CCTV Policy

Policy Reference:	*A114*
Version Number:	2
Applies to:	All services
Associated documents:	A65 Data Protection Policy and appendix Privacy notices A1 Child Protection Policy A2 Adult Safeguarding Policy
Approved by:	Data Protection Officer
Implementation date:	September 2024
Next review due by:	September 2026
This policy has been reviewed to ensure it promotes safeguarding and does not present barriers to participation or disadvantage any protected groups	

© The Aurora Group 2023

Summary of changes since previous version of policy

- Reviewed September 2025, no changes

1. Aims

This policy aims to set out the Aurora Group's approach to the operation, management and usage of surveillance and closed-circuit television (CCTV) systems on Aurora property.

1.1 Statement of intent

The purpose of the CCTV system is to:

- Make members of the Aurora service feel safe and reduce the fear of crime;
- Protect members of the service from harm to their person or to their property;
- Deter criminality in the service;
- Protect Aurora's buildings and assets;
- Assist the police in preventing and detecting crime;
- To assist in identifying, apprehending and prosecuting offenders;
- Determine the cause of accidents and other adverse incidents and prevent reoccurrence;
- Assist in the effective resolution of any disputes which may arise in the course of disciplinary and grievance proceedings;
- To assist in the defense of any litigation proceedings; and
- To assist in managing the service.

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 particular 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.

The service will treat the system, all information, documents and recordings (both those obtained and those subsequently used) as data protected under the Act.

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.

Warning signs, as required by the Code of Practice of the Information Commissioner will be clearly visible on the site and make clear who is responsible for the equipment.

2. Legislation and statutory requirements

This policy is based on:

2.1 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 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 Guidance

- Surveillance Camera Code of Practice (2021)

3. 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

The service: the Aurora school, college and/or residential home

4. Covert surveillance

Aurora does not condone the use of covert surveillance when monitoring the staff, residents, pupils and or volunteers. Covert surveillance will only be used in extreme circumstances, such as where there is suspicion of a criminal offence. If the situation arises where covert surveillance is needed (such as following police advice for the prevention or detection of crime or where there is a risk to public safety), a data protection impact assessment will be completed in order to comply with data protection law.

5. Location of the cameras

Cameras are located in places that require monitoring in order to achieve the aims of the CCTV system (stated in section 1.1).

Please see the service's local procedures for information regarding the location of cameras.

Wherever cameras are installed appropriate signs are displayed so that staff, students, residents, visitors and members of the public are made aware that they are entering and area covered by CCTV.

The signs identify the service as the data controller and operator of the CCTV system. The signs also contain contact details as well as a statement of purposes for which CCTV is used.

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

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

6. Roles and responsibilities

6.1 The Operations Director

The Operations Director has the ultimate responsibility for ensuring the CCTV system is operated within the parameters of this policy and that the relevant legislation (defined in section 2.1) is complied with.

6.2 The Service Lead

The Service Lead 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 service is compliant with legislation
- Ensure all persons with authorisation to access the CCTV system and footage have received proper training from the DPO and IT team 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 the IT team and taken into account 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

6.3 The Service Business Manager (SBM)

The SBM will:

- Train persons with authorisation to access the CCTV system and footage in the use of the system and in data protection
- Ensure all staff can recognise a subject access request and understand how to report and act on it
- Undertake data protection impact assessments
- Ensure data is handled in accordance with data protection legislation

© The Aurora Group 2023

- Ensure footage is obtained in a legal, fair and transparent manner
- Take care of the day-to-day maintenance and operation of the CCTV system
- Ensure footage is destroyed when it falls out of the retention period
- Keep accurate records of all data processing activities and make the records public on request
- Inform subjects of how footage of them will be used by the service, what their rights are, and how the service will endeavour to protect their personal information
- Report any issues where CCTV systems are not working properly to the IT team
- 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 in consultation with the DPO

6.4 The IT team

The IT team will:

