CCTV Policy

Local Procedures

Aurora Meldreth and Orchard Manor

Please refer to Group CCTV Policy A114

Local procedure

This local procedure is to set out the Meldreth and Orchard Manor site's approach to the operation, management and usage of surveillance and closed-circuit television (CCTV) systems on the site property.

Statement of intent

The purpose of the CCTV system is:

- To protect residents, staff and visitors against harm to their person and/or property.
- Make members of the site community feel safe.
- Deter criminality on the site.
- Protect the site's assets and buildings.
- Assist police to deter and detect crime.
- Assist in identifying, apprehending and prosecuting offenders
- Determine the cause of accidents.
- Assist in the effective resolution of any disputes which may arise during disciplinary and grievance proceedings.
- To assist in the defence of any litigation proceedings

The CCTV system will not be used to:

- Encroach on an individual's right to privacy.
- Monitor people in spaces where they have a heightened expectation of privacy (including toilets and changing rooms)
- Follow individuals, unless there is an ongoing emergency incident occurring.
- Pursue any other purposes than the ones stated above.

The list of uses of CCTV is not exhaustive and other purposes may be or become relevant.

The CCTV system is registered with the Information Commissioner under the terms of the Data Protection Act 2018. The system complies with the requirements of the Data Protection Act 2018 and UK GDPR.

Footage or any information gleaned through the CCTV system will never be used for commercial purposes.

In the unlikely event that the police request that CCTV footage, be released to the media, the request will only be complied with when written authority has been provided by the police, and only to assist in the investigation of a specific crime.

The footage generated by the system should be of good enough quality to be of use to the police or the court in identifying suspects.

The purpose of this policy is to regulate the management, operation and use of the CCTV at the site.

Legislation

- UK General Data Protection Regulation
- Data Protection Act 2018
- Human Rights Act 1998
- European Convention on Human Rights
- The Regulation of Investigatory Powers Act 2000
- The Protection of Freedoms Act 2012
- The Freedom of Information Act 2000
- The Freedom of Information and Data Protection (Appropriate Limit and Fees) Regulations 2004
- The School Standards and Framework Act 1998

Guidance

- Surveillance Camera Code of Practice (2021)

Definitions

Surveillance: the act of watching a person or a place
CCTV: closed circuit television; video cameras used for surveillance.
Covert surveillance: operation of cameras in a place where people have not been made aware they are under surveillance.

Data Protection Impact Assessment

The service recognises that CCTV systems can be privacy intrusive.

For this reason, the service has carried out a data protection impact assessment with a view to evaluating whether the CCTV system in place is a necessary and proportionate means of achieving the legitimate objectives as set out in the Aurora Group CCTV Policy.

The result of the data protection impact assessment has informed the service's use of CCTV and the contents of this procedure.

Details and location of CCTV system

The CCTV system used by the service comprises of and are located at:

Camera Type	Location	Sound	Recording Capacity	Swivel/Fixed
Hikvision	Main entrance gate (right)	N	Y	F
	Orchard House Flats (pointing towards Manor Road Terraces)	N	Y	F
	Orchard House Flats (pointing towards the Hostel / House 17 carpark)	N	Y	F
	Plumtree building (pointing to the Arc main entrance)	N	Y	F
	Plumtree building (pointing to the Skills Development Centre entrance)	N	Y	F
	Workshop area (2 cameras, one pointing to the right of Workshop	N	Y	F

	courtyard, the other to the left)			
	Workshop store	N	Y	F
	Workshop joinery store	N	Y	F
	Workshop mower store	N	Y	F
	Main carpark (3 static cameras)	N	Y	F
	Main carpark (360 PTZ camera)	N	Y	S
	Indoor arena / overflow carpark (1 pointing to entrance in, the other a panoramic view inside)	N	Y	F
	Workshop area (pointing to the main carpark pedestrian gate)	N	Y	F
	Arc (pointing to the Arc main entrance)	N	Y	F
	Arc (pointing to the footpath towards main carpark)	N	Y	F
	Arc (pointing to Woodpecker flat entrance)	N	Y	F
	Peartree building (pointing to Kingfisher flat entrance)	N	Y	F
	Peartree building (pointing to Kingfisher flat conservatory entrance)	N	Y	F
	Peartree building (pointing to the driveway of Orchard Manor Flat 1/2)	N	Y	F
	Apple Tree building (pointing to the rear entrance of school)	N	Y	F
	Apple Tree building (pointing to the Apple Tree covered walkway)	N	Y	F
	Cherry Tree building (pointing to the Cherry Tree courtyard)	N	Y	F
	Cherry Tree building (pointing to the Cherry Tree rear entrance)	N	Y	F

CCTV cameras are installed in such a way that they are not hidden from view. Warning signs, as required by the Code of Practice of the Information Commissioner, are clearly visible on the site and make clear who is responsible for the equipment. Signs are predominantly displayed where relevant, so that staff, children/adults, 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.

CCTV cameras are not installed in areas in which individuals would have an expectation of privacy such as any internal spaces.

Cameras are not and will not be aimed off the site grounds into public spaces or people's private property.

Cameras are positioned to maximise coverage, but there is no guarantee that all incidents will be captured on camera.

Roles & Responsibilities

The Governing Board has the ultimate responsibility for ensuring the CCTV system is operated within the parameters of this policy and that the relevant legislation (as defined above) is complied with.

