CCTV Policy 2023

Approved date		November 2021
Review date		January 2023
Pending approval		April 2023 at FAR committee

Contents

Policy Aim

This document will enable staff of Horizon Multi Academy Trust to comply with legislation relating to CCTV in all circumstances.

1. **Executive Summary**

1.1 The Horizon Multi Academy Trust (MAT) deploys CCTV where it is felt that the presence of the cameras and the capture of images aids in facilitating the security and safety of all students, staff, visitors, contractors plus the Trust's assets.
(Although there is no expectation CCTV would be deployed to support disciplinary issues of staff or contractors in the unlikely events issues are recorded may be used appropriately.)

1.2 The policy will set out the purpose of using CCTV, what information will be recorded, who will have access to this information and how this information will be stored and disposed of.

2. **Policy Statement**

2.1. This Policy seeks to ensure that the Close Circuit Television (CCTV) system used at Horizon Multi Academy Trust's schools are operated in compliance with the law relating to data protection (currently the General Data Protection Regulation ("GDPR") and the Data Protection Act 2018 ("DPA 2018") and as amended from time to time and includes the principles governing the processing of personal data as set out in the Trust's GDPR policy. It also seeks to ensure compliance with privacy law. It considers best practice as set out in codes of practice issued by the Information Commissioner and by the Home Office. Horizon MAT therefore uses CCTV only where it is necessary in pursuit of a legitimate aim, as set out in clause 2.2, and only if it is proportionate (as determined by the Trust) to that aim.

2.2. Horizon MAT seeks to ensure, as far as is reasonably practicable, the security and safety of all students, staff, visitors, contractors, its property, and premises.

Horizon MAT therefore deploys CCTV to:

- promote a safe Horizon MAT community and to monitor the safety and security of its premises, staff, and students.
- assist in the prevention, investigation, and detection of crime.
- assist in the apprehension and prosecution of offenders, including use of images as evidence in criminal proceedings; and
- assist in the investigation of breaches of its codes of conduct and policies by students and, where relevant and appropriate, investigating complaints.
- assist (where images captured) in the investigation of breaches of its codes of conduct and policies by staff and contractors and, where relevant and appropriate, investigating complaints.

2.3 This policy will be reviewed annually by the MAT Data Protection Officer to assess compliance with clauses 2.1 and 2.2 and to determine whether the use of the CCTV system

remains compliant. The DPO will also ensure there have been no changes in legislation or guidance that required the policy to be updated.

2.4 The operational requirements for the CCTV system in use across Horizon MAT's schools are documented in a "CCTV Operational Requirement Report", held, and maintained by the Data Protection Officer.

3. Scope

3.1 This policy applies to CCTV systems in all parts of Horizon MAT and other related facilities.

3.2 This policy does not apply to any Webcam systems located in meeting rooms, classrooms, or other areas in school, which are used for the purposes of to assist with the use of the audio-visual equipment, virtual meetings, or remote learning.

3.3 This policy applies to all persons employed or contracted by Horizon MAT and/or allowed access to CCTV system including Security Management and Staff, and the Data Protection Officer.

4. Roles and responsibilities

4.1 The Data Protection Officer has the overall responsibility for this policy but has delegated day-to-day responsibility for overseeing its implementation to the appropriate staff member at each school, usually the Head Teacher and/or the Site Manager and/or Business Manager or Senior Administrator. All relevant members of staff have been made aware of the policy and have received appropriate training.

4.2 The Business Operations Manager of Horizon Multi Academy Trust is responsible for ensuring that the CCTV system including camera specifications for new installations complies with the law and best practice referred to in clause 2.1 of this policy. Where new surveillance systems are proposed, the Business Operations Manager will consult with the Data Protection Officer to assist with the creation of the required data protection impact assessment. This will also apply if systems are modified.

4.3 Only the Site Manager at each school or a properly appointed maintenance contractor for Horizon MAT CCTV system is authorised to install and/or maintain it to ensure it is working correctly.

