




St Augustine's Catholic High School and Sixth Form

CCTV Policy

Approved		Date
Principal G T O'Connor		01.07.20
Cycle of Review:	3 years	
Next Review Date:	June 2023	



ST AUGUSTINE'S CATHOLIC HIGH SCHOOL AND SIXTH FORM

DEVELOPING THE WHOLE PERSON

CCTV POLICY

'For I know the plans I have for you, declares the LORD, plans for welfare and not for evil, to give you a future and a hope.'

Jeremiah 29:11

St Augustine's Catholic High School uses closed circuit television (CCTV) and the images produced to prevent or detect crime and to monitor the school buildings and grounds in order to provide a safe and secure environment for its pupils, staff and visitors, and to prevent loss or damage to school property and surrounds. This policy outlines the school's use of CCTV and how it complies with the General Data Protection Regulation; it is to be read in conjunction to the School's data protection policy.

Statement of Intent

1. CCTV System:
 - a. The systems comprise of a number of fixed cameras.
 - b. The system do not have sound recording capability enabled
 - c. The system is not linked to automated facial recognition or number plate recognition software thus all individuals' images are anonymous until viewed.
2. The CCTV system is owned and operated by the school, the deployment of which is determined by the school's Senior Leadership Team with the Principal having overall responsibility.
3. The CCTV is monitored from secure offices. The CCTV stores the images and is retained for a minimum of seven days to a maximum of 30 days. Access to the images is controlled by the school's Senior Leadership Team, Lourdes IT and the Pastoral Team.
4. The introduction of, or changes to, CCTV monitoring will be subject to consultation with Facilities Manager and Principal.
5. All authorised operators and employees with access to images are aware of these procedures that need to be followed when accessing the recorded images. Through this policy, all operators are made aware of their responsibilities in following the CCTV Code of Practice. The school's 'Data Controller' (Principal) will ensure that all employees are aware of the restrictions in relation to access to and disclosure of, recorded images by publication of this policy.

6. The school complies with the Information Commissioner's Office (ICO) CCTV Code of Practice to ensure that CCTV is used responsibly and safeguards both trust and confidence in its continued use. The Code of Practice is published at:

<https://ico.org.uk/media/for-organisations/documents/1542/cctv-code-of-practice.pdf>

7. The School's CCTV surveillance cameras are a passive technology that only records and retains images. They are not linked to automated decision making or facial or number plate recognition software.
8. CCTV warning signs are clearly and prominently placed at the main external entrance to the school, including further signage in other outdoor areas in close proximity to camera positions. Signs will contain details of the purpose for using CCTV. In areas where CCTV is used, the school ensures prominent signs are placed within the controlled area.
9. The original planning, design and installation of CCTV equipment endeavoured to ensure that the scheme will deliver maximum effectiveness and efficiency but it is not possible to guarantee that the system will cover or detect every single incident taking place in the areas of coverage
10. Cameras are sited so that they only capture images relevant to the purposes for which they are installed (described above) and care will be taken to ensure that reasonable privacy expectations are not violated.
11. The school will make every effort to position cameras so that their coverage is restricted to the school premises, which includes outdoor/indoor areas. The system design is sympathetic to the privacy of surrounding public and does not monitor public space outside the legitimate areas of interest for the School.
12. CCTV will not be used in classrooms but in limited areas within the school building that have been identified as not being easily monitored at all times.
13. Members of staff will have access to details of where CCTV cameras are situated on the premises.

Covert Monitoring

14. It is not policy to conduct 'Covert Monitoring' unless there are 'exceptional reasons' for doing so. Any such monitoring would be temporary and be justified as 'exceptional'. The covert surveillance activities of public authorities are governed by the Regulation of Investigatory Powers Act (RIPA) 2000. Such type of recording is covert and directed at an individual or individuals. The school may, in exceptional circumstances, determine a sound reason to covert monitor via CCTV. For example: Where there is good cause to suspect that an illegal or unauthorised action(s), is taking place, or where there are grounds to suspect serious misconduct; where notice about the monitoring would seriously prejudice the reason for making the recording. In these circumstances authorisation must be obtained from the Principal before any commencement of such covert monitoring.
15. Covert monitoring must cease as soon as necessary, such as following completion of an investigation. Cameras sited for the purpose of covert monitoring will not be used in areas which are reasonably expected to be private, for example toilet cubicles, changing areas etc.

Storage and Retention of CCTV images

16. Recorded data will not be retained for longer than is necessary. While retained, the integrity of the recordings will be maintained to ensure their evidential value and to protect the rights of the people whose images have been recorded.

17. All retained data will be stored securely at all times and permanently deleted as appropriate/required.
18. Recorded images will be kept for no longer than 30 days, except where there is lawful reason for doing so, such as discipline investigations. Images are deleted from the CCTV server.
19. Access to CCTV recorded images will be restricted to those staff authorised to view them and will not be made more widely available.
20. Access to stored images will only be granted in the case of an incident. To be viewed in the course of the incident's investigation.

Subject Access Requests (SAR)

21. Individuals have the right to request access to CCTV footage that constitutes their personal data, unless an exemption applies the General Data Protection Regulations.
22. All requests should be made directly to the school. The school will inform the Chair of Governors of the requests and must be reported on the school Subject Access Request Log. Individuals submitting requests for access will be asked to provide sufficient information to enable the footage relating to them to be identified. For example, date, time and location.
23. The school will respond to requests within one month of receiving the written request. All requests must be logged and stored securely.
24. Disclosure of information from surveillance systems must be controlled and consistent with the purpose(s) for which the system was established. When disclosing surveillance images of individuals, particularly when responding to subject access requests, the school will consider whether the identifying features of any of the other individuals in the image need to be obscured. In most cases the privacy intrusion to third party individuals will be minimal and obscuring images will not be required. However, consideration will be given to the nature and context of the footage.
25. The subject will be supplied with a copy of the information in a permanent form. There are limited circumstances where this obligation does not apply. The first is where the data subject agrees to receive their information in another way, such as by viewing the footage. The second is where the supply of a copy in a permanent form is not possible or would involve disproportionate effort, whereby the disproportionate effort may incur an administration fee.

Access to and Disclosure of Images to Third Parties

26. There will be no disclosure of recorded data to third parties other than to authorised personnel such as the Police and service providers to the school where these would reasonably need access to the data (e.g. investigators).
27. Requests for images and data should be made to the school directly.
28. The data may be used within the school's discipline and grievance procedures as required and will be subject to the usual confidentiality requirements of those procedures. Data transfer will be made securely and using encryption as appropriate.