The Site Principal will:

- Take responsibility for all day-to-day leadership and management of the CCTV system.
- Liaise with the data protection officer (DPO) to ensure that the use of the CCTV system is in accordance with the stated aims and that its use is needed and justified.
- Ensure that the guidance set out in this policy is followed by all staff.
- Review the CCTV policy to check that the site is compliant with legislation.
- Ensure all persons with authorisation to access the CCTV system and footage have received proper training from the DPO in the use of the system and in data protection.
- Sign off on any expansion or upgrading to the CCTV system, after having taken advice from the DPO and considered the result of a data protection impact assessment.
- Decide, in consultation with the DPO, whether to comply with disclosure of footage requests from third parties.

The Data Protection Officer (DPO) will:

- Train all staff to recognise a subject access request.
- Deal with subject access requests.
- Monitor compliance with UK data protection law.
- Advise on and assist the site with carrying out data protection impact assessments.
- Act as a point of contact for communications from the Information Commissioner's Office.
- Conduct data protection impact assessments.
- Ensure data is handled in accordance with data protection legislation.
- Ensure footage is obtained in a legal, fair, and transparent manner.
- Ensure footage is destroyed when it falls out of the retention period.
- Keep accurate records of all data processing activities.
- Inform subjects of how footage of them will be used by the site, what their rights are, and how the site will endeavour to protect their personal information.
- Ensure that the CCTV system is not infringing on any individual’s reasonable right to privacy in public spaces.
- Carry out termly checks to determine whether footage is being stored accurately and being deleted after the retention period.
- Receive and consider requests for third-party access to CCTV footage.

The System Manager will:

- Take care of the day-to-day maintenance and operation of the CCTV system.
- Ensure the CCTV systems are working properly and that the footage they produce is of high quality so that individuals pictured in the footage can be identified.
- Oversee the security of the CCTV system and footage.
- Check the system for faults and security flaws six monthly.
- Ensure the data and time stamps are accurate six monthly.

System Management

Access to the CCTV system and data is password protected and kept in a secure area.

Access will only be given to authorised persons, for the purpose of pursuing the aims as outlined in the Statement of Intent above or if there is a lawful reason to access the footage.

The following members of staff have authorisation to access the CCTV footage:

- The Site Principal
- The Site Data Protection Lead
- The Site System Manager
- The Site Maintenance Team Leader
- Anyone with express permission of the Site Principal
- The Site Reception Team (view access only)

Staff with approved access is provided with individual logon details which allows them full access to view, record, snapshot, and store video footage.

Where a person other than those mentioned above, requests access to the CCTV data or system, a request for access should be submitted via the IT Team, stating the user's name, email address, the reason for the access, the level of access they require, and any shut-off date to stop them from accessing the system. The System Manager must satisfy him/herself of the identity and legitimacy of purpose of any person making such request. Where any doubt exists, access will be refused.

CCTV footage will only be accessed from authorised personnel's work devices, or from the visual display monitors.

Any visual display monitors will be positioned so only authorised personnel will be able to see the footage.

All members of staff who have access will undergo training to ensure proper handling of the system and footage.

Details of all visits to view and requests for access will be recorded in a system logbook including time/date of access and details of images viewed and the purpose for so doing.

Any member of staff who misuses the surveillance system may be committing a criminal offence and will face disciplinary action.

The CCTV system will be administered and managed by the Estates Officer who will act as System Manager and take responsibility for restricting access, in accordance with the principles and objectives expressed in the Aurora Group CCTV Policy. In the absence of the Systems Manager, the system will be managed by the Maintenance Team Leader.

The CCTV system is designed to be in operation 24 hours a day, 365 days a year, though the service does not guarantee that it will be working during these hours.

- The system is registered with the Information Commissioner's Office.
- The system will not record audio.
- Recordings will have date and time stamps. This will be checked by the system manager six monthly and when the clocks change.

CCTV images are not retained for longer than necessary, taking into account the purposes for which they are processed. Data storage is automatically overwritten by the system after a period of 14 days. Additionally, all access to the system is logged and saved for 90 days.

Recorded images will only be retained long enough for any incident to come to light (e.g., for a theft to be noticed) and the incident to be investigated. In the absence of a compelling need to retain images for longer (such as an ongoing investigation or legal action), data will be retained for no longer than 6 months.

The System Manager will check and confirm the efficiency of the system regularly and in particular that the equipment is properly recording and that cameras are functional. If the CCTV system is not working properly the System Manager will report the fault to the IT Team.

Cameras have been selected and positioned so as to best achieve the objectives set out in the Group CCTV Policy in particular by proving clear, usable images.

Details of all visits and visitors and requests to view images will be recorded in a CCTV Access log book including time/date of access and details of images viewed and the purpose for so doing which will be held by the Service Business Manager who will act as the Site Data Protection Lead.

The System Manager will ensure that the equipment is serviced periodically by a competent professional.

Complaints About the Use of CCTV

Any complaints in relation to the use of the CCTV system should be addressed to the Principal or DPO and should be made according to the site's complaints policy.

Requests for Access by the Data Subject

The Data Protection Act 2018 provides data subjects – those whose image has been captured by the CCTV system and can be identified – with the right to access data held about themselves, including those obtained by CCTV. Requests for such data should be made to the Site Principal.

Details of all subject access requests for images will be recorded on GDPR Sentry and in the CCTV Incident and Request Log that show the date of the disclosure, details of who was provided with the information (the name of the person and the organisation they represent), and why they required it.

Individuals wishing to make an SAR can find more information about their rights, the process of making a request, and what to do if they are dissatisfied with the response to the request on the ICO website.

Public Information

Copies of the Aurora Group CCTV Policy and this local procedure will be available to the public upon request.