Ormiston Academies Trust

Thomas Wolsey Ormiston Academy

CCTV policy

Policy version control

Policy type	Mandatory
Author	Alexandra Coughlan Data Protection and Complaints Manager Kevin Oldman Regional Estates Manager – South and East
Approved by	James Miller, May 2022
Release date	May 2022
Review	Policies will be reviewed in line with OAT's internal policy schedule and/or updated when new legislation comes into force
Description of changes	▪ Changes detailed in appendix 3

Contents

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 Trust's Academies and ensure that:

- The images captured are being handled in accordance with data protection legislation as set out under UK 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 Protection of Freedoms Act 2012
- The UK General Data Protection Regulation
- The Data Protection Act 2018
- 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:

- Amended surveillance camera code of practice 2021
- ICO (2022) 'Guide to the UK General Data Protection Regulation (UK GDPR)'
- 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.

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

4. Roles and responsibilities

4.1. Ormiston Academies Trust, as the corporate body, is the data controller. The CEO of the Trust therefore has overall responsibility for ensuring that records are maintained, including security and access arrangements in accordance with regulations, however this will be delegated to Principals.

4.2. The Data Protection Officer for the Trust is responsible for providing advice and guidance on any potential risks to the rights and freedoms of individuals

4.3. The Data Protection Lead deals with the day-to-day matters relating to data protection

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 equipment, 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.

5.7. The lawful bases we rely on to process CCTV footage are:

Article 6 (1) (e) Processing is necessary to perform a task in the public interest or for our official functions, and the task or function has a clear basis in law. Our basis in law is set out in:
- Section 175 of the Education Act 2002
- the Education (Independent School Standards) Regulations 2014
- the Non-Maintained Special Schools (England) Regulations 2015
- the Education and Training (Welfare of Children) Act 2021
- Keeping Children Safe in Education 2021
- the Health and Safety at Work etc Act 1974

Article 6 (1) (f) the processing is necessary for our legitimate interests unless there is a good reason to protect the individual's personal data which overrides those legitimate interests

6.Protocols

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

6.2. The surveillance system is a closed system which must not have the option to record sound enabled

6.3. 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 7 for additional information.

6.4. 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.

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

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

7.Code of practice

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

7.2. The Trust notifies all pupils, staff and visitors of the purpose for collecting surveillance data via a privacy notice which will be displayed on notice boards and on individual academy websites

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

7.4. 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.

7.5. 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.

7.6. 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

7.7. 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.

7.8. 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.

8. Right of Access

8.1. Under the UK GDPR, individuals have the right to obtain confirmation that their personal information is being processed in line with the data protection principles.

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

8.3. Individuals have the right to submit a Subject Access Request (SAR) to gain access to their personal data in order to verify the lawfulness of the processing.

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

8.5. 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.

8.5.1. Where an SAR has been made electronically, the information will be provided in a commonly used electronic format.

8.5.2. 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.

8.5.3. Where a request is manifestly unfounded, excessive or repetitive, a reasonable fee could be charged *however*

8.5.4. 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.

8.5.5. All fees will be based on the administrative cost of providing the information.

8.5.6. All requests will be responded to without delay and at the latest, within one calendar month of receipt.

8.5.7. 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.

8.5.8. 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.

8.5.9. 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.

8.5.10. 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

8.6. 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.

8.7. Due to differing timescales for retention of CCTV footage, it may not be possible to provide the requested footage as it may have been overwritten prior to the request being received.

8.8. The Data Protection Act 2018 that says a data controller does not have to comply with a SAR, if doing so means disclosing information which identifies another individual, except where the consent of that third party has been obtained OR where it is reasonable to comply without the consent of a third party. This could mean that it is not possible to comply with requests due to the inability to redact images of third parties successfully.