- Ensure that the CCTV systems are working properly, that the equipment is properly recording, that the cameras are functional 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 termly
- Ensure the data and time stamps are accurate termly

6.5 The Data Protection Officer

The Data Protection Officer (DPO) will:

- Ensure persons with authorisation to access the CCTV system and footage have had training in the use of the system and in data protection
- Ensure all staff are trained to recognise and respond to a subject access request
- Monitor compliance with UK data protection law
- Advise on and assist the service with carrying out data protection impact assessments
- Act as a point of contact for communications from the Information Commissioner's Office
- Oversee and review 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 and make the records public on request
- Carry out annual checks to determine whether footage is being stored accurately, and being deleted after the retention period
- Consider requests for third-party access to CCTV footage and support services to respond appropriately

7. Operation of the CCTV system

The CCTV system will be operational 24 hours a day, 365 days a year.

© The Aurora Group 2023

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 termly and when the clocks change.

8. Storage of CCTV footage

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.

On occasion footage may be retained for longer than 14 days, for example where a law enforcement body is investigating a crime, to give them the opportunity to view the images as part of an active investigation. 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.

Recordings will be downloaded and encrypted, so that the data will be secure, and its integrity maintained, and so that it can be used as evidence if required.

The SBM will carry out termly checks to determine whether footage is being stored accurately and being deleted after the retention period. The DPO will audit this on an annual basis.

9. Access to CCTV footage

Access will only be given to authorised persons, for the purpose of pursuing the aims stated in section 1.1, or if there is a lawful reason to access the footage.

Any individuals that access the footage must record their name, the date and time, and the reason for access in the access log together with details of images viewed.

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

Access to the CCTV system and data shall be password protected and will be kept in a secure area.

9.1 Staff access

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

- The Service Lead
- The Operations Director
- The Data Protection Officer
- The system manager (the SBM and IT Lead)
- Anyone with express permission of the Service Lead

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

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

Where a person other than those mentioned above, requests access to the CCTV data or 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.

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

© The Aurora Group 2023

9.2 Subject access requests (SAR)

According to UK GDPR and Data Protection Act 2018, individuals have the right to request a copy of any CCTV footage of themselves.

Upon receiving the request, the service will implement our Subject Access Request policy and aim to provide verified requests within 30 days wherever possible. All staff have received training to recognise SARs.

When making a request, individuals should provide the service lead with reasonable information such as the date, time, and location the footage was taken to aid staff in locating the footage.

On occasion the service will reserve the right to refuse a SAR, if, for example, the release of the footage to the subject would prejudice an ongoing investigation.

Images that may identify other individuals need to be obscured to prevent unwarranted identification. The service will attempt to conceal their identities by blurring out their faces, or redacting parts of the footage. If this is not possible the service will seek their consent before releasing the footage. If consent is not forthcoming redacted still images may be released instead or the footage will be withheld.

Aurora reserves the right to charge a reasonable fee to cover the administrative costs of complying with an SAR that is repetitive, unfounded or excessive.

Footage that is disclosed in a SAR will be disclosed securely to ensure only the intended recipient has access to it.

Records will be kept on GDPR Sentry 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.

9.3 Third-party access

CCTV footage will only be shared with a third party to further the aims of the CCTV system set out in section 1.1 (e.g., assisting the police in investigating a crime).

Footage will only ever be shared with authorised personnel such as law enforcement agencies or other service providers who reasonably need access to the footage (e.g., investigators).

All requests for access should be set out in writing and sent to the service lead and the DPO.

The Aurora Group will comply with any court orders that grant access to the CCTV footage. Aurora will provide the courts with the footage they need without giving them unrestricted access. The DPO will consider very carefully how much footage to disclose and seek legal advice if necessary.

The DPO will ensure that any disclosures that are made are done in compliance with UK GDPR.

All disclosures will be recorded by the DPO.

