Ormiston Academies Trust

Cowes Enterprise College, an Ormiston Academy CCTV policy

Policy version control

Policy type	Mandatory
Author	Les Leese
Approved by	James Miller, October 2019
Release date	November 2019
Next release date	November 2021
Description of changes	New policy

Contents

1. Introduction....3
2. Legal framework....3
3. Definitions....4
4. Roles and responsibilities....4
5. Purpose and justification....5
6. Data protection principles....5
7. Objectives....5
8. Protocols....6
9. Signage....6
10. Security....6
11. Privacy by design....7
12. Code of practice....7
13. Access....8

Appendix 1....10

Appendix 2....11

1. Introduction

1.1. At Ormiston Academies Trust (referred to as "the Trust" and any or all its academies), we take our responsibility towards the safety of staff, visitors and pupils very seriously. To that end, we use surveillance cameras to monitor for the safety and wellbeing of students, staff and visitors.

1.2. The purpose of this policy is to manage and regulate the use of the surveillance and CCTV systems at the Trusts Academies and ensure that:

- The images captured are being handled in accordance with data protection legislation as set out under GDPR
- The images that are captured are useable for the purposes we require them for.

1.3. This policy covers the use of surveillance and CCTV systems which capture moving and still images. of people who could be identified, as well as information relating to individuals for any of the following purposes:

- Observing what an individual is doing to ensure safety of students, staff and visitors
- Taking action to prevent a crime
- Using images of individuals that could affect their privacy

2. Legal framework

2.1. This policy has due regard to legislation including, but not limited to, the following:

- The Regulation of Investigatory Powers Act 2000
- The Protection of Freedoms Act 2012
- The General Data Protection Regulation
- The Freedom of Information Act 2000
- The Education (Pupil Information) (England) Regulations 2005 (as amended in 2016)
- The Freedom of Information and Data Protection (Appropriate Limit and Fees) Regulations 2004
- The School Standards and Framework Act 1998
- The Children Act 1989
- The Children Act 2004
- The Equality Act 2010

2.2. This policy has been created with regard to the following statutory and non-statutory guidance:

- Home Office (2013) 'The Surveillance Camera Code of Practice'
- ICO (2017) 'Overview of the General Data Protection Regulation (GDPR)'
- ICO (2017) 'Preparing for the General Data Protection Regulation (GDPR) 12 steps to take now'
- ICO (2017) 'In the picture: A data protection code of practice for surveillance cameras and personal information'

3. Definitions

3.1. For the purpose of this policy a set of definitions will be outlined, in accordance with the surveillance code of conduct:

- Surveillance – monitoring the movements and behaviour of individuals; this can include video, audio or live footage. For the purpose of this policy only video and audio footage will be applicable.
- Overt surveillance – any use of surveillance for which authority does not fall under the Regulation of Investigatory Powers Act 2000.
- Covert surveillance – any use of surveillance which is intentionally not shared with the subjects it is recording. Subjects will not be informed of such surveillance.

3.2. The Trust does not condone the use of covert surveillance when monitoring the academy's staff, pupils and/or volunteers. Covert surveillance will only be operable in extreme circumstances.

3.3. Any overt surveillance footage will be clearly signposted around the academy.

4. Roles and responsibilities

4.1. Cowes Enterprise College, an Ormiston Academy, as the corporate body, is the data controller. The principal of Cowes Enterprise College, an Ormiston Academy therefore has overall responsibility for ensuring that records are maintained, including security and access arrangements in accordance with regulations.

4.2. The Data Protection Lead (DPL) deals with the day-to-day matters relating to data protection and thus, for the benefit of this policy will act as the data controller.

4.3. The role of the data controller includes:

4.3.1. Processing surveillance and CCTV footage legally and fairly.
4.3.2. Collecting surveillance and CCTV footage for legitimate reasons and ensuring that it is used accordingly.
4.3.3. Collecting surveillance and CCTV footage that is relevant, adequate and not excessive in relation to the reason for its collection.
4.3.4. Ensuring that any surveillance and CCTV footage identifying an individual is not kept for longer than is necessary.
4.3.5. Protecting footage containing personal data against accidental, unlawful destruction, alteration and disclosure – especially when processing over networks.

4.4. The role of the principal includes:

4.4.1. Meeting with the Data Protection Officer (DPO) to decide where CCTV is needed to justify its means.
4.4.2. Conferring with the DPO with regard to the lawful processing of the surveillance and CCTV footage.
4.4.3. Monitoring legislation to ensure the academies is using surveillance fairly and lawfully.
4.4.4. Communicating any changes to legislation with the Trust.