Appendix 1

9.Roles and Responsibilities

9.1. The role of the data controller includes:

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

9.2. The role of the principal includes:

9.2.1. Meeting with the relevant project lead to decide where CCTV is needed to justify its means.
9.2.2. Conferring with the DPO with regard to the lawful processing of the surveillance and CCTV footage.
9.2.3. Complete a DPIA to ensure all risk have been identified and mitigated sufficiently

9.3 The role of the DPO includes:

4.5.1 Monitoring legislation to ensure the academy is using surveillance fairly and lawfully.
4.5.2 Communicating any changes to legislation with the Trust.
4.5.3 Advising on the appropriate lawful basis for processing CCTV footage
4.5.4 Assisting with the completion of a DPIA
4.5.5 Assisting with the completion of a legitimate interests assessment where necessary

9.4 The role of the DPL includes:
9.4.1 Administering requests for CCTV footage
9.4.2 Ensuring records of all viewing requests are kept up to date
9.4.3 Ensuring footage is deleted in line with stated retention periods

10. Signage

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

10.1.1. Ensure signage is clear and visible, e.g. outdoor signs are not covered by overhanging branches.
10.1.2. 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.
10.1.3. Ensure, if it captures images outside the academy's site, signs are clearly displayed for pedestrians.
10.1.4. Ensure staff know who to talk to if they get asked about the images captured on CCTV.

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

10.2.1 The details of the organisation operating the system.
10.2.2 The purpose of its use, e.g. crime prevention.
10.2.3 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.

11 Security

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

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

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

11.4 Surveillance and CCTV systems will not be intrusive.

11.5 Any unnecessary footage captured will be securely deleted from the academy's system.

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

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

11.8 The ICO surveillance checklist will be completed annually and kept on file

11.9 When CCTV is viewed, downloaded or extracted from the system, a record will be made in the CCTV log which details time, date, reason, who the footage was shared with and in what format it was provided.

12 Privacy by design

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

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

12.3 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.

12.4 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.

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

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

13 Access

13.1 Options for responding where the academy does not have redaction technology could include:

Inviting the data subject and/or their representative in to view the footage while manually redacting third parties

Providing a still of the footage with third parties manually redacted

Obtaining consent from third parties

Refusing to comply with the request

14 Authorised Users

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

Name	Ian Lipman
Job Role	Operations Manager
Access Level (Full Admin, View, Copy, Live, etc.)	Full admin
Reason for access	System administrator, camera setup and maintenance
Cameras that can be accessed (Ref to camera list in Appendix 2)	All
Name	Alex Rose

Job Role	ICT Manager
Access Level (Full Admin, View, Copy, Live, etc.)	Full admin
Reason for access	System administrator, camera setup and maintenance
Cameras that can be accessed (Ref to camera list in Appendix 2)	All

Appendix 2 List of cameras

Please list all cameras and locations

Camera Number	Location	Live / Live & Record / Record
	Reception	Live and Record
	Community Entrance	Live and Record
	Pupil Entrance	Live and Record

Appendix 3

Old Section	New Section	Change
1	1	GDPR changed to UK GDPR
2	2	2.1 removed reference to RIPA General data protection regulation changed to UK….. 2.2 Home Office (2013) 'The Surveillance Camera Code of Practice' Changed to Amended surveillance camera code of practice 2021 ICO (2017) 'Overview of the General Data Protection Regulation (GDPR)' changed to ICO (2022) 'Guide to the UK General Data Protection Regulation (UK GDPR)' ICO (2017) 'Preparing for the General Data Protection Regulation (GDPR) 12 steps to take now' removed
3	3	3.2 'covert surveillance will only be operable in extreme circumstances' removed
4	4	4.1 Academy name changed to Ormiston Academies Trust Principal changed to CEO…however this is delegated to Principals 4.2 DPO role included 4.3 now DPL role Original 4.3 and 4.4 now moved to appendix 1 section 9
5	5	5.7 lawful bases added
6		removed
7		removed
8	6	6.2 now says 'must not have the option to record sound enabled'
9		Appendix 1 Section 10
10		Appendix 1 section 11
11		Appendix 1 section 12
12	7	7.2 now says via a privacy notice 7.4 school to complete retention period
13	8	8.1 changed to UK GDPR 8.7 new section

		8.8 new section
Appendix 1	Appendix 1	9.4 added in 10 added in 11 schools to complete highlighted sections 12 added in 13 added in
Appendix 2	Appendix 2	Removed reference to covert cameras