

|  |  |
| --- | --- |
| Version number: | 2.0 |
| Policy owner: | Head of Campus and Residential Services |
| Effective date: |  |
| Review date: |  |
|  |  |

University of Chichester

CCTV Policy

**Table of Contents**

1. Policy Statement 2
2. Definitions 2
3. About this Policy 3
4. Personnel Responsible 3
5. Reasons for the use of CCTV 4
6. Monitoring 4
7. How we will operate any CCTV 4
8. Use of data gathered by CCTV 5
9. Retention and erasure of data gathered by CCTV 5
10. Use of additional surveillance systems 6
11. Covert Monitoring 6
12. Ongoing review of CCTV use 6
13. Requests for disclosure 6
14. Automatic Number Plate Recognition Cameras (ANPR) 7
15. Subject Access Requests 7
16. Complaints 7
17. Requests to prevent processing 7
18. Appendix A – for security reasons not published NA
19. Appendix B – Request to Share Personal Data Form 8
20. Appendix C – CCTV Retention Log 11
21. Appendix D – University Privacy Statement 12

# Policy Statement

We believe that CCTV and other surveillance systems have a legitimate role to play in helping to maintain a safe and secure environment for all our students, staff and visitors. However, we recognise that this may raise concerns about the effect on individuals and their privacy. This policy is intended to address such concerns.

Images recorded by surveillance systems may contain personal data which must be processed in accordance with data protection laws. We are committed to complying with our legal obligations and ensuring that the legal rights of students, staff and visitors relating to their personal data, are recognised and respected.

This policy is intended to assist staff in complying with their own legal obligations when working with personal data. In certain circumstances, misuse of information generated by CCTV or other surveillance systems could constitute a criminal offence.

# Definitions

For the purposes of this policy, the following terms have the following meanings:

* + 1. **CCTV** means fixed and domed cameras designed to capture and record images of individuals and property including automatic number plate recognition. This also includes security body worn cameras that capture sound and vision.
    2. **Data** is information which is stored electronically, or in certain paper-based filing systems. In respect of CCTV, this generally means video images. It may also include static pictures such as printed screen shots.
    3. **Data subjects** means all living individuals about whom we hold personal information as a result of the operation of our CCTV (or other surveillance systems).
    4. **Personal data** means data relating to a living individual who can be identified from that data (or other data in our possession). This will include video images of identifiable individuals.
    5. **Data controllers** are the people who, or organisations which, determine the manner in which any personal data is processed. They are responsible for establishing practices and policies to ensure compliance with the law. [We are the data controller of all personal data used in our business for our own.]
    6. **Data users** are those of our employees whose work involves processing personal data. This will include those whose duties are to operate CCTV cameras and other surveillance systems to record, monitor, store, retrieve and delete images. Data users must protect the data they handle in accordance with this policy and our Data Protection Policy.
    7. **Data processors** are any person or organisation that is not a data user (or other employee of a data controller) that processes data on our behalf and in accordance with our instructions (for example, a supplier which handles data on our behalf).
    8. **Processing** is any activity which involves the use of data. It includes obtaining, recording or holding data, or carrying out any operation on the data including organising, amending, retrieving, using, disclosing or destroying it. Processing also includes transferring personal data to third parties.
    9. **Surveillance systems** means any devices or systems designed to monitor or record images of individuals or information relating to individuals. The term includes CCTV systems as well as any technology that may be introduced in the future such as, body worn cameras, unmanned aerial systems and any other systems that capture information of identifiable individuals or information relating to identifiable individuals.

# About this Policy

We currently use CCTV cameras to view and record individuals on and around University premises. This policy outlines why we use CCTV, how we will use CCTV and how we will process data recorded by CCTV cameras to ensure we are compliant with data protection law and best practice. This policy also explains how to make a subject access request in respect of personal data created by CCTV.

We recognise that information that we hold about individuals is subject to data protection legislation. The images of individuals recorded by CCTV cameras are personal data and therefore subject to the legislation. We are committed to complying with all our legal obligations and seek to comply with best practice suggestions from the Information Commissioner's Office (ICO).

This policy covers all employees (academic and professional services), students, consultants, contractors, freelancers, volunteers, interns, casual workers, and agency workers and may also be relevant to visiting members of the public.

This policy is non-contractual and does not form part of the terms and conditions of any employment or other contract. We may amend this policy at any time without consultation and the policy will be regularly reviewed to ensure that it meets legal requirements and relevant guidance published by the ICO and industry standards.

A breach of this policy may, in appropriate circumstances, be treated as a disciplinary matter. Following investigation, a breach of this policy may be regarded as misconduct leading to disciplinary action, up to and including dismissal.

# Personnel Responsible

The Director of Estate Management has overall responsibility for ensuring compliance with relevant legislation and the effective operation of this policy. Day-to-day management responsibility for deciding what information is recorded, how it will be used and to whom it may be disclosed has been delegated to The Head of Campus and Residential Services. Day- to-day operational responsibility for CCTV cameras and the storage of data recorded is the responsibility of Campus Services Manager.

