St Chad's College
Durham

Policy and Procedure for the use of CCTV

Contents

1. Introduction

i. St Chad's College ("the College") has in place a CCTV surveillance system ("the CCTV system") in its Main College buildings at 18 North Bailey, Durham, DH1 3RH. This policy details the purpose, use and management of the CCTV system at the College and details the procedures to be followed in order to ensure that the College complies with relevant legislation and the current Information Commissioner's Office CCTV Code of Practice.

ii. The College will have due regard to the Data Protection Act 2018, the General Data Protection Regulation (GDPR) and any subsequent data protection legislation, and to the Freedom of Information Act 2000, the Protection of Freedoms Act 2012 and the Human Rights Act 1998.

iii. This policy is based upon guidance issued by the Information Commissioner's Office: 'In the picture: A data protection code of practice for surveillance cameras and personal information'.1

iv. CCTV images are monitored and recorded in strict accordance with this policy.

2. Purposes of the CCTV system

i. The principal purposes of the College's CCTV system are as follows:
   a. to prevent, reduce, detect and investigate crime and other incidents of misconduct or unacceptable behaviour
   b. to improve the safety of staff, students and visitors

c. to assist in the investigation of suspected breaches of College regulations by staff or students that are likely to result in the instigation of disciplinary proceedings.

ii. The CCTV system will not be routinely monitored by staff on duty in reception, but it will be used to help them to monitor possible intruders or incidents to which they have been alerted and which may require a response.

iii. The live feed from the Bar will NOT be routinely monitored.2 It may be monitored if there is reasonable cause, but only with the permission of the Duty Officer and in consultation with the Bar President or cellarman on duty.

i. Bar staff may request that live feed is monitored if they are concerned about safety or security.

ii. The live feed from the Dining Hall will NOT be routinely monitored. It may be monitored if there is reasonable cause, but only with the permission of the Duty Officer and in consultation with the JCR President or another elected student representative where possible.

iii. The live feeds from the Bar or the Dining Hall may be monitored on an ad hoc basis if a serious incident has been reported.

3. CCTV System overview

i. The CCTV system is owned by the College and managed by the College and its appointed agents. Under current data protection legislation the College is the data Controller' for the images produced by the CCTV system. The College is registered with the Information Commissioner's Office and the registration number is Z1470934. The CCTV system is operated in such a way as to meet the requirements of the Data Protection Act and the Information Commissioner's guidance.

ii. The Finance & Operations Director is responsible for the overall management and operation of the CCTV system, including activities relating to installations, recording, reviewing, monitoring and ensuring compliance with this policy.

iii. The CCTV system operates across the communal (and semi-public) areas of the College. There are no cameras in residential corridors or Common Rooms.

iv. Signs are placed at all pedestrian entrances in order to inform staff, students, visitors and members of the public that CCTV is in operation. The signage indicates that the system is managed by the College and a 24 hour contact number is provided.

v. The Finance & Operations Director is responsible for ensuring that adequate signage is erected in compliance with the ICO CCTV Code of Practice.3

vi. Cameras are installed throughout the College to ensure that they cover communal areas of College premises as far as is possible.

vii. The CCTV system is operational and is capable of being monitored 24 hours a day, every day of the year.

4. Monitoring and Recording

i. Cameras are monitored in Reception, which is a secure area, staffed 24 hours a day.

ii. Images are recorded on computer and are located securely in the College. Recordings can be routinely accessed only by College Officers. Additional staff may be authorised by the Finance & Operations Director or the Principal to monitor cameras sited within

their own areas of responsibility on a view only basis. This may include elected student representatives as appropriate.

iii. The CCTV system allows monitoring via remote access. This facility will be used on rare occasions. The remote connection will be routed through, and access will be restricted by, the University Network (VPN access, CIS security and multi-factor authentication). Remote access will be strictly limited to College Officers (Principal, Vice-Principal and Finance and Operations Director).

iv. The cameras installed provide images that are of suitable quality for the specified purposes for which they are installed and all cameras are checked daily to ensure that the images remain fit for purpose and that the date and time stamp recorded on the images is accurate.

v. All images recorded by the CCTV System remain the property and copyright of the College.

vi. The CCTV system will not routinely be used for monitoring of staff activities. However, the College reserves the right to carry out such monitoring with the express permission of the Finance & Operations Director or the Principal and only in accordance with Part 3 of the IOC Employment Practices Code.4

vii. The use of covert cameras will be restricted to rare occasions, when a series of criminal acts have taken place within a particular area that is not otherwise fitted with CCTV. A request for the use of covert cameras will clearly state the purpose and reasons for use and the authority of the Finance & Operations Director and another College Officer will be sought before the installation of any covert cameras. Appropriate elected student representatives (members of the JCR Executive committee and/or members of the MCR Executive committee) will be notified of the College's intention to use covert surveillance. The Finance & Operations Director should be satisfied that all other physical methods of prevention have been exhausted prior to the use of covert recording.

viii. Covert recording will only take place if informing the individual(s) concerned would seriously prejudice the reason for making the recording and where there is reasonable grounds to suspect that illegal or unauthorised activity is taking place.

ix. All such monitoring will be fully documented and will only take place for a limited and reasonable period.

x. Covert recording will never be used in bathrooms, toilets or showers. It will only ever be used in student bedrooms with the explicit consent of the occupant(s), at their request, and at agreed times.

