D'OVERBROECK'S
OXFORD
A NORD ANGLIA EDUCATION SCHOOL

CCTV POLICY

Last reviewed:	September 2025
Next review due:	September 2027
Reviewed by:	Head of IT (UK) Operations Manager

1. Purpose

CCTV is used as part of the school's wider safeguarding framework. While it is not a substitute for the professional vigilance of staff, it provides additional reassurance in supporting the school's duty to keep children safe in education, in line with DfE guidance and Keeping Children Safe in Education (KCSIE).

This policy sets out the accepted use of CCTV in the workplace to ensure that d'Overbroeck's complies with its legal obligations and respects the individual privacy of its students, staff, contractors and visitors.

d'Overbroeck's uses CCTV in its legitimate interests to deter and assist in the prevention or detection of crime, monitor security and identify actions which might result in disciplinary action.

2. Operation of the system

All CCTV footage is stored securely, with access restricted to authorised staff only. Access is password-protected, monitored, and subject to encryption to ensure compliance with GDPR security requirements.

The CCTV monitoring system will be provided and operated in a way that is consistent with an individual's right to privacy.

Cameras are located across all sites at d'Overbroeck's, including boarding houses. These are located to ensure that expectations of privacy are respected. All cameras are recording 24 hours a day 7 days a week.

Signs are prominently displayed informing people that monitoring is in use.

At the Senior School site, small CCTV monitors are located in Reception so they are visible to the Receptionist on duty but not to passers-by.

Ordinarily, images are retained for 14 days. Routine access to images is restricted to specific members of staff within the IT and Facilities & Maintenance departments at d'Overbroeck's.

3. Legislative framework

The Data Protection Act 2018 and The General Data Protection Regulation 2018 (GDPR) cover the rights of individuals (data subjects) in respect of their personal data. Identifiable images of individuals are personal data.

The system is administered and managed by the school, who act as the Data Controller. This policy will be reviewed regularly, and should be read with reference to the school's Data Protection Policy and Privacy Notices which can be found on the school website. For further guidance, please visit the Information Commissioner's Office website.

The Human Rights Act 1998 enshrines 'respect for private and family life'.

4. Individual access rights

All requests to access CCTV footage are logged and retained for audit purposes.

This policy will be reviewed annually by the Head of IT and the Operations Manager, with input from the DSL to reflect changes in safeguarding and data protection law.

Information about CCTV use is communicated through the school website. This ensures transparency and that all stakeholders are aware of the purpose and scope of CCTV monitoring.

The Data Protection Act gives individuals the right to access personal information about themselves, including images.

Requests by individuals for access to a copy of video footage must be made in writing. External requests to review footage should be submitted via the electronic form Data Request Form – External Requests (available from the Policies page of the school website). The form must be completed in full and include as much information as possible, particularly:

- the date and time the images were recorded;
- the location of the camera;
- information to identify the individual if necessary; and
- proof of your identity.

Completed forms must be emailed to the Data Compliance Administrator (see section 10 below). If d'Overbroeck's cannot comply with the request, the reasons will be documented.

5. Process to be followed if footage of CCTV is required by staff

All internal requests by staff to review footage should be submitted via the electronic form Data Request Form - Internal Requests (available from the Data Protection section of the Staff handbook via SharePoint).

The form must be completed in full and emailed to the Data Compliance Administrator (see section 10 below). The Data Compliance Administrator will sign this off or, in some circumstances, pass this on to the Director of Operations for further authorisation depending on the nature of the request. All action taken will be recorded.

6. Third party access

Disclosure of images to third parties, is limited to the following:

- Law enforcement agencies (where the images recorded would assist in a specific criminal enquiry);
- Prosecution agencies;

- Appropriate members of d'Overbroeck's staff in the course of staff or student disciplinary proceedings or prospective proceedings to ensure compliance with the organisation's regulations and policies; and
- People whose images have been recorded and retained (unless disclosure to the individual would prejudice criminal enquiries).

Data should not be shared with any third parties (even police) unless the appropriate formal data requests have been issued to us.

7. Requests to prevent processing

The school has carried out a Data Protection Impact Assessment (DPIA) for the use of CCTV. This assessment is reviewed annually or when significant changes are made to the system, to ensure ongoing compliance with GDPR and safeguarding requirements.

In addition to rights of access, data subjects also have rights under the Data Protection Act to prevent processing (ie, monitoring and recording CCTV images) likely to cause substantial and unwarranted damage to that person.

If a data subject has any concerns regarding the operation of the CCTV system, the data subject should contact the Data Compliance Administrator in writing (see section 10 below) and register a 'request to prevent processing', stating the reason for the request. In some cases d'Overbroeck's may be unable to comply with the request. A copy of the request and response will be retained.

8. Retention and disposal

While images are ordinarily retained for 14 days, any images required for an ongoing investigation or disciplinary/court proceedings will be securely stored until the matter is concluded. Once no longer required, images will be securely deleted.

All CCTV recordings are accessed via the cloud.

9. Limits on use of CCTV and covert monitoring

The organisation will not use CCTV for monitoring the work of employees.

Areas where a high level of privacy is expected, such as toilets or changing rooms, will remain private.

Covert CCTV will only ever be set up for the investigation or detection of crime or serious misconduct. The use of covert CCTV will be justified only in circumstances where the investigator has a reasonable suspicion that the crime or serious misconduct is taking place and where CCTV use is likely to be a proportionate means of securing evidence.

10. Data Compliance Administrator

Any questions or requests relating to this policy should be directed to the Data Compliance Administrator, who can be emailed at tracy.roslyn@doverbroecks.com.

*