9.4 Downloading Captured Data on to Other Media

In order to maintain and preserve the integrity of the data (and to ensure their admissibility in any legal proceedings), any downloaded media used to record events from the hard drive/cloud storage must be prepared in accordance with the following procedures: -

(a) Each downloaded media must be identified by a unique mark.

(b) Before use, each downloaded media must be cleaned of any previous recording.

(c) The System Manager will register the date and time of downloaded media insertion, including its reference.

(d) Downloaded media required for evidential purposes must be sealed, witnessed and signed by the System Manager, then dated and stored in a separate secure evidence store. If a downloaded media is not copied for the police before it is sealed, a copy may be made at a later date providing that it is then resealed, witnessed and signed by the System Manager, then dated and returned to the evidence store.

(e) If downloaded media is archived, the reference must be noted.

(f) If downloaded media is put onto a device, the device will be encrypted and password protected.

Images may be viewed by the police for the prevention and detection of crime and by the Systems Manager, his/her replacement and the Site Lead, the DPO and other authorised senior leaders. However, where one of these people may be later called as a witness to an offence and where the data content may be used as evidence, it shall be preferable if possible, for that person to withhold viewing of the data until asked to do so by the police.

A record will be maintained of the viewing or release of any downloaded media to the police or other authorised applicants.

Should images be required as evidence, a copy may be released to the police under the procedures described in this policy. Images will only be released to the police on the clear understanding that the downloaded media (and any images contained thereon) remains the property of the service and downloaded media (and any images contained thereon) are to be treated in accordance with Data Protection legislation.

The service also retains the right to refuse permission for the police to pass the downloaded media (and any images contained thereon) to any other person. On occasions when a Court requires the release of a downloaded media, this will be produced from the secure evidence store, complete in its sealed bag.

The police may require the service to retain the downloaded media for possible use as evidence in the future. Such downloaded media will be properly indexed and securely stored until needed by the police.

Applications received from outside bodies (e.g., solicitors or parents) to view or release images will be referred to the Data Protection Officer and a decision made by a Site Lead in consultation with the Data Protection Officer.

10. Data Protection Impact Assessment (DPIA)

The Aurora Group follows the principle of privacy by design. Privacy is taken into account during every stage of the deployment of the CCTV system, including its replacement, development and upgrading.

Aurora recognises that CCTV systems can be privacy intrusive.

The system is used only for the purpose of fulfilling its aims (stated in section 1.1).

When the CCTV system is implemented, replaced, developed, or upgraded a DPIA will be carried out to be sure the aim of the system is still a justifiable, necessary and proportionate means of achieving the legitimate objectives set out below.

The DPO will provide guidance on how to carry out the DPIA. The DPIA will be carried out by the School Business Manager in conjunction with the Site Lead.

Those whose privacy is most likely to be affected, including the those regularly accessing the service and neighbouring residents, will be consulted during the DPIA, and any appropriate safeguards will be put in place.

A new DPIA will be done annually whenever cameras are moved, or new cameras are installed.

If any security risks are identified in the course of the DPIA, the service will address them as soon as possible.

11. Data Security

- The system manager will be responsible for overseeing the security of the CCTV system and footage
- The system will be checked for faults once a term
- Any faults in the system will be reported as soon as they are detected and repaired as soon as possible, according to the proper procedure
- Footage will be stored securely and encrypted wherever possible
- The CCTV footage will be password protected and any camera operation equipment will be securely locked away when not in use
- Proper cyber security measures will be put in place to protect the footage from cyber attacks
- Any software updates (particularly security updates) published by the equipment's manufacturer that need to be applied, will be applied as soon as possible

12. Complaints

Complaints should be directed to the Service Lead and should be made according to the service's complaints policy.

13. Monitoring

The policy will be reviewed annually by the DPO to consider whether the continued use of a surveillance camera remains necessary, proportionate, and effective in meeting its stated purposes. Local procedures will also be renewed annually by the Service Lead.

© The Aurora Group 2023