Responsibility for keeping this policy up to date has been delegated to the Head of Campus and Residential Services.

# Reasons for the use of CCTV

We currently use CCTV around our sites as outlined below. We believe that such use is necessary for legitimate business purposes, including:

* + 1. to prevent crime and protect buildings and assets from damage, disruption, vandalism and other crime;
    2. for the personal safety of students, staff, visitors and other members of the public and to act as a deterrent against crime;
    3. to support law enforcement bodies in the prevention, detection and prosecution of crime;
    4. to assist in day-to-day management, including ensuring the health and safety of staff, students and others;
    5. to assist in the identification of actions that may result in disciplinary proceedings against staff or students or action against contractors providing services to the University;
    6. to promote a safe community environment; and
    7. to assist in traffic management and parking enforcement.
    8. To assist staff in emergency situations

This list is not exhaustive and other purposes may be or become relevant.

# Monitoring

Predominately CCTV monitors the exterior of the buildings and covers entrances and exits to site. The number of cameras is suitably modest and locations have been prioritised to prevent excessive coverage. There are a small number of cameras located internally in key locations for the protection of assets. Halls of Residence have internal cameras which only focus on the main entrance door to the block. Locations of cameras are at Appendix A, but for security reasons are not for publication. No cameras are hidden or covert. Where possible cameras are placed out of risk of criminal damage.

Cameras are positioned so that they only cover public or shared areas. As far as practically possible no cameras focus directly into private residential areas or offices.

Surveillance systems, other than body cameras do not record sound.

Cameras are not actively monitored. Images are recorded 24 hours a day, 7 days a week, 365 days a year. Images will only be examined where there is justification i.e. when investigating an incident, seeking clarification of an event, improving understanding in relation to Health and Safety or performance matters or when a crime has occurred or is suspected. This has been communicated to staff who operate the system.

Staff using surveillance systems will be given appropriate training to ensure they understand and observe the legal requirements related to the processing of relevant data.

# How we will operate any CCTV

We will ensure that signs are displayed at the entrance of the surveillance zone to alert individuals that their image may be recorded. Such signs will contain details of the organisation operating the system, the purpose for using the surveillance system and who to contact for further information, where these things are not obvious to those being monitored.

Live feeds from CCTV cameras will only be monitored where this is reasonably necessary, for example to protect health and safety.

We will ensure that live feeds from cameras and recorded images are only viewed by approved members of staff whose role requires them to have access to such data. Recorded images will only be viewed in designated, secure offices.

In exceptional circumstances contracted security officer may use body worn cameras that capture both sound and vision.

# Use of data gathered by CCTV

In order to ensure that the rights of individuals recorded by the CCTV system are protected, we will ensure that data gathered from CCTV cameras is stored in a way that maintains its integrity and security. This may include encrypting the data, where it is possible to do so.

At the request of the Police, other agency or a third party, a nominated officer may review the recorded footage from the CCTV system to establish whether an incident was captured by any of the cameras.

The nominated officer may then advise the third party making the enquiry whether the incident has been captured and recorded on the system. They will not, at this stage, indicate to the third party the specific nature of what has been recorded.

Should the Police, an agency or a third party wish to view footage relating to an incident they must complete the Request to Share Personal Data Form (see Appendix B). This will require the approval of one off the nominated officers. The same procedure applies for requests of duplicate copies.

Nominated officers have been informed of the procedures to follow in relation to law enforcement, subject and third-party requests. Critically, they know not to deviate from this policy and not to disclose information to others unless it is explicitly permitted.

Once information has been disclosed to the Police they become the Data Controller for the purposes of data protection legislation.

# Retention and erasure of data gathered by CCTV

Data recorded by the CCTV system will be stored on the system’s hard drive. The data is stored for 31 days when it is automatically overwritten and so permanently deleted. Images retained for the purpose of investigation may be retained for a longer period of time. Exactly how long images will be retained for will vary according to the purpose for which they are being recorded. For example, where images are being recorded for crime prevention purposes, data will be kept long enough only for incidents to come to light. All data will be permanently deleted once it is no longer useful for the purpose to which it was retained. Any data that is retained will be logged so as to keep a record; an example log appears at Appendix C.

At the end of their useful life, all digital information stored in whatever format will be erased permanently and securely. Any physical matter such as tapes or discs will be disposed of as confidential waste. Any still photographs and hard copy prints will be disposed of as confidential waste.

Any footage recorded by security officers using body worn cameras will be downloaded to a memory card. This would be securely stored in a locked safe until it can be transported to their Head Office where it will be transferred to a secure encrypted storage device. Data will be permanently deleted after 31 days if not passed to relevant authorities.

# Use of additional surveillance systems

Prior to introducing any new surveillance system, including placing a new CCTV camera in any workplace location, we will carefully consider if they are appropriate by carrying out a Data Protection Impact Assessment (DPIA).

A DPIA is intended to assist us in deciding whether new surveillance cameras are necessary and proportionate in the circumstances and whether they should be used at all or whether any limitations should be placed on their use.

