CANTERBURY CHRIST CHURCH UNIVERSITY

Code of Practice on the Siting of CCTV Cameras

Signage

1 The General Data Protection Regulation (GDPR) and the Data Protection Act (DPA) 2018 obligates the University, as the data controller, to comply with requirements relating to the fair processing of data when operating Closed Circuit Television ('CCTV') and similar surveillance systems. To be compliant, the University has to provide the following information to individuals, at the point of obtaining their images:

a) the identity of the person or organisation responsible for the scheme
b) the purposes of the scheme; and
c) details of whom to contact regarding the scheme.

2 This information should be provided by appropriate signage.

The Information Commissioner gives the following examples of good practice, adapted for use within the University

1 Where an image of a camera is not used on a sign - the following wording is recommended:

"Images are being monitored for the purposes of crime prevention and public safety. This scheme is controlled by Canterbury Christ Church University. For further information contact XXXXX-XXXXXX"

2 Where an image of a camera is used on a sign - the following wording is recommended:

"This scheme is controlled by Canterbury Christ Church University. For further information contact XXXXX-XXXXXX "

3 The University seeks to follow the recommendations of the Information Commissioner's Code of Practice with regard to signage:

- Signs are placed so the public are aware they are entering a zone covered by surveillance equipment.
- The signs are clearly visible and legible to members of the public.
- The size of signs will vary according to circumstances.

3 The contact point indicated on the sign should be available to members of the public during office hours. Employees staffing that contact point should be aware of the policies and procedures governing the use of this equipment.

Covert Surveillance

4 There is an exemption from the requirement to inform the data subject that their personal data is being processed where the purpose of the processing is

the prevention and detection of crime, or the apprehension and prosecution of offenders. However, it is important to note this only applies as far as compliance with the requirement to inform would prejudice the purpose of preventing and detecting crime.

5 On the authorisation of the University Solicitor, covert cameras may be used under the following circumstances where:

- informing the individual(s) concerned that recording was taking place would seriously prejudice the objective of making the recording; and
- there is reasonable cause to suspect that unauthorised or illegal activity is taking place or is about to take place.

6 In determining whether to engage in covert surveillance, it is necessary to:

- identify the specific criminal activity;
- identify the reasons for the need to use surveillance to obtain evidence of that criminal activity;
- assess whether the use of signs would prejudice success in obtaining such evidence;
- assess how long covert monitoring should take place, to make sure it is not carried out for longer than necessary

7 Any such covert processing will be carried out for a limited and reasonable period consistent with the objectives of making the recording and relate to the specific suspected unauthorised activity.

8 The decision to adopt covert recording will be documented and will set out how the decision to use covert recording was reached. A record of the decision will be kept.

9 Information obtained by covert surveillance for the prevention and detection of crime, or the apprehension and prosecution of offenders, must not be used for any other purpose.

Location of Cameras

10 Cameras should be situated so they will capture images relevant to the purpose for which the scheme has been established, including the physical conditions in which the cameras are located. When installing cameras, account must be taken of the light conditions in which the cameras are located.

11 Consideration needs giving to the siting and use of cameras so they do not record more information than necessary for the purposes for which they were installed. For example, cameras set up for the purpose of recording acts of vandalism in car parks should not overlook private residences. If the purpose of the scheme is the prevention and detection of crime, the cameras should be sited so facial images are captured.

12 Static cameras are not to focus on private homes, gardens and other areas of private property. The processing of such data is potentially a breach of the Human Rights Act 1998, concerning the right to privacy and family life.

13 Cameras should be properly maintained and serviced to ensure that clear images are recorded. A maintenance log is to be kept by the Operational Manager, which is to be retained for one year.

14 The Operational Manager is to establish in writing procedures to be followed when a camera is damaged which make clear who is responsible for

a) making arrangements for ensuring that the camera is repaired
b) ensuring that the camera is repaired within a specific period
c) monitoring the quality of the maintenance work
d) reporting the incident to the University's Insurance Officer

Approval and Review

15 The Senior Management Team approved this Code of Practice in 2006. The Code was reviewed and updated in July 2019 to take account of changes in data protection legislation.

16 The Data Protection Officer will monitor the Code of Practice to ensure compliance with legal obligations and the provisions of the code of practice issued by the Information Commissioner.