5. Purpose and justification

5.1. The purpose of CCTV monitoring is to deter crime and to protect the safety and property of the academy. Safety and security purposes include, but are not limited to:

5.2. Protection of individuals, including students, staff and visitors;

5.3. Protection of academy-owned and/or operated property and buildings, including building perimeters, entrances and exits, lobbies and corridors, and internal spaces;

5.4. Verification of alarms and access control systems;

5.5. Patrol of common areas and areas accessible to the public

5.6. Investigation of criminal activity, safeguarding incidents and serious disciplinary activity.

6. Data protection principles

6.1. Data collected from surveillance and CCTV will be:

6.1.1. Processed lawfully, fairly and in a transparent manner in relation to individuals.
6.1.2. Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes.
6.1.3. Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.
6.1.4. Accurate and, where necessary, kept up to date; every reasonable step will be taken to ensure that personal data that is inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.
6.1.5. Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods, insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals.
6.1.6. Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

7. Objectives

7.1. The surveillance system will be used to:
7.1.1. Maintain a safe environment.
7.1.2. Ensure the welfare of pupils, staff and visitors.

7.1.3. Deter criminal acts against persons and property.
7.1.4. Assist the academy and police in identifying persons who have committed an offence.

8. Protocols

8.1. The surveillance system will be registered with the ICO in line with data protection legislation.

8.2. The surveillance system is a closed system which does not record audio.

8.3. Warning signs have been placed throughout the premises where the surveillance system is active, as mandated by the ICO's Code of Practice. See section 9 for additional information.

8.4. The surveillance system has been designed for maximum effectiveness and efficiency; however, the academies cannot guarantee that every incident will be detected or covered and 'blindspots' may exist.

8.5. The surveillance system will not be trained on individuals unless an immediate response to an incident is required.

8.6. The surveillance system will not be trained on private vehicles or property outside the perimeter of the academy.

9. Signage

9.1. The ICO confirm that for academies to ensure their CCTV in operation signs are GDPR compliant, they should:

9.1.1. Ensure signage is clear and visible, e.g. outdoor signs are not covered by overhanging branches.
9.1.2. Ensure signage is an appropriate size, e.g. if the CCTV is located near a drop off point it needs to be big enough for driver to see it from inside a car.
9.1.3. Ensure, if it captures images outside the academies site, signs are clearly displayed for pedestrians.
9.1.4. Ensure staff know who to talk to if they get asked about the images captured on CCTV.

9.2. Furthermore, when creating CCTV in operation signs, the wording used must include:

9.2.1. The details of the organisation operating the system.
9.2.2. The purpose of its use, e.g. crime prevention.
9.2.3. Who to contact if individuals have any enquires pertaining to the images being captured by the CCTV, e.g. the data protection officer (DPO) or principal.

10. Security

10.1. Access to the surveillance system, software and data will be strictly limited to authorised operators and will be password protected.

10.2. The main control facility is kept secure and locked when not in use.

10.3. If, in exceptional circumstances, covert surveillance is planned, or has taken place, copies of the Home Office's authorisation forms will be completed and retained.

10.4. Surveillance and CCTV systems will be tested for security flaws once a month to ensure that they are being properly maintained at all times.

10.5. Surveillance and CCTV systems will not be intrusive.

10.6. Any unnecessary footage captured will be securely deleted from the academies system.

10.7. Any cameras that present faults will be repaired as soon as possible to avoid any risk of a data breach.

10.8. Visual display monitors are located in secure areas where they cannot be overseen.

11. Privacy by design

11.1. The use of surveillance cameras and CCTV will be critically analysed using a Data Protection Impact Assessment (DPIA), in consultation with the DPO.

11.2. A DPIA will be carried out prior to the installation of any mew surveillance and CCTV system.

11.3. If the DPIA reveals any potential security risks or other data protection issues, the academy will ensure they have provisions in place to overcome these issues.

11.4. Where the academy identifies a high risk to an individual's interests, and it cannot be overcome, the academy will consult the ICO before they use CCTV, and the academy will act on the ICO's advice.

11.5. The academy will ensure that the installation of the surveillance and CCTV systems will always justify its means.

11.6. If the use of a surveillance and CCTV system is too privacy intrusive, the academy will seek alternative provision.

12. Code of practice

12.1. The academy understands that recording images of identifiable individuals constitutes as processing personal information, so it is done in line with data protection principles.

12.2. The academy notifies all pupils, staff and visitors of the purpose for collecting surveillance data via notice boards, letters and emails.

