EDINBURGH NAPIER UNIVERSITY
CODE OF PRACTICE FOR
CCTV AND SIMLIAR SURVEILLANCE EQUIPMENT SYSTEMS

Introduction

The monitoring, recording, holding and processing of images and recordings of identifiable individuals constitutes personal data as defined by the UK General Data Protection Regulation (UK GDPR) and UK Data Protection Act 2018 (together referred to as "the Data Protection Legislation" below). This Code of Practice is intended to ensure that in its use of Closed Circuit Television (CCTV) and Body Worn Radio Audio Recordings (BWR), Edinburgh Napier University is fully compliant with the requirements of the Act, related and relevant legislation including the Human Rights Act, the CCTV Code of Practice for Surveillance Cameras and Personal Information published by the Office of the UK Information Commissioner (UK ICO) and established best practice in the management of CCTV, such as the Surveillance Camera Code of Practice. If at any time mobile cameras are employed, their use will also be governed by this Code of Practice.

1. Data Protection Legislation

Edinburgh Napier University will comply with the Data Protection principles contained in the Data Protection Legislation, any associated legislation and any future changes in legislation. The principles are the personal data shall be:

- processed lawfully, fairly and in a transparent manner in relation to the data subject.
- 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 (data minimisation).
- accurate and, where necessary, kept up to date.
- kept for no longer than is necessary.
- processed in a manner that ensures appropriate security using technical or organisational measures

2. Definitions

For the purposes of this Code of Practice, the following definitions will apply:

2.1 **'University'**
Edinburgh Napier University

2.2 **'CCTV'**
Edinburgh Napier University closed circuit television surveillance systems

2.3 **'Body Worn Radio' (BWR)**
The University's digitally encrypted secure radio TRBONet system operated by University Security Staff

2.4 **'CCTV and Similar Surveillance Equipment Systems (The Systems)'** means:

- Edinburgh Napier University closed circuit television surveillance systems
- The University's TRBONet Secure Radio system

2.6 **'Data Controller'**
Edinburgh Napier University

3. Ownership and Operation

3.1 The CCTV and Similar Surveillance Equipment systems, all recorded material and/or copyright are owned by Edinburgh Napier University. The Head of Hospitality and Facilities Services is the designated University officer having responsibility for the Systems and their operation. Operational responsibilities and management are delegated as necessary and appropriate.

3.2 The CCTV and TRBONet Systems are operated by Property & Facilities Services Security Department whose personnel are employed directly and trained by Edinburgh Napier University.

4. Scope of the Code

4.1 This Code of Practice is binding on:

- all employees and students of Edinburgh Napier University
- all employees of contracted out services

4.2 This Code applies also to all other persons who for whatever reason may be present on Edinburgh Napier University premises, grounds or in student residential accommodation.

5. The Code's principles

The following principles will govern the operation of the Systems:

5.1 The Systems will be operated fairly and lawfully and only for the purposes authorised by Edinburgh Napier University.

5.2 The Systems will be operated with due regard for the privacy and safety of individuals

5.3 Any changes to the purposes for which the CCTV and BWR systems are operated will require the prior approval of the Head of Hospitality and Facilities Services, who will consult as necessary with Governance Services and will be publicised in advance of any such changes being made.

6. Purposes for the CCTV and BWR systems

6.1 CCTV

6.1.1 CCTV has been installed by the University for the following purposes:

i) public safety and security of students and employees of the University, visitors to the University and members of the public passing through the University campuses and utilising University facilities, including car parks and EN[GAGE] sports facilities
ii) prevention and detection of crime and the reduction of the fear of crime generally
iii) provide emergency services assistance
iv) assist with health and safety
v) support insurance claims
vi) protect the physical environment
vii) gather evidence by a fair and accountable method for:
  a) investigations or complaints arising under the University's Disciplinary Procedure, Student Conduct Regulations or Complaints Handling Procedure; or
  b) investigations undertaken by Police Scotland in relation to any on Campus or Accommodation incident resulting in potential criminal proceedings
  c) investigations under the Student Accommodation Code of Practice and/or of alleged breaches of a student tenancy agreement.

