Bournemouth University	Document Title: Section: Procedure Location: Author: Reviewer: Version Number: Date Created / Last Amended: Amended By: Document Review:	CCTV Policy & Procedures Strategic Documents Estates / Private / Soft Services/Security/Policy Documents/CCTV Head of FM / Deputy Head of Legal Services Dir Estates Version 4 18/05/2022 Jim Evans/Brent Hatzer May 2023, then annually

BOURNEMOUTH UNIVERSITY
CCTV Policy & Procedures

CONTENTS

Section

Appendices

5.2 Requests for imagery from data subjects

5.2.1 Where operators or system administrators receive a request from a member of staff, a student or a visitor in relation to their personal data (images or sound recordings of them or associated with them, for example, of their car) recorded on a CCTV system, they should refer the matter to the Information Office, c/o Legal Services.

5.2.2 The contact details for paragraph 5.2.1 are:

E: dpo@bournemouth.ac.uk

T: 01202 961 315

Information Officer
Legal Services
Bournemouth University
Studland House
Christchurch Road
Bournemouth
Dorset

5.2.3 BU's Data Protection Policy applies equally to CCTV recordings as it does to other personal data.

5.3 Internal requests for imagery that is not own personal data

5.3.1 Any staff member who wishes to review a CCTV recording, for example, to investigate an incident, must approach the system administrator. System administrator details are set out in Paragraph 1.3 above and Appendix 1.

5.3.2 The staff member must explain the reason for the request, and must provide the reason in writing if required by the system administrator. The system administrator will decide whether the request is consistent with the purposes for which the CCTV system was operated. If satisfied on this front, the staff member will be permitted to view (and, if applicable, listen to) the recording.

5.3.3 Any dispute on access will be referred to the Legal Services department (legalservices@bournemouth.ac.uk) for advice. The requesting staff member and system administrator may be required to put their reasons in writing.

5.4 CCTV recording on permanent media

5.4.1 Other than system administrators, and operators under their direction, the only persons authorised to receive CCTV recordings on permanent media are:

- members of the Human Resources department authorised for these purposes by the Director of Human Resources Services;

- (recordings relating to students only) members of the Student Services and Student Administration departments responsible for student complaints and authorised for these purposes by, as the case may be, the Director of Student Services or Academic Registrar;

- the Director of Estates, the Head of Facilities Management, the Campus Services Manager (Facilities) and any other members of the Estates department authorised for those purposes by the Director of Estates;

- members of the Legal Services department and others authorised for those purposes by them, for example solicitors acting for the University's insurers;

- the University's Insurance Officer; and

- the police (where procedures below have been followed).

5.4.2 System administrators will comply with directions from any of the above for supply of relevant recordings. Any dispute over supply will be referred to Legal Services for resolution; and Legal Services will liaise with the University Executive Team as necessary.

5.5 Requests from the police to either see recordings or be supplied with recordings on permanent media

5.5.1 Unless there is a statutory duty to disclose, the University doesn't have to disclose information without a court order. Members of staff should not be bullied into disclosing personal data if there is any doubt as to the validity of the request. It is, however, the University's expectation that it will be able to work co-operatively with the police to promptly help them in the execution of their duty.

5.5.2 The police have standard forms (formerly known as section 29 forms and now often referred to as Schedule 2[1] forms) for requesting personal data in accordance with guidance issued by the National Police Chiefs' Council.

5.5.3 The form should certify that the information is required for an investigation concerning the prevention or detection of crime or the apprehension or prosecution of offenders and that the investigation would be prejudiced by a failure to disclose the information.

5.5.4 Subject to the emergency procedure discussed below, unless the request is in person (not over the telephone) from a member of the University's Neighbourhood Policing Team known personally to the system administrator or CCTV operator to be a member of that team, all police requests should be in writing.

5.5.5 Check any written request purporting to be from the police for authenticity. In particular, check any sending email address, and seek to verify via an alternative source if possible. For example, if possible check the switchboard telephone number and calling the relevant officer via that route.

5.5.6 Whether or not the request is from the University's Neighbourhood Policing Team, check the basis for disclosure. In particular:

- be clear why not releasing the information sought would be likely to prejudice (that is, significantly harm) any attempt by the requester to prevent crime or catch a suspect; and;

[1] Schedule 2 to the Data Protection Act 2018.

- you should only release the minimum data required to for the requester to be able to do their job.

5.5.7 If there is any doubt about the validity of a request you should not disclose the personal data and should contact Legal Services urgently for advice (legalservices@bournemouth.ac.uk).

5.5.8 As soon as possible after the disclosure, make and retain a record of any disclosure made. Keep the request or court order received alongside this.

- Keep the record securely, by scanning and placing in the collaborative folder in the I-Drive under Estates/CCTV (Administrative support will be provided by the Campus Services Manager (Facilities)). Delete any other local copy of the record once lodged in the collaborative folder.

- The record should state the:
  - name of member of staff authorising the disclosure;
  - the recipient's name, serial number and force;
  - the time, date and reason for the disclosure (why the information was required and the grounds on which the information was disclosed);
  - any advice sought and received;
  - if known, name(s) of the affected staff or student(s);
  - details of the information that was disclosed.