12.3. CCTV cameras are only placed where they do not intrude on anyone's privacy and are necessary to fulfil their purpose.

12.4. All surveillance footage will be kept for up to six months for security purposes; the principal and the Data Protection Lead are responsible for keeping the records secure and allowing access.

12.5. The academy has a surveillance system for the purpose of the prevention and detection of crime and the promotion of the health, safety and welfare of staff, pupils and visitors.

12.6. The surveillance and CCTV system is owned by the academy and images from the system are strictly controlled and monitored by authorised personnel only. Please see appendix 1

12.7. The academy will ensure that the surveillance and CCTV system is used to create a safer environment for staff, pupils and visitors to the academy, and to ensure that its operation is consistent with the obligations outlined in data protection legislation.

12.8. The surveillance and CCTV system will:

- Be designed to take into account its effect on individuals and their privacy and personal data.
- Be transparent and include a contact point, the DPL, through which people can access information and submit complaints.
- Have clear responsibility and accountability procedures for images and information collected, held and used.
- Only keep those images and information for as long as required after six months.
- Restrict access to retained images and information with clear rules on who can gain access.
- Consider all operational, technical and competency standards, relevant to the surveillance and CCTV system and its purpose, and work to meet and maintain those standards in accordance with the law.
- Be subject to stringent security measures to safeguard against unauthorised access.
- Be regularly reviewed and audited to ensure that policies and standards are maintained.
- Only be used for the purposes for which it is intended, including supporting public safety, the protection of pupils, staff and volunteers, and law enforcement.
- Be accurate and well maintained to ensure information is up-to-date.

13. Access

13.1. Under the GDPR, individuals have the right to obtain confirmation that their personal information is being processed.

13.2. All disks containing images belong to, and remain the property of, the trust.

13.3. Individuals have the right to submit an SAR to gain access to their personal data in order to verify the lawfulness of the processing.

13.4. The academy will verify the identity of the person making the request before any information is supplied.

13.5. A copy of the information will be supplied to the individual free of charge; however, the academy may impose a ‘reasonable fee’ to comply with requests for further copies of the same information.

13.5.1. Where an SAR has been made electronically, the information will be provided in a commonly used electronic format.
13.5.2. Requests by persons outside the academy for viewing or copying disks, or obtaining digital recordings, will be assessed by the principal, who will consult the DPO, on a case-by-case basis with close regard to data protection and freedom of information legislation.
13.5.3. Where a request is manifestly unfounded, excessive or repetitive, a reasonable fee will be charged.
13.5.4. All fees will be based on the administrative cost of providing the information.
13.5.5. All requests will be responded to without delay and at the latest, within one calendar month of receipt.
13.5.6. In the event of numerous or complex requests, the period of compliance will be extended by a further two months. The individual will be informed of this extension and will receive an explanation of why the extension is necessary, within one month of the receipt of the request.
13.5.7. Where a request is manifestly unfounded or excessive, the academy holds the right to refuse to respond to the request. The individual will be informed of this decision and the reasoning behind it, as well as their right to complain to the ICO and to a judicial remedy, within one month of the refusal.
13.5.8. In the event that a large quantity of information is being processed about an individual, the academy will ask the individual to specify the information the request is in relation to.
13.5.9. It is important that access to, and disclosure of, the images recorded by surveillance and CCTV footage is restricted and carefully controlled, not only to ensure that the rights of individuals are preserved, but also to ensure that the chain of evidence remains intact, should the images be required for evidential purposes.
13.5.10. Releasing the recorded images to third parties will be permitted only in the following limited and prescribed circumstances, and to the extent required or permitted by law:

- The police – where the images recorded would assist in a specific criminal inquiry
- Prosecution agencies – such as the Crown Prosecution Service (CPS)
- Relevant legal representatives – such as lawyers and barristers
- Persons who have been recorded and whose images have been retained where disclosure is required by virtue of data protection legislation and the Freedom of Information Act 2000

13.6. Requests for access or disclosure will be recorded and the principal will make the final decision as to whether recorded images may be released to persons other than the police.

Appendix 1

Staff members who are authorised to access and process data contained in the CCTV system and who have had appropriate training are:

Name	
Job Role	
Access Level (Full Admin, View, Copy, Live, etc.)	
Reason for access	
Cameras that can be accessed (Ref to camera list in Appendix 2)	

Appendix 2

Please list all cameras and locations, any camera not listed will be categorised as ‘Covert’:

Camera Number	**Location**	**Live / Live & Record / Record**
e.g. 001	e.g. Main Hall	e.g. L&R