CANTERBURY CHRIST CHURCH UNIVERSITY

POLICY ON THE USE OF CLOSED CIRCUIT TELEVISION SYSTEMS

1 Introduction

1.1 Canterbury Christ Church University ('the University') uses Closed Circuit Television ('CCTV') and similar surveillance systems to ensure site security and the safety of staff, students and visitors.

1.2 Legitimate concerns exist over the use of CCTV. To maintain general confidence, it is necessary to respect individual privacy and ensure adequate control and supervision of these systems, together with scrutiny of their operation.

1.3 As a user of CCTV, the University has an obligation to comply with the provisions of the General Data Protection Regulation (GDPR) and the Data Protection Act (DPA) 2018, as these systems invariably require the processing of personal data.

1.4 This Policy and the accompanying University Codes of Practice are based on the Information Commissioner's Code of Practice for the users of CCTV and similar surveillance equipment that monitors spaces to which the public have access[1].

1.5 The CCTV Scheme is registered with the Information Commissioner under the terms of the GDPR and DPA 2018 and operates to meet the requirements of the Data Protection Legislation and the Information Commissioner's Code of Practice.

1.6 The purposes of this Policy are to establish:

- the purpose of the scheme
- responsibility for the scheme, including the day-to-day management
- security and disclosure procedures

1.7 The Policy and the accompanying University Codes of Practice aim to aid users of CCTV systems in meeting their legal obligations. Compliance may be a consideration in the determination by the Information Commissioner as to whether the University has made proper use of CCTV. Therefore, the University will review compliance with the policy requirements on a periodic basis.

2 Purposes of the University CCTV System

2.1 CCTV monitoring systems are in use throughout the University's academic, administrative and residential sites.

2.2 CCTV systems operate to improve the safety and security of the University community. The benefits of operating CCTV for these purposes may include reduction of the fear of crime and the provision of a safer public

[1] 'CCTV Code of Practice' (June 2017) issued in accordance with Data Protection Act 1998 s51(3)(b)

environment for the benefit of those who live or work within University sites or are visitors to these sites.

2.3 The objectives of the University CCTV systems are to

2.2.1 Provide reassurance by enhancing community safety
2.2.2 Protect University buildings and their assets
2.2.3 Provide a deterrent to potential offenders
2.2.4 Facilitate the identification, apprehension and prosecution of offenders in relation to crime and public order
2.2.5 Provide and operate the system in a manner that is consistent with respect for the individual's privacy

2.4 The legal basis for processing the personal data is in the legitimate interests of the University.

3 Use of CCTV

3.1 CCTV monitoring systems may focus on the activities of particular people by directing cameras at an individual's activities. This may entail looking out for particular individuals or examining recorded CCTV images to find things out about the people in them, such as identifying an individual who may be engaged in an illegal activity or a witness to a particular action.

3.2 Use of CCTV for anything other than the most basic of surveillance will have to comply with the DPA, but not all their images will be covered in all circumstances. The basic principle is that surveillance entailing taking images concerning an identifiable person's activities is covered by the DPA. If a general scene is recorded without any incident occurring, and with no focus on any particular individual's activities, the images are not covered by the DPA.

3.3 The University will ensure the public is made aware of the presence of the system and its ownership by appropriate signage. This sets out the purposes for processing CCTV images, and identifies the University as responsible for processing those images.

3.4 Images captured on camera will be transmitted to the relevant Control Room, where they will be recorded for use in accordance with the accompanying Code of Practice on the Administration of the Control Room.

3.5 All means of recording images belong to, and remain the property of, the University.

3.6 Copyright of the images recorded by CCTV cameras is the property of Canterbury Christ Church University.

3.7 Materials obtained through CCTV will not be used for any commercial purpose. The material may be released to the media, following discussions with the Director of External Relations, the University Solicitor and the Police, for use in the investigation of a specific crime, but never for the purposes of entertainment.