6.2 TRBONet Radio Systems (BWR)

6.2.1 The facility to make BWR recordings is intended primarily as a deterrent in serious cases of aggressive and abusive behaviour towards a member of the University's Security Staff. Recordings will only be made as a last resort and in certain strictly limited situations, in accordance with this Code and the specific Guidance for their use.
6.2.2 Where a recording is made in accordance with 6.2.1 above, this may be used for:

i) the detection of an alleged criminal offence
ii) investigations or complaints arising under the University's Disciplinary Procedure, Student Conduct Regulations or Complaints Handling Procedure
iii) investigations under the Student Accommodation Code of Practice and/or of alleged breaches of a student tenancy agreement

7. Covert Surveillance

7.1 Covert surveillance will only be used in exceptional and limited circumstances. Any such request must be submitted in writing and referred to the Director of Property & Facilities or their nominee who will consult with the Data Protection Officer, University Secretary and the Director of People and Services as appropriate.

7.2 Covert surveillance may only be used if all of the following criteria are met:

- Its use is part of a specific investigation
- There are grounds for suspecting criminal activity or equivalent malpractice
- The use of CCTV is the only reasonable way to investigate the matter
- Informing people about the monitoring would impede the effectiveness of the monitoring.
- The cameras are not in 'private areas' such as toilets or individual offices (except in the case of suspected serious crime with the intention of involving the police).

Covert surveillance must cease as soon as the investigation is complete.

7.2 For the avoidance of doubt, the use of BWR for covert surveillance is strictly prohibited.

8. Related signage, privacy notices and verbal warnings

8.1 CCTV

Visible and legible signs indicating the operation of CCTV Systems have been placed at the three main University Campuses. These signs indicate:

- the presence of such equipment
- the reasons for the equipment
- ownership of the system
- contact details

8.2 CCTV Installation

8.2.1 Any installation connected with the CCTV Systems must be appropriate to its purposes and comply with the requirements of this Code of Practice.
8.2.1 Cameras have been installed in such a manner as not to overlook private areas outwith the University's boundaries.
8.2.2 Where it is proposed to upgrade current CCTV systems or install new systems, a Privacy Impact Assessment must be carried out.

8.3 BWR Recordings

8.3.1 All Security Staff must ensure that the required verbal warnings about the making of audio recordings are given in accordance with the Operational Guidance and that appropriate signage is worn on their person.

8.3.2 References to the use of BWR recordings has been included in relevant privacy notices and the Staff and Student Privacy Notices.

9. Processing the Systems Data

9.1 This must be done strictly in accordance with Data Protection legislation. Access to, and disclosure of, images and recordings is restricted and carefully controlled to safeguard the rights of individuals and ensure that evidence remains intact, should the images or recordings be required for the evidential purposes referred to in 6.1 and 6.2 above.

9.2 Requests to view images and/or to listen to recordings will be managed in accordance with sections 12 and 13 below.

9.3 No persons other than authorised Security staff will be permitted to download personal data from either CCTV or BWR systems and this will be done strictly for the purposes stated in sections 12 and 13 below.

9.4 A log of those accessing recorded footage from the Systems will be kept to ensure there is an audit trail.

10. Retention and use of recorded material on CCTV Systems

10.1 In accordance with the fifth principle, recorded material will not be kept for longer than the purpose for which it is being retained.

10.2 Discs of CCTV images will be retained for 14 days on campuses and 28 days for accommodation sites and then deleted securely in accordance with the University's guidance on the Safe Disposal of Confidential Waste, unless a request under section 12 of this Code is made.

10.3 BWR audio recordings will be retained for a period of 14 days and then deleted as in 10.2 above unless a request under section 12 of this Code is made.

10.3 Still photographs may be generated from recordings made by the System only where these are required for evidential purposes by the University as referred to in 6.1 and 6.2 above, the police or other bodies with prosecuting powers or where appropriate in response to a formal subject access request.

10.4 Edinburgh Napier University reserves the right to use a recording made by the System and/or still images generated from such recordings in any civil prosecution brought by the University.

10.5 Where appropriate, the police may be asked to investigate any matter recorded by the System which is deemed to be of a potential criminal nature. Where we are aware of a specific incident for which CCTV footage would be key, Edinburgh Napier University reserves the right to store these images until such times as requested by Police Scotland, and deleted immediately thereafter.

10.6 Recordings and/or still images will only be authorised for use in potential staff or student disciplinary hearings following approval from the Director of People and Services or the Head of Student Accommodation or their nominee, in consultation with the Head of Hospitality and Facilities Services.

11. Retention and use of recorded material on BWR Systems

11.1 In accordance with the fifth data protection principle, recorded material will not be kept for longer than the purpose for which it is being made.