Any DPIA will consider the nature of the problem that we are seeking to address at that time and whether the surveillance camera is likely to be an effective solution, or whether a better solution exists. In particular, we will consider the effect a surveillance camera will have on individuals and therefore whether its use is a proportionate response to the problem identified.

No surveillance cameras will be placed in areas where there is an expectation of privacy (for example, in changing rooms) unless, in very exceptional circumstances, it is judged by us to be necessary to deal with very serious concerns.

# Covert monitoring

We will never engage in covert audio-visual monitoring or surveillance (that is, where individuals are unaware that the monitoring or surveillance is taking place) unless, in highly exceptional circumstances, there are reasonable grounds to suspect that criminal activity or extremely serious malpractice is taking place and, after suitable consideration, we reasonably believe there is no less intrusive way to tackle the issue.

In the unlikely event that covert monitoring is considered to be justified, it will only be carried out with the express authorisation of The Vice Chancellor’s Group. The decision to carry out covert monitoring will be fully documented and will set out how the decision to use covert means was reached and by whom. The risk of intrusion on innocent staff and students will always be a primary consideration in reaching any such decision.

Only limited numbers of people will be involved in any covert monitoring.

Covert monitoring will only be carried out for a limited and reasonable period of time consistent with the objectives of making the recording and will only relate to the specific suspected illegal or unauthorised activity.

# Ongoing review of CCTV use

We will ensure that the ongoing use of existing CCTV cameras in the workplace is reviewed at least every 12 months to ensure that their use remains necessary and appropriate, and that any surveillance system is continuing to address the needs that justified its introduction. We will maintain a log of such reviews for audit purposes.

# Requests for disclosure

We may share data with third parties where we consider that this is reasonably necessary for any of the legitimate purposes set out above in paragraph 5.1.

No images from our CCTV cameras will be disclosed to any third party, without express permission being given by Head of Campus and Residential Services. Data will not normally

be released unless satisfactory evidence that it is required for legal proceedings or under a court order has been produced.

In other appropriate circumstances, we may allow law enforcement agencies to view or remove CCTV footage where this is required in the detection or prosecution of crime.

We will maintain a record of all disclosures of CCTV footage.

No images from CCTV will ever be posted online or disclosed to the media.

# Automatic Number Plate Recognition (ANPR) Cameras

# 14.1 ANPR cameras are located at the main entrance to all University Campuses for the purpose of parking enforcement. This system and is operated and managed by a contracted third-party specialist company, Parking Eye.

# 14.2 A full DPIA was completed in consultation with the University Data Protection Officer before the system went live.

# 14.3 All staff and students have been notified of the use of ANPR cameras and there is appropriate, legally compliant signage at entrances and throughout car parks.

# 14.4 All staff and students, when applying to park on campus will be required to positively accept Parking Eye’s Terms & Conditions and the University Privacy Statement, which can be found at Appendix D.

# Subject Access Requests

# 15.1 Data subjects may make a request for disclosure of their personal information and this may include CCTV images (data subject access request). A data subject access request is subject to the statutory conditions from time to time in place and should be made in writing, [in accordance with our subject access policy which can be found at https://[www.chi.ac.uk/about-us/policies-and-statements/data-protection](http://www.chi.ac.uk/about-us/policies-and-statements/data-protection)

# 15.2 In order for us to locate relevant footage, any requests for copies of recorded CCTV images must include the date and time of the recording, the location where the footage was captured and, if necessary, information identifying the individual

# 15.3 We reserve the right to obscure images of third parties when disclosing CCTV data as part of a subject access request, where we consider it necessary to do so

# Complaints

# 16.1 If any member of staff has questions about this policy or any concerns about our use of CCTV, then they should speak to the Head of Campus and Residential Services in the first instance.

# 16.2 Where this is not appropriate or matters cannot be resolved informally, employees should use our formal grievance procedure.

# Requests to prevent processing

# 17.1 We recognise that, in rare circumstances, individuals may have a legal right to object to processing and in certain circumstances to prevent automated decision making (see Articles 21 and 22 of the General Data Protection Regulation). For further information regarding this, please contact the University Data Protection Officer [dpofficer@chi.ac.uk.](mailto:dpofficer@chi.ac.uk)

**Appendix B: Request to Share Personal Data Form**

Before releasing personal data to the Police, we require sufficient information to demonstrate that disclosure is necessary and proportionate, and that it cannot be obtained through other means.

1. **Details of request**

|  |  |
| --- | --- |
| Name: | Click or tap here to enter text. |
| Police force: | Click or tap here to enter text. |
| Date of request: | Click or tap to enter a date. |
| Police ref: | Click or tap here to enter text. |
| Crime ref if applicable: | Click or tap here to enter text. |
| Authorising Officer (name and rank/role)\*: | Click or tap here to enter text. |

***\*please note requests need to be authorised by an officer of the rank of Inspector or above.***

|  |
| --- |
| **What information is requested?** |
| Please be specific about the scope of your request, ensuring that you are only asking for necessary information, and please specify whether [special category data](https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/special-category-data/) is required:  Click or tap here to enter text. |
|  |
| **What time