4.4 The Responsible Person at each school will be determined by the Business Operations Manager and DPO but will be one or more of the following roles: Head Teacher; Site Manager Business Manager/Senior Administrator. They will be responsible for the evaluation of locations where live and historical CCTV images are available for viewing. The list of such locations (all must be a secure and non-public private location) and the list of persons authorised to view CCTV images is maintained by the Business Operations Manager.

4.5 Changes in the use of Horizon MAT CCTV system can be implemented only in consultation with Horizon MAT Data Protection Officer or the Horizon MAT Legal Advisors.

5. System Description – Fixed Cameras

5.1 The CCTV systems installed in and around Horizon MAT's various schools cover building entrances, car parks, perimeters, and external areas such as courtyards. They are not usually present in internal areas. However, it might be deemed that social spaces, computer rooms, rooms with high value equipment, some corridors and reception areas may benefit from the fitment of a CCTV system. The CCTV systems typically continuously record activities in these areas [though some of the cameras are set to motion detection]. Where possible, CCTV cameras have been positioned to be mindful of neighbouring properties and not intrude on neighbour's privacy.

5.2 CCTV Cameras are not installed in areas in which individuals would have an expectation of privacy such as toilets, changing facilities and classrooms etc.

5.3 CCTV cameras are installed in such a way that they are not hidden from view. Signs are prominently displayed where relevant, so that staff, students, visitors, and members of the public are made aware that they are entering an area covered by CCTV. The signs also contain contact details as well as a statement of purposes for which CCTV is used and direct people to Horizon MAT's website for more information.
The contact point for queries about CCTV around (Horizon Multi Academy Trust) should be available to staff, students, and members of the public during normal business hours. Any employees staffing the contact point must be familiar with this document and the procedures to be followed if an access request is received from a Data Subject or a third party.

6. Covert Recording

6.1 Covert recoding (i.e. recording which takes place without the individual's knowledge) will not take place.

7. Operating Standard

7.1 The operation of the CCTV system will be conducted in accordance with this policy.

7.2 All CCTV control equipment, recordings, logs and data will be secured where only authorised personnel can access the system controls / see the recorded images. This may be a lockable cabinet, in a secure area. Where this is not possible the DVR will be secured (bolted) to something that is not removable, to prevent the recording device being removed from any location.

7.2.1 No unauthorised access will be permitted to the controls or images of the CCTV system.

7.2.2 A register of authorised persons which can access the system / view the images in each school is maintained by the DPO. This is expected to be Head Teacher, Assistant Headteacher(s), Site Manager, Business Manager, Senior Administrator.

7.2.3 CCTV Systems Monitors are not visible from outside the room where the CCTV is located. The position / methodology where/how the CCTV system / recordings are accessed must not be overlooked so that only the authorised persons can see the images / data.

7.2.4 Before permitting anyone access to the footage, the Site manager, head teacher, Business Manager/Senior Administrator or DPO will satisfy themselves of the identity of any visitor and existence of the appropriate authorisation. These persons are assumed to be

- persons specifically authorised by the Site Manager of the school,
- maintenance engineers,
- police officers where appropriate; and
- any other person with statutory powers of entry.

All visitors are required to complete and sign the visitors' log, which includes details of their name, department and/or the organisation that they represent, the person who granted authorisation and the times of viewing footage.

7.2.5 A log shall be retained setting out the following:

- person reviewing recorded footage.
- time, date, and location of footage being reviewed; and
- purpose of reviewing the recordings.

7.3 Processing of Recorded Images

7.3.1 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 workstations, 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.

7.4 Quality of Recorded Images

7.4.1 Images produced by the recording equipment must be as clear as possible, so 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 clause 1 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 purpose 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 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.

8. **Retention and Disposal**

8.1 CCTV images are not to be retained for longer than necessary, considering the purposes for which they are being processed. Data storage is automatically managed by the CCTV digital records which overwrite historical data in chronological order to produce an approximate 28-day rotation in data retention, though this may be extended to 8 weeks during the school summer holiday period. The Site manager at each school is responsible for ensuring this happens.