11.2 Recordings will be used and retained as required by Operational Guidance

12. Disclosure of personal data

The Data Protection legislation and the Freedom of Information Act (Scotland) Act 2002 will be strictly adhered to in handling requests for the disclosure of personal data. Requests made under either Act for CCTV images and/or BWR recordings, must be made to the Head, Campus Services or his/her deputy, who will consult as necessary with the Information Governance Manager.

12.1 Request by a data subject

12.1.1 Individuals have the right to access their personal data, which includes images captured by CCTV systems and recordings made by BWR. The data subject will be asked whether they would be satisfied with viewing the images or listening to the recordings held. This must be done strictly in accordance with Data Protection legislation and the provisions of sections 12.1.5 of this Code with regard to third party images or voices.

12.1.2 Where a request is made as a result of a data subject being a victim of a potential or actual criminal offence, they will be advised to contact the police in the first instance and obtain a crime reference number. The University will liaise with the police thereafter about any relevant footage or recording, in order not to prejudice or compromise a criminal investigation. The University reserves the right to retain these images outwith the 28 day retention period until such times as the police are able to accept the data and will be deleted immediately thereafter.

12.1.3 If a data subject wishes to have copies of their personal data held on either CCTV or BWR systems, any such request should be made to the Head of Hospitality and Facilities Services or their deputy and submitted with the following:

- details of the dates and times when they visited the University and their location e.g. which campus site and specific area or building. Data subjects may wish to use the University's standard request form
- two photographs of the data subject - one full face one side view with the completed form
- proof of the data subject's identity e.g. staff or student ID card, a utility bill, a driving licence or a passport
- in the case of a request for a BWR recording, any such additional relevant information as may reasonably be required by Security staff to enable a data subject's identity to be verified with reference to any recording being requested.

12.1.4 The University is not obliged to comply with a request made under s.12 unless it is supplied with the required documentation, is satisfied as to the identity of the data subject and can locate the personal data which the subject is seeking.

12.1.5 Where the University cannot comply with the request without disclosing the image or voice of another identifiable individual it is not obliged to do so unless:

- the other individual has consented to the disclosure of the information to the

person making the request; or
- it is reasonable in all the circumstances to comply with the request without the consent of the other individual.

12.1.6 Where a request is manifestly unfounded or excessive the University may charge a "reasonable fee" for the administrative costs of complying with the request. However, this would only apply in extremely limited circumstances and on the decision of the University's Data Protection Officer only.

12.1.7 A written decision on the request will be sent to the data subject within 21 days and if access to the images or recordings is to be provided, such access will be given within one month of the University receiving the request or if later, the date when the University receives the complete set of documentation and proof of identity from the data subject.

12.2 Requests from third parties

12.2.1 Requests made by the police or agencies with prosecuting powers to view personal data captured by the CCTV system and/or to listen to BWR recordings made, will be handled under Data Protection legislation. All other requests from third parties to view CCTV and/or to listen to BWR recordings will be treated as requests under the Freedom of Information (Scotland) Act 2002.

12.2.2 Requests to view CCTV and/or to listen to BWR recordings are likely to be made for any one or more of the following purposes:
- providing evidence to assist in criminal proceedings
- the investigation and/or detection of crime
- identification of witnesses
- illegal or unauthorised activity in/on or adjacent to University campus car parks and grounds
- providing evidence for civil proceedings or tribunals

12.2.3 The Police and other third parties will be required to show adequate grounds for disclosure of data within the above criteria and may include but are not limited to:
- Statutory authorities with powers to prosecute
- Solicitors
- Plaintiffs or authorised representatives in civil proceedings
- Accused persons or defendants in criminal proceedings, but subject strictly to 13.2.5 c) below

12.2.4 Requests for information must be submitted to the Head of Hospitality and Facilities Services, who will consult as necessary with the Data Protection Officer, University Secretary and Director of People and Services or their nominated direct report. Police and prosecuting authorities' requests must be accompanied by their relevant organisational form signed by the appropriate authorised officer(s) while other third parties will be required to submit their requests on letter headed notepaper and a form which complies with the University's requirements as provided in the online guidance. All those seeking disclosure should give:

- the authority under which the request is made
- reasonable proof of the requester's personal identity and organisational affiliation e.g. police officers will be expected to quote their identification numbers and/or produce their warrant cards
- details of the nature of the personal data requested, the purpose for which it is being requested and confirmation that the scope of the request is necessary and proportionate

