



.....

CCTV

POLICY

.....

This policy will be kept up to date and will be reviewed once per year as part of the company's Quality Assurance arrangements.

Review Period
1 Year

Approved by
Directors/Governors

Review Carried Out By
Quality Team

Date of Approval
August 2019

CCTV Policy

Introduction

Orion uses Close Circuit Television (CCTV) on its site to reduce crime and monitor the school buildings in order to provide a safe and secure environment for students, staff and visitors, and to prevent the loss or damage to school property, also to help prevent crime and assist law enforcement agencies in apprehending offenders.

This policy applies to all members of staff, students, visitors and all other persons whose images may be captured by the CCTV system.

This policy takes account of all applicable legislation and guidance including:

- General Data Protection Regulation ("GDPR")
- Data Protection Act 2018 (together the Data Protection Legislation)
- CCTV Code of Practice produced by the Information Commissioner
- Human Rights Act 1998

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
- Taking action to prevent a crime
- Using images of individuals that could affect their privacy

Legal Framework

This policy has due regard to legislation and statutory guidance, 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 (GDPR)
- The Data Protection Act 1998
- The Freedom of Information Act 2000
- The Education (Student 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

Statutory and Non-statutory guidance

This policy has been created with regard to the following statutory and no statutory guidance:

- Home Office (2013) 'The Surveillance Camera Code of Practice'
- Information Commissioner's Office (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'

Definitions

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.

Orion does not condone the use of covert surveillance when monitoring the school's staff, students and/or visitors. Covert surveillance will only be operable in extreme circumstances. Any overt surveillance footage will be clearly signposted around the school.

Positioning of Camera

All CCTV cameras will be sited in such a way as to meet the purpose for which the CCTV is operated. Cameras will be sited in prominent positions where they are clearly visible to staff, students and visitors.

Cameras will not be sited, so far as possible, in such a way as to record areas that are not intended to be the subject of surveillance. Orion will make all reasonable efforts to ensure that areas outside of Orion's premises and grounds are not recorded.

Signs will be visible to inform individuals that they are in an area within which CCTV is in operation.

Cameras will not be sited in areas where individual have a heightened expectation of privacy, such as changing rooms or toilets. Cameras may be located in classrooms and where this is

the case the staffs and students will all be aware. Access to the footage is restricted and will only be used to fulfil the purposes stated in the introduction.

Privacy Impact Assessment

Prior to the installation of any CCTV camera, or system, a privacy impact assessment will be conducted by the school to ensure that the proposed installation is compliant with legislation and ICO guidance.

The school will adopt a privacy by design approach when installing new cameras and systems, taking into account the purpose of each camera so as to avoid recording and storing excessive amounts of personal data.

Security Access

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

The school's authorised CCTV system operators are:

- Head of School (Murett Mendez)
- Designated Safeguarding Lead (Elizabeth Caldicott)
- Data controller (Georgina Mendez)

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

Surveillance and CCTV systems will be tested for security flaws annually to ensure that they are being properly maintained at all times. Surveillance and CCTV systems will not be intrusive. The Head of School will decide when to record footage, e.g. a continuous loop will be recorded at each location, any unnecessary footage captured will be securely deleted from the school system. Any cameras that present faults will be repaired immediately as to avoid any risk of a data breach.

Under the GDPR, individuals have the right to obtain confirmation that their personal information is being processed. All disks containing images belong to, and remain the property of, the school.

Individuals have the right to submit an SAR (Data, Subject Access request) to gain access to their personal data in order to verify the lawfulness of the processing. The school will verify the identity of the person making the request before any information is supplied. A copy of the information will be supplied to the individual free of charge; however, the school may impose a 'reasonable fee' to comply with requests for further copies of the same information.

Where an SAR has been made electronically, the information will be provided in a commonly used electronic format. Requests by persons outside the school for viewing or copying disks, or obtaining digital recordings, will be assessed by the Head of School.

Where a request is manifestly unfounded, excessive or repetitive, a reasonable fee will be charged. All fees will be based on the administrative cost of providing the information. All requests will be responded to without delay and at the latest, within one month of receipt.

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.

Where a request is manifestly unfounded or excessive, the school 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.

In the event that a large quantity of information is being processed about an individual, the school will ask the individual to specify the information the request is in relation to. 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. 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

Requests for access or disclosure will be recorded the Head of School will make the final decision as to whether recorded images may be released to persons other than the police.

Code of practice

Orion understands that recording images of identifiable individuals constitutes as processing personal information, so it is done in line with data protection principles. The school notifies all students, staff and visitors of the purpose for collecting surveillance data via signs in the school grounds where cameras are based.

CCTV cameras are only placed where they do not intrude on anyone's privacy and are necessary to fulfil their purpose. All surveillance footage will be kept for 14 days/One month for security purposes; the Head of School is responsible for keeping the records secure and allowing access. The school 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, students and visitors.

The surveillance and CCTV system are owned by the school and images from the system are strictly controlled and monitored by authorised personnel only. The school will ensure that the surveillance and CCTV system are used to create a safer environment for staff, students and visitors to the school, and to ensure that its operation is consistent with the obligations outlined in data protection legislation.

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 Head of School), through which people can access information and submit complaints.
- Have clear responsibility and accountability procedures for images and information collected, held and used.
- Have defined policies and procedures in place which are communicated throughout the school.
- Only keep images and information for as long as required.
- 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 students, staff and volunteers, and law enforcement. Be accurate and well maintained to ensure information is up-to-date

Responsibilities

The Head of School will:

- Ensure that the use of CCTV systems is implemented in accordance with the policy set down by Orion.
- Oversee and co-ordinate the use of CCTV monitoring for safety and security purposes within Orion.

- Ensure that all existing CCTV monitoring systems will be evaluated for compliance with this policy
- Ensure that the CCTV monitoring at Orion is consistent with the highest standards and protections
- Review camera locations and be responsible for the release of any information or recorded CCTV materials stored in compliance with this policy
- Maintain a record of access (e.g. an access log) to or the release of tapes or any material recorded or stored in the system
- Ensure that monitoring recorded tapes are not duplicated for release
- Ensure that the perimeter of view from fixed location cameras conforms to this policy both internally and externally
- Approve the location of temporary cameras to be used during special events that have particular security requirements and ensure their withdrawal following such events.
- Give consideration to both students and staff feedback/complaints regarding possible invasion of privacy or confidentiality due to the location of a particular CCTV camera or associated equipment
- Ensure that all areas being monitored are not in breach of an enhanced expectation of the privacy of individuals within the school and be mindful that no such infringement is likely to take place
- Co-operate with the Health & Safety Officer (Azim Kazi) in reporting on the CCTV system in operation in the school
- Ensure that monitoring tapes are stored in a secure place with access by authorised personnel only
- Ensure that images recorded on tapes/DVDs/digital recordings are stored for a period not longer than 28 days and are then erased unless required as part of a criminal investigation or court proceedings (criminal or civil).
- Ensure that camera control is solely to monitor suspicious behaviour, criminal damage etc. and not to monitor individual characteristics
- Ensure that camera control is not infringing an individual's reasonable expectation of privacy in public areas