5.6 How to deal with emergency situations involving the police

5.6.1 An emergency situation is one where there is a reasonable belief that there is a life or death situation or a significant risk of serious harm (either to a staff member, student or any other person).

5.6.2 Where information is required in an emergency, unless the request has come from an individual you are used to dealing with (such as a member of BU's Neighbourhood Policing Team), ask the caller to provide a switchboard number and call them back through the organisation's switchboard before providing any personal data.

5.6.3 Where personal data is disclosed, you should make a record of the enquiry and the information disclosed. You may find it helpful to run through the points at paragraph 5.5.8 above when making a record of the disclosure. The record should be retained as for a normal police request (see paragraph 5.5.8 above).

6. Staff training

6.1. General

6.1.1. The Estates team will provide an initial induction to all new staff allowed access to the primary system.

6.1.2. The Estates team will provide regular training to all staff operating the primary CCTV system to ensure that they comply with this policy, the applicable data protection law and the ICO's CCTV Code of Practice 2015 (the **Code**). The Code is available here: https://ico.org.uk/media/for-organisations/documents/1542/cctv-code-of-practice.pdf

6.1.3. The training provision, will be reviewed on a regular basis (at minimum annually) to ensure the content is current and applicable. A training record of those trained and authorised to use the system will be incorporated into the Estates Training Matrix.

6.1.4. For secondary systems, the relevant Accountable Person through the respective nominated administrators identified at 1.1.7 and Appendix 1 is responsible and accountable for sourcing appropriate training for all staff using their CCTV systems. The University expects the training for secondary systems to be no less than offered by Estates to those administrating and operating the primary system.

6.1.5 The level of training required will vary depending upon skills and knowledge already acquired, the nature of the system and its operation and the working environment (how secure, etc.).

6.1.6 System administrators will ensure that for themselves and each operator they:

- assess the particular training needs.
- explain the training objectives, as set out in paragraph 6.1.3 above and 6.2 below as a minimum;
- establish the training content;
- choose an appropriate delivery method and monitor and evaluate delivery; and
- oversee the provision of continuous development and refreshment.

6.1.7 Training records must be kept and made available for inspection by internal audit as needed.

6.2 Training programme content

6.2.1 As noted in paragraph 6.1.2 above, training needs to ensure system compliance with this policy, the law and the Code. This is likely to include, without limitation:

- the necessary justifications for each camera, and associated audit trail;
- general arrangements for accessing CCTV recordings;
- what to do if requests for access come from the police;

- the BU Data Protection Policy;
- the applicable data protection legislation as it applies to CCTV systems; and the Code.

Appendix 1

BOURNEMOUTH UNIVERSITY CCTV Policy & Procedures 2022

Details of Secondary Systems

Faculty / Professional Service	Accountable Person	Address	Administrator	Contact Details (Phone & e-mail)	Remarks / Number of secondary CCTV assets in use?
Faculty of Science and Technology	*Natalie Andrade* *Operations Manager* nandrade@bournemouth.ac.uk 01202 961533	*Faculty of Science & Technology* *Bournemouth University* *Poole House* *Talbot Campus* *Fern Barrow* *Poole* *BH12 5BB*	*Technical Support Manager*	*Tel: 01202 965497* *gtoms@bournemouth.ac.uk*	*28 cameras for security & safety management*
The Student Union Bournemouth University is not covered by this CCTV policy, however, details of known systems that they operate are listed below					
The Old Fire Station	*Samantha Leahy-Harland, Chief Executive, SUBU* *01202 965767* *sleahyharland@bournemouth.ac.uk*	*Student Centre* *Bournemouth University* *Poole House* *Talbot Campus* *Fern Barrow* *Poole* *BH12 5BB*	*Mr Sam Cox* *Venue Manager*	*Tel: 01202 963889* *scox@bournemouth.ac.uk*	
The Student Union Shop	*Samantha Leahy-Harland, Chief Executive, SUBU* *01202 965767* *sleahyharland@bournemouth.ac.uk*	*Student Centre* *Bournemouth University* *Poole House* *Talbot Campus* *Fern Barrow* *Poole* *BH12 5BB*	*Mr Richard Gerrard* *Shop Manager*	*Tel: 01202 965855* rgerrard@bournemouth.ac.uk	*4 Cameras in Student Shop*

Appendix 2

BOURNEMOUTH UNIVERSITY CCTV Policy & Procedures

To be completed by each Accountable Person (one per Faculty and Professional Service) as specified in the CCTV Policy & Procedures and **returned to the Soft Services Manager, Estates annually by 1 December** and when any changes occur

Nil responses are required

Faculty / Professional Service:				
Accountable Person	**Name:**		**Post:**	
	Telephone		**E-mail:**	

Camera Name & Location (room number)	**Coverage**	**Purpose**	**Date Installed / Removed**	**CCTV Administrator (name and contact detail)**	**Where is CCTV data stored?**	**Who has access to the data?**	**Remarks**

Signed…….. **Dated……..**
Accountable Person