- where applicable, the relevant DPA exemption or other legislation which authorises the University to release the information
- where applicable, a warranty that it will be held and processed in conformity with the Data Protection Principles

12.2.5 The Head of Hospitality and Facilities Services or deputy will consult as necessary with Governance Services to ensure:

a) No undue obstruction of any third party investigation to verify existence of data
b) The retention of data which may be relevant to a request
c) Where relevant, that the release of images or recordings will not compromise or prejudice a criminal investigation; and
d) The request is responded to within 20 working days

13. Location of Systems

13.1 CCTV images will be monitored and captured in the Security Control Room at the Merchiston Campus, other security offices on University campuses and in student residential accommodation.

13.2 BWR recordings will be made and held on the TRBONet secure system, which is hosted on University servers.

14. Access to and use of Security Control Room & offices with CCTV systems

14.1 Access to the University's monitoring and recording facilities will be prohibited except for lawful, proper and sufficient reasons (e.g. official visits from law enforcement or inspection agencies, security staff, senior management, authorised Student Accommodation Officers, external engineers effecting repairs and cleaning staff) and only then with the personal authority (verbal or written) of the Head of Hospitality and Facilities Services, or their nominated deputy.

14.2 Regardless of their status, all persons visiting the Security Control Room or other security offices with the purpose of viewing images, recorded data or audio recordings will be supervised at all times. A register of visitors will be maintained at each site for audit purposes. Any visits will be conducted and recorded in accordance with University Security procedures.

14.3 In the event of a major incident, such as bomb threats, explosions, serious fires, terrorism and/or serious public disorder, the police authorities will be authorised to access the Security Control Room, other security offices, or student residence offices to make use of CCTV facilities and/or to listen to BWR recordings. Such action will be agreed and authorised by the Facilities Services Manager or their nominated deputy.

15. Responsibilities

15.1 The Head of Hospitality and Facilities Services, or their nominated deputy, is responsible for the operation of the CCTV and BWR Systems and for ensuring compliance with this Code of Practice, in the first instance. Operational responsibilities and management are delegated as necessary and appropriate.

16. Breaches, Disciplinary Action & Complaints arising from use of the Systems

16.1 Any use of the Systems or recorded data that is not in compliance with this Code and is inconsistent with the objectives of the Systems, will be considered to be a breach of Edinburgh Napier University policy. Any breach to be reported in line with the guidance given online.

16.2 Persons found to have misused the Systems may be subject to Edinburgh Napier University's disciplinary procedures for staff or students. If any such misuse also constitutes a criminal offence or a breach of civil law then court proceedings may be commenced.

16.3 Complaints regarding the use, operation of and/or compliance with the Systems will be handled in accordance with Edinburgh Napier University's Complaints Handling Procedure and should be addressed to the Head of Hospitality and Facilities Services.

16.4 Complaints arising from a subject access request for CCTV and/or BWR images should be addressed in the first instance to:

The Head of Hospitality and Facilities Services Room 6 B. 22
Sighthill Campus
Edinburgh, EH11 4BN
Tel: 0131-455-3726

16.5 In the event that a data subject remains dissatisfied about the handling of their request they may write to:
The Data Protection Officer
c/o dataprotection@napier.ac.uk

16.6 Alternatively, a data subject has the right to appeal direct to the UK Information Commissioner (ICO), who has responsibility for overseeing the Act, about any aspect of the handling of their personal data by the University. The contact details for the ICO's Scottish office are:

UK Information Commissioner's Office
45 Melville Street
Edinburgh, EH3 7HL
Telephone: 0131 244 9001; Email: Scotland@ico.gsi.org.uk

17. Monitoring and Review

This Code of Practice will be kept under review. Any questions about its interpretation or operation should be referred to the Head of Hospitality and Facilities Services.

18. Public Information

This Code of Practice will be published on the University's intranet site and a copy made available on request.

Document Control Information	
Title	Code of Practice on CCTV and Similar Surveillance Equipment Systems
Version	v.3.0
Authors	Property & Facilities Services and Governance Services
Date Approved	By University Information Governance Group 20190219 By the University Secretary 20190221 By UIGG and the Convenor of RRC 27/10/2021 By UIGG and the Convenor of RRC 23/06/2022
Review Date	Biennially
Scope	All University employees, students, third party users of University premises & estate
Edinburgh Napier University acknowledges the use of some content from the University of Edinburgh's CCTV Policy.	