8.2 Provided that there is no legitimate reason for retaining the CCTV images (such as for use in disciplinary and/or legal proceedings), the images will be erased following the expiration of the retention period (normally 28 days/1 calendar month but extended during the school summer holidays to 8 weeks). Should data need to be retained longer than stated in this policy, then the BOM and DPO must be informed.

8.3 All retained CCTV images will be stored securely, on a device that is password protected; the device is in a lockable cabinet or secured so cannot be removed easily from its secure location. Data is destroyed by deleting electronic files from all storage locations including the Digital Video Recording device, cloud-based storage, and physical server storage both on and off site.

9. **Data Subject Rights**

9.1 Recorded images, which directly or in combination with other factors enable a data subject to be identified, are considered to be the personal data of the individuals whose images have been recorded by the CCTV system.

9.2 Data Subjects have a right of access to the personal data under the GDPR and DPA 2018. They also have other rights under the GDPR and DPA 2018 in certain limited circumstances, including the right to have their personal data erased, rectified, to restrict processing and to object to the processing of their personal data.

9.3 Data Subjects can exercise their rights by submitting a request in accordance with the Horizon MAT Data Protection policy.

9.4 On receipt of the request, the Data Protection Officer, or their representative, will liaise with the Business Operations Manager regarding compliance with the request, and subject to clause 10.5, the Data Protection Officer will communicate the decision without undue delay and at the latest within one month of receiving the request from the Data Subject.

9.5 The period for responding to the request may be extended by two further months where necessary, considering the complexity and number of the requests. The Data Protection Officer will notify the Data Subject of any such extension within one month of receipt of the request together with reasons.

10. **Third Party Access**

10.1 Third party requests for access will usually only be considered in line with the GDPR and DPA 2018 in the following categories:

- legal representative of the Data Subject.
- law enforcement agencies including the Police.
- disclosure required by law or made in connection with legal proceedings; and
- HR staff responsible for employees and administrative staff responsible for students in disciplinary and complaints investigations and related proceedings.

10.2 Legal representatives of the Data Subjects are required to submit to Horizon MAT a letter of authority to act on behalf of the Data Subject along with appropriate proof of the Data Subject's identity.

The Data Protection Officer will disclose recorded images to law enforcement agencies including the Police once in possession of a form certifying that the images are required for either:

- an investigation concerning national security.
- the prevention or detection of crime; or
- the apprehension or prosecution of offenders
- and that the investigation would be prejudiced by failure to disclose the information. Where images are sought by other bodies/agencies with a statutory right to obtain information, evidence of that statutory authority will be sought before CCTV images are disclosed.

10.4 Every CCTV image disclosed a record is made and sent securely to the DPO. It contains:

- the name of the police officer or other relevant person in the case of other agencies/bodies receiving the copy of the recording.
- brief details of the images captured by the CCTV to be used in evidence or for other purposes permitted by this policy.
- the crime reference number where relevant; and
- date and time the images were handed over to the police or other body/agency.

10.5 Requests of CCTV images for staff or student disciplinary purposes shall be submitted in writing to Business Operations Manager in consultation with the Data Protection Officer.

10.6 Requests for CCTV information under the Freedom of Information Act 2000 will be considered in accordance with that regime.

11. **Complaints and Procedure**

11.1 Any complaints relating to the CCTV system should be directed in writing to the Business Operations Manager promptly and in any event within 7 days of the date of the incident giving rise to the complaint. A complaint will be responded to within a month following the date of its receipt. Records of all complaints and any follow-up action will be maintained by the relevant office. If a complainant is not satisfied with the response, they may appeal to CEO.

11.2 Complaints in relation to the release of images should be addressed to the Business Operations Manager as soon as possible and in any event no later than three months from the event giving rise to the complaint.

12. USEFUL LINKS

The Information Commissioner's Code of Practice can be found at:
https://ico.org.uk/media/for-organisations/documents/1542/cctv-code-of-practice.pdf