5. Compliance with Data Protection Legislation

i. The College seeks to operate its CCTV system in a manner that is consistent with respect for the individual's privacy.

ii. In its administration of its CCTV system, the College complies with the General Data Protection Regulation (GDPR) and the Data Protection Act 2018. Due regard is given to the data protection principles embodied in GDPR. These principles require that personal data shall be:

- processed lawfully, fairly and in a transparent manner;
- collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes;

- adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
- accurate and, where necessary, kept up to date;
- kept in a form which permits identification of the data subjects for no longer than is necessary for the purposes for which the personal data are processed;
- processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

iii. The College ensures it is responsible for, and able to demonstrate compliance with GDPR.

iv. Please see the College Privacy Notice for Individuals whose images are captured on CCTV.

6. Applications for disclosure of images Applications by individual data subjects:

i. Requests by individual data subjects for images relating to themselves ("Subject Access Request") should be submitted in writing to the Finance & Operations Director together with proof of identity. Further details of this process are detailed on the College's Information Compliance policy

ii. In order to locate the images on the College's system, sufficient detail must be provided by the data subject in order to allow the relevant images to be located and the data subject to be identified.

iii. Where the College is unable to comply with a Subject Access Request without disclosing the personal data of another individual who is identified or identifiable from that information, it is not obliged to comply with the request unless satisfied that the individual has provided their express consent to the disclosure, or if it is reasonable, having regard to the circumstances, to comply without the consent of the individual.

Access to and disclosure of images to third parties:

i. A request for images made by a third party should be made in writing to the Finance & Operations Director – using the appropriate form as required under GDPR

ii. In limited circumstances it may be appropriate to disclose images to a third party, such as when a disclosure is required by law, in relation to the prevention or detection of crime or in other circumstances where an exemption applies under relevant legislation.

iii. Such disclosures will be made at the discretion of the Finance & Operations Director, with reference to relevant legislation and where necessary, following advice from the University's Information Governance Team.

iv. Where a suspicion of misconduct arises and at the formal request of the investigating Officer, the Finance & Operations Director may provide access to CCTV images for use in staff disciplinary cases.

v. The Finance & Operations Director may provide access to CCTV images to Investigating Officers when sought as evidence in relation to student discipline cases.
vi. A record of any disclosure made under this policy will be held on the CCTV management system, itemising the date, time, camera, requester, authoriser and reason for the disclosure.

7. Retention of images

i. Unless required for evidential purposes, the investigation of an offence or as required by law, CCTV images will be retained for no longer than 30 days from the date of recording. Images will be automatically overwritten after this point.
ii. Where an image is required to be held in excess of the retention period referred to in 7.
iii. The Finance and Operations Director or their nominated deputy, will be responsible for authorising such a request.
iv. Images held in excess of the standard retention period will be reviewed on a three monthly basis; any images no longer required for evidential purposes will be deleted.
v. Access to retained CCTV images is restricted to the Finance & Operations Director and other persons as required and as authorised by the Finance & Operations Director

8. Monitoring Compliance

i. All staff involved in the operation of the College's CCTV System will be made aware of this policy and will only be authorised to use the CCTV System in a way that is consistent with the purposes and procedures contained therein.
ii. All staff with responsibility for accessing, recording, disclosing or otherwise processing CCTV images will be required to undertake data protection training.

9. Damage to, and misuse of, the CCTV system

i. Any staff member, student, or other member of College removing, damaging or tampering with any components of the CCTV system will be subject to disciplinary action.
ii. Unauthorised use of the system or accessing recordings without express permission will also be subject to disciplinary action.

10. Complaints procedure

i. Complaints concerning the College's use of its CCTV system or the disclosure of CCTV images should be made in writing to the Finance & Operations Director at chads.bursar@durham.ac.uk
ii. Any appeals against a decision of the Finance & Operations Director should be made in writing to the Principal: Dr Margaret Masson m.j.masson@durham.ac.uk

11. Policy review

i. The College's usage of CCTV and the content of this policy shall be reviewed annually by the Finance & Operations Director with reference to the relevant legislation or guidance in effect at the time. Additional reviews may take place as required.