CCTV Policy

Local Procedure

Aurora Boveridge College

Please refer to Group CCTV Policy A114

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
Wisenet	Main building reception	No	Yes	fixed
Wisenet	Main building – rear corridor	No	Yes	fixed
Unknown	External – fixed to tree facing main gates	No	Yes	fixed
Unknown	External – fixed outside science classroom (facing courtyard)	No	Yes	fixed
Unknown	External – fixed outside English classroom (facing courtyard)	No	Yes	fixed
Unknown	External – fixed outside maintenance office (facing carpark)	No	Yes	fixed

Signs are displayed on Main Gate, external front and rear entrance – main building, internal front/main reception area, external courtyard education area, so that staff, students, residents, visitors and members of the public are made aware that they are entering an area covered by CCTV.

The signs contain contact details as well as a statement of purpose for which CCTV is used.

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

System Management

Access to the CCTV system and data shall be password protected and will be kept in a secure area. Hardware located in the maintenance IT office which has restricted access, no access to onsite staff. This system is managed centrally and requests for access are raised with the central IT department.

The CCTV system will be administered and managed by the Vice Principal 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 Principal.

The CCTV system is designed to be in operation twenty-four hours each day of the year, though the service does not guarantee that it will be working during these hours.

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.

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 to best achieve the objectives set out in the Group CCTV Policy by proving clear, usable images.

Details of all visits and visitors and requests to view images will be recorded in a CCTV Access logbook including time/date of access and details of images viewed and the purpose for so doing which will be held by Vice Principal – Teams GDPR file (access restricted).

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.

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 Principal.

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

Public Information

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