

CCTV POLICY

Last reviewed:	September 2019
Next review due:	September 2021
Reviewed by:	Facilities & Compliance Manager IT Manager HR Administrator

Purpose

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.

Operation of the system

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.

Ordinarily images are retained for 28 days. Routine access to images is restricted to specific members of staff within the IT and Facilities departments at d'Overbroeck's.

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 subject to review from time to time, and should be read with reference to the School's Data Protection Policy and Privacy Notices which can be found on our Website & Firefly. For further guidance, please review the Information Commissioner's CCTV Code of Practice <https://ico.org.uk/media/1542/cctv-code-of-practice.pdf>.

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

The Data Controller is d'Overbroeck's and Heather Bates is the School's Data Compliance Administrator, heather.bates@doverbroecks.com.

Individual access rights

The DPA gives individuals the right to access personal information about themselves, including images.

All requests for access to a copy of video footage by individuals should be made in writing to the Data Compliance Administrator heather.bates@doverbroecks.com. Requests for access to CCTV images must include:

- The date and time the images were recorded;
- The location of the camera;
- Information to identify the individual if necessary; and
- Proof of identity.

If d'Overbroeck's cannot comply with the request, the reasons will be documented.

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

All requests to review footage should be completed on a 'Data Request Form - Internal Requests' and sent to the Data Compliance Administrator heather.bates@doverbroecks.com. The form can be found on Firefly under Staff / HR / GDPR and must be completed in full. The Data Compliance Administrator will sign this off or, in some circumstances, pass this on for further authorisation depending on the nature of the request. All action taken will be recorded.

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 with any third parties (even police) unless the appropriate formal data requests have been issued to us.

Requests to prevent processing

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 be directed to the Data Compliance Administrator where a request to prevent processing is made, this will be considered by the Data Compliance Administrator. A copy of the request and response will be retained.

Retention and disposal

Unless required for evidential purposes or the investigation of crime or otherwise required by law, recorded images will ordinarily be retained for no longer than 28 days from the date of recording.

At the end of their useful life all images stored in whatever format will be erased securely and permanently.

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.

*