14.0 REVIEW

14.1 The Service's DPO and SLT will review this document annually to reflect changes in best practice, legislative changes and guidance from the Regulatory Authority (Information Commissioner's Office).