Earlscliffe CCTV and Door Access Policy

Member of SLT responsible: Head Teacher
Date of review: September 2025
Date of next review: June 2026

1.0 Introduction

This policy governs the use of Closed-Circuit Television (CCTV) and the UniFi Door Access System at Earlscliffe, an international boarding school. It outlines the purpose of the systems, how data is collected and processed, and the rights of individuals in accordance with the UK General Data Protection Regulation (GDPR), the Data Protection Act 2018, and other relevant legislation.

2.0 Purpose of the Systems

Earlscliffe uses CCTV and a door access system in its legitimate interests to ensure the safety and security of its students, staff, and visitors, and to protect school property. The systems are used for the following specific purposes:

- To deter and assist in the prevention or detection of crime.
- To monitor security across the school campus.
- To control and manage access to buildings and specific areas.
- To identify actions that might result in disciplinary action for staff or students.

3.0 Data Controller and Data Protection Officer (DPO)

Earlscliffe is the Data Controller responsible for the processing of personal data collected by these systems. The school's designated Data Protection Officer (DPO) can be contacted for any queries or requests related to this policy at: dataprotection@earlscliffe.co.uk.

4.0 Scope of the Policy

This policy applies to all CCTV cameras and the door access system installed at Earlscliffe.

4.1 **CCTV Cameras**: External cameras are installed across the campus, and internal cameras are located in public spaces such as entrance halls, dining rooms, and kitchens. No cameras are installed in private areas such as bathrooms or individual bedrooms.

4.2 **Door Access System**: The UniFi door access system controls entry to school buildings and designated areas using facial recognition and unique user access permissions.

4.3 **CCTV Signage**: Clear and prominent signs will be placed at the entrance to each building and in other appropriate locations where CCTV is in operation. The signage will inform individuals that they are entering an area under surveillance, the purpose of the CCTV, and provide a contact email address for queries: cctv@earlscliffe.co.uk. For all formal data protection requests, please refer to this policy.

5.0 Data Protection Impact Assessment (DPIA)

Prior to the installation and ongoing use of CCTV and biometric door access, a **Data Protection Impact Assessment (DPIA)** has been conducted to assess necessity, proportionality, and risks to individuals' rights. This DPIA is reviewed annually and whenever significant changes to the system occur.

6.0 Consultation and Transparency

In line with ICO and DfE guidance, Earlscliffe has consulted with staff regarding the introduction of CCTV and the biometric door access system. This included an opportunity to raise concerns and provide feedback. Ongoing communication will be maintained through policy updates, newsletters, and staff/student briefings.

7.0 CCTV System Details

7.1 **Data Collection**: The UniFi CCTV system captures video footage of individuals and their actions. It also uses AI to recognise objects such as people, animals, and cars to trigger notifications for security purposes.

7.2 **Data Retention**: All CCTV camera footage is stored locally on-site for a period of 30 days, after which it is automatically deleted. Any footage that needs to be retained for a legitimate purpose, such as a criminal investigation or disciplinary proceeding, may be backed up to a secure cloud storage service.

7.3 **Live Viewing**: Live footage from the CCTV system is not routinely monitored, with the exception of the live feed from the door access system, which may be viewed by authorised staff (e.g. receptionists and house managers) for the sole purpose of managing and verifying access.

8.0 Door Access System Details

8.1 **Access Method**: The UniFi door access system uses facial recognition to allow authorised individuals entry to the buildings and doors to which they have been granted permissions. This biometric data is used for security and access control only. The photo is converted to data and cannot be accessed within the system.

8.2 **Biometric Consent**: In compliance with the **Protection of Freedoms Act 2012**, parental consent is required before processing biometric data of students under 18. Students also have the right to refuse the use of their biometric data, and alternative access methods will be provided if consent is not granted.

8.3 **Permissions**: All users are given appropriate access to the buildings and doors they require for their role or studies at the school.

8.4 **Access Logs**: Door access logs are retained for a maximum of **90 days**, after which they are automatically deleted unless required for investigation or safeguarding purposes.

9.0 Data Security and Access

9.1 **System Security**: All camera and door access data is stored locally on a secure system. Access to live feeds and recorded footage is strictly controlled and limited to trained and authorised staff.

9.2 **Staff Training**: Staff with access to the systems are provided with training to ensure compliance with GDPR and safeguarding principles.

9.3 **Audit Logs**: The UniFi system maintains a full audit log of all user activity, including who has accessed the system, viewed footage, or downloaded video files, to ensure accountability.

9.4 **Emergency Procedures**: The door access system includes emergency override functions for lockdowns or emergency releases. All such actions are logged for post-incident review.

10.0 Data Sharing and Third-Party Disclosure

Disclosure of images or data to third parties is limited and conducted only under the following conditions:

- To law enforcement agencies, upon receipt of a formal data request.
- To prosecution agencies, upon receipt of a formal data request. - To school staff in the context of disciplinary proceedings.
- To individuals requesting access to their own images, unless this would prejudice criminal investigations.

Data will not be shared with any third parties (including police) without an appropriate formal data request.

11.0 International Data Transfers

All data is stored locally in the UK, with evidential backups securely stored in a cloud service located within the EU. Data will not be transferred outside the UK/EU.

12.0 Limits on Use of CCTV and Covert Monitoring

- CCTV will not be used to monitor staff work performance.
- No cameras will be installed in areas of high privacy (e.g. toilets, changing rooms).
- Covert monitoring will only be used where there is a reasonable suspicion of crime or serious misconduct, and only where lawful, necessary, and proportionate.

13.0 Data Subject Rights

Under GDPR, individuals have the following rights:

- **Right to be Informed**: This policy provides the necessary details.
- **Right of Access**: You may request access to your personal data (including CCTV footage of yourself) by contacting the DPO at dataprotection@earlscliffe.co.uk.
- **Right to Object**: You may object to processing in certain circumstances.
- **Right to Erasure**: You may request deletion of retained data where there is no legitimate reason for continued processing.

Concerns may be raised directly with the DPO or with the Information Commissioner's Office (ICO).

14.0 Review of Necessity and Proportionality

This policy, along with the associated DPIA, will be reviewed annually to assess whether CCTV and door access systems remain necessary and proportionate. The review will include an evaluation of effectiveness, stakeholder feedback, and any emerging privacy risks.