University of
St Andrews

CCTV policy

[

Document type	**Policy**
Scope (applies to)	Public
Applicability date	20/09/2023
Review / Expiry date	19/09/2024
Approved date	01/11/2023
Approver	Vice-Principal (Governance)
Document owner	Business Manager
School / unit	Estates
Document status	Published
Information classification	Public
EDI review/Equality impact assessment	21/09/2023
Key terms	Estate/Facilities management/Security
Purpose	This policy details the purpose, use and management of the CCTV system at the university and details the procedures to be followed in order to ensure that the university complies with relevant legislation and the current Information Commissioner's Office CCTV Code of Practice

CONTENTS

1. Introduction

1.1 The University of St Andrews (the University) has in place a CCTV surveillance system (the CCTV system) across its estate. This policy details the purpose, use and management of the CCTV system at the University and details the procedures to be followed in order to ensure that the University complies with relevant legislation and the Information Commissioner's Office CCTV Code of Practice. For the purposes of this policy, vehicle dashcams and authorised covert cameras shall be considered an extension of the CCTV system.

1.2 This policy is based upon all relevant legislation and guidance issued by the Information Commissioner's Office, 'In the picture: A data protection code of practice for surveillance cameras and personal information' (the Information Commissioner's Guidance).

2. CCTV System Overview

2.1 The CCTV system is owned and operated by the University of St Andrews, College Gate, North Street, St Andrews, Fife KY16 9AJ and managed by the University. The University may from time-to-time appoint third parties to maintain CCTV systems and by exception to operate such, under a Data Processor Agreement.

2.2 Under current data protection legislation the University of St Andrews is the 'Controller' i.e. responsible for all personal data that flows through the CCTV system.

2.3 The University is registered with the Information Commissioner's Office and the registration number is Z5909128. The CCTV system operates to meet the requirements of the Data Protection Act and the Information Commissioner's guidance.

2.4 The University Security Manager 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.

2.5 The CCTV system operates across the University's academic, administrative and residential sites. Details of the number and general location of cameras can be found at: Appendix A

2.6 Signs are placed at strategic points across the estate 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 University of St Andrews and supplies a 24-hour contact number for the Security and Response Team Control Room.

2.7 The Security Manager is responsible for ensuring that adequate signage is erected in compliance with the Information Commissioner's Office CCTV Code of Practice.

2.8 Cameras are sited to ensure that they cover University premises as far as is possible. Cameras are installed throughout the University's sites including roadways, car parks, buildings, residential accommodation, licensed premises, within buildings and externally in vulnerable public facing areas.

2.9 Cameras are not sited to focus on private residential areas and cameras situated in University residential accommodation focus on entrances and communal areas. Where static cameras in part overlook private residential areas, privacy screens will be fitted. For cameras that can be moved, operators will be trained to ensure they do not focus into private areas.

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

2.11 The CCTV system is subject to a Data Protection Impact Assessment (DPIA).

2.12 Any proposed new CCTV camera installation will be subject to a DPIA prior to progression.

3. Purposes of the CCTV system

3.1 The principal purposes of the University's CCTV system are as follows:

- For the prevention, reduction, detection and investigation of crime and other incidents;
- To ensure the safety of staff, students visitors and the general public;
- To assist in locating individuals believed to be missing, vulnerable or otherwise at risk of harm.
- To assist in formal investigations of suspected breaches of University regulations / policies by staff or students; and
- The monitoring and enforcement of traffic related matters.

3.2 The CCTV system will be used to observe the University estate and areas under surveillance in order to identify incidents requiring a response from the Police and/or the University staff as appropriate. Any response should be proportionate to the incident being witnessed.

4. Monitoring and Recording

4.1 Cameras are monitored in the Security and Response Control Room, which is a secure area, staffed 24-hours a day. The Control Room is equipped with a Home Office licensed radio system linking it with uniformed security officers who provide mobile and foot patrols and are able to respond to incidents identified on CCTV monitors.

4.2 Images are recorded centrally on servers located securely in the University of St Andrews Data Centre. The images are viewable by all security staff in the Control Room or elsewhere via devices enabled for that purpose on the approval of the Security Manager.

4.3 Additional staff may be authorised by the Security Manager to monitor cameras sited within their own areas of responsibility on a view only basis.

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

4.5 All images recorded by the CCTV System remain the property and copyright of the University.

4.6 The monitoring of staff activities will be carried out in accordance with Part 3 of the Information Commissioner's Office Employment Practices Code.

4.7.1 Covert cameras

4.7.1 The use of covert cameras will be restricted to exceptional occasions, when a series of criminal acts have taken place or where the seriousness of what has taken place in a single instance, in an area without CCTV, requires that response

4.7.2 Deployment of a covert camera is conditional on a DPIA establishing that its use is proportionate, legal and necessary.

4.7.3 Covert recording will only take place if informing the individual(s) concerned would seriously prejudice the reason for making the recording and where there are reasonable documented grounds to suspect that illegal or unauthorised activity is taking place. All such monitoring will be fully documented in a DPIA, and will only take place for a limited and reasonable period.

4.7.4 A request for the use of covert cameras will require to be submitted via the relevant Head of School/Unit (or Deputy) to the Security Manager. The application must clearly state the purpose and reasons for the request. The Security Manager will liaise with the Head of Information Assurance and Governance to be satisfied that the relevant criteria for deployment is met. Once satisfied that all relevant criteria have been met, the application will be forwarded to the Vice Principal Governance for consideration.

4.7.5 The Vice Principal Governance, in whose absence a delegated member of Principal's office, must decide whether an application for covert installation of CCTV is justified.

