

CCTV Policy

Local Procedures

Aurora Severnside School

Please refer to Group A114 CCTV Policy

Local Procedure

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:

Camera Type	Location	Sound	Recording Capacity	Swivel/Fixed
External	Front right of building	Disabled	Yes	Fixed
External	Front left of building	Disabled	Yes	Fixed
External	Rear left of building	Disabled	Yes	Fixed
External	Rear right of building	Disabled	Yes	Fixed
Internal	Main entrance	Disabled	Yes	Fixed
External	Main entrance	Disabled	Yes	Fixed
Internal	Admin corridor/meeting room	Disabled	Yes	Fixed
Internal	Admin corridor/staff room	Disabled	Yes	Fixed

Signs are displayed clearly across the site so that staff, students, visitors and members of the public are made aware that they are entering an area covered by CCTV.

The signs contain information that:

- Identifies the school as the operator of the CCTV system.
- Identifies the school as the data controller.
- Provides contact details for the school.

CCTV cameras are not installed in any internal areas and/or areas in which individuals would have an expectation of privacy such as toilets, changing facilities, etc.

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

System Management

Access to the CCTV system and data shall be password protected and will be kept securely by the School Business Manager.

The CCTV system will be administered and managed by the School Business Manager 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 Headteacher

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

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.

The Head Teacher 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 school 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 System Manager will:

- Take care of the day-to-day maintenance and operation of the CCTV system
- 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.

Footage will be retained for 14 days. At the end of the retention period, the files will be overwritten automatically.

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.

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

Access will only be given to authorised persons 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.

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

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

- The Head Teacher: Rachel Lynch
- The School Business Manager : Nikki Elliott
- Anyone with express permission of the Head Teacher

CCTV footage will only be accessed from authorised personnel's work devices, or from the visual display monitors. The CCTV system will be password protected on the personnel's work device and the password will be contained to only the user.

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

Complaints About the Use of CCTV

Complaints should be directed to the Head Teacher or the DPO and should be made according to the school'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 Head of School.

Details of all subject access requests for images will be recorded on GDPR Sentry and in the CCTV Incident and Request Log.

Public Information



Policy Ref: A114-SEV

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