3.8 There is currently no sound recording from any part of the CCTV system.

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

4 Managerial Responsibility

4.1 The CCTV installation is entirely owned by the University. Director of Estates and Facilities has strategic managerial responsibility for the CCTV scheme.

4.2 Operational management and maintenance responsibility lies with the Operational Manager.

4.3 The Operational Manager at each location is to ensure

- the CCTV is operated in accordance with this Policy and the accompanying Codes of Practice
- the operating procedures for the scheme have been complied with
- the purposes and objectives of the scheme are not exceeded
- the regular evaluation and assessment of the usage and efficiency of the system is carried out
- persons entering the University are notified that a CCTV scheme is in operation

4.4 The system is operational, and images are capable of being monitored, for twenty-four hours a day throughout the year.

4.5 The University Data Protection Officer is responsible for ensuring the University is compliant with the requirements of the GDPR and DPA 2018 for providing advice to members of the University.

5 Access by Individual Data Subjects

5.1 Requests by individual data subjects for disclosure of images relating to them should be submitted to the Operational Manager or the University Data Protection Officer using the appropriate form.

5.2 The University undertakes to respond within one month of receipt of fee and completed request form. The Operational Manager is responsible for meeting the request to provide the images.

5.3 All requests will be recorded, and records maintained. Where the request is denied, the reason will be documented.

5.4 A copy of all data requests will be forwarded to the University Data Protection Officer for information.

6 Access to and disclosure of images to third parties

6.1 There will normally be no disclosure of recorded images to third parties other than the Police. Where disclosure is made, it will be because the

images would assist in a specific criminal enquiry, or to identify a victim, witness or perpetrator in relation to a criminal incident.

6.2 All requests for access or disclosure will be made to the Operational Manager for the site concerned, identified in Section 4. A form for making the request is available from the Operational Manager and Data Protection Officer.

6.3 All requests will be recorded, and records maintained. Where the request is denied, the reason will be documented.

6.4 A copy of all data requests will be forwarded to the University Data Protection Officer for information.

7 Monitoring Compliance and Complaints Procedure

7.1 There is recognition that members of the University community and the public may have matters of concern in respect of CCTV operations.

7.2 Any individual who wishes to express a concern in respect of CCTV operations or University compliance should be address those in the first instance to the University Data Protection Officer.

7.3 The Data Protection Officer will provide advice and assistance to staff, students and visitors on all matters in relation to the GDPR and DPA 2018, and their individual rights.

7.4 The University Data Protection Officer can be contacted as follows:

Robert Melville
Assistant University Secretary
Canterbury Christ Church University
Rochester House
St George's Place
Canterbury
CT1 1UT
E-mail: dp.officer@canterbury.ac.uk
Telephone: 01227 767700

Further information about how CCCU processes personal data and your rights related to it, is in our Data Protection Policy at:
https://www.canterbury.ac.uk/privacy/universitypolicy

8 Media Enquiries

8.1 Any enquiries from the media about the use of CCTV should be referred to the Data Protection Officer.

9 Availability of CCTV Policy and Codes of Practice

9.1 The University Policy on the use of CCTV on University premises is available on the University website at:

http://www.canterbury.ac.uk/support/university-solicitor/data-protection/cctv-policy-and-code-of-practice.asp

9.2 A paper copy is available from the Data Protection Officer.

9.3 The University Policy is supported by Codes of Practice on

- Siting of CCTV Cameras
- Administration of the Control Room
- Handling Requests from Outside the University for CCTV Images

9.4 Other Codes of Practice may be issued should the need arise.

10 Breaches of the Policy and Code (including breaches of security)

10.1 Any breach of the Policy or Codes of Practice issued under the Policy by University staff will be investigated and appropriate disciplinary action taken, using the University's Disciplinary Procedure.

11 Approval and Review

11.1 The Senior Management Team approved this Policy.

11.2 The Data Protection Officer will monitor the operation of the Policy, the Codes of Practice and procedures to ensure compliance with legal obligations and the provisions of the code of practice issued by the Information Commissioner.

Reviewed and Updated July 2019