5. Compliance with Data Protection Legislation

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

a) processed lawfully, fairly and in a transparent manner;

b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes;

c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;

d) accurate and, where necessary, kept up to date;

e) 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;

f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

The University ensures it is responsible for, and able to demonstrate compliance with UK-GDPR

6. Applications for disclosure of images

6.1 Applications by individual data subjects

6.1.1 Requests by individuals for images relating to themselves (commonly known as a Subject Access Request) should be made to dataprot@st-andrews.ac.uk

6.1.2 In order to locate the images from the University CCTV, sufficient detail must be provided by the requestor in order to allow the relevant images to be identified and located. The right of subject access only extends to an individual's personal data – in this instance their imagery, where captured and held. If a request is made and the imagery of others is present then the University may not be able to provide imagery of the requestor.

6.2 Access to and disclosure of images

6.2.1 An individual or organisation should submit their request for images from the CCTV system in writing to the Security Manager.

6.2.2 In limited circumstances it may be appropriate to disclose images to a third party, such as the Police, when a disclosure is required by law, in relation to the prevention or detection of crime or in other circumstances.

6.2.3 Disclosures of CCTV imagery for the purposes of the prevention and detection of crime are managed under University Policy i.e. Requests for personal data by the Police or a similar third party for the purposes of the prevention or detection of crime, apprehension or prosecution of offenders, or for taxation

6.2.4 Disclosures of CCTV imagery for other purposes may be made at the discretion of the Security Manager, with reference to relevant legislation and where necessary, following advice from the University Head of Information Assurance and Governance.

6.3. Where a formal investigation into possible staff misconduct has been launched in accordance with the University's Investigation Procedure, the appointed Investigation Manager (IM) may formally request the Security Manager to provide access to relevant CCTV images. The IM should seek the advice of the relevant HR Business Partner, and must document their reason for making this request. This documentation of the IM's reason for request must be made available to the investigated employee along with all other documents pertaining to the investigation at the time of notification that an investigation is underway.

6.3.1 The Security Manager may release images to the University Environmental Health and Safety Services as part of a Health and Safety investigation.

6.3.2 The Security Manager may provide access to CCTV images to Student Services, the Student Conduct Officer or Residential Services Managers when sought as evidence in relation to risk assessment and/or investigations under University non-academic misconduct policy or residential contracts.

6.3.3 A record of any disclosure made under this policy will be held on the CCTV management system, itemising the date, time, camera, requestor, authoriser and reason for the disclosure.

7. Retention of images

7.1 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 or deleted after this point.

7.2 Where an image is required to be held in excess of the retention period referred to above, the Security Manager or their nominated deputy, will be responsible for authorising such a request.

7.3 Images held in excess of their retention period will be reviewed on a three monthly basis and any not required for evidential purposes will be deleted.

7.4 Access to retained CCTV images is restricted to the Security Manager and other persons as required and as authorised by the Security Manager.

8. Complaints procedure

8.1 Complaints concerning the University's use of its CCTV system or the disclosure of CCTV images should be made in writing to the Security Manager at: securitymanager@st.andrews.ac.uk.

8.2 All appeals against the decision of the Security Manager should be made in writing to Head of Information Assurance & Governance at: dataprot@st.andrews.ac.uk

8.3 If it transpires that an issue of complaint concerns data protection rights, available under the UK-GDPR that will then be investigated by the University Data Protection Officer, or their nominee.

9. Monitoring Compliance

9.1 All staff involved in the operation of the University'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.

9.2 All staff with responsibility for accessing, recording, disclosing or otherwise processing CCTV images will be required to undertake data protection training.

9.3 Any breaches of this policy or misuse of accessed footage will be considered under the relevant disciplinary process.

10.Policy review

10.1 The University's use of CCTV and the content of this policy shall be reviewed annually by the Security Manager with reference to the relevant legislation or guidance in effect at the time. Further reviews will take place as required.

11.Links to Reference Material

The Data Protection Act 2018

The General Data Protection Regulation (GDPR) - UK Government

The General Data Protection Regulation (GDPR) - Information Commissioners Office

The Freedom of Information (Scotland) Act 2002

The Human Rights Act 1998

The Scottish Government National Strategy Document for Public Space CCTV in Scotland.

Information Commissioner's Office, 'In the picture: A data protection code of practice for surveillance cameras and personal information

Information Commissioner's Office, "The employment Practices Code"

University of St Andrews Use of Captured Content Policy (Lectures) (see 2.5 to 2.7)

University of St Andrews: Regulations governing the use of University information and communications technology (ICT) facilities (see section 9)

University of St Andrews privacy notice: collection and use of employee personal data (see sections 12 and 18)

University of St Andrews privacy notice: Undergraduate and taught post graduate students (see section 4.18)

University of St Andrews Non-Academic Misconduct Policy (See section 7)

University of St Andrews Investigation Procedure

Appendix A

CCTV Installations
August 2023

The University of St Andrews seeks to ensure, as far as is reasonably practicable, the safety and security of University staff, students, visitors, contractors, grounds, buildings and their contents. To assist in achieving this, the University deploys CCTV cameras, of varying types, around the estate in pursuance of the prevention, detection and investigation of crime and other incidents including internal disciplinary matters.

The Security Manager has overall responsibility for CCTV installations, recording and monitoring. The viewing of live and recorded images is restricted to persons authorised by the Security Manager. The principles of the Data Protection Act 2018 and the CCTV Code of Practice are observed to ensure compliance with the legal framework under which personal details relating to individuals is processed.

The University currently has 479 CCTV installations

Eden Campus (Guardbridge)	83
St Andrews East Shore	22
St Andrews North Haugh	100
St Andrews St Mary's	37
St Andrews Town Centre	142
St Andrews Town West	95

Version number	Purpose / changes	Document status	Author of changes, role and school / unit	Date
1	New policy	Public	Security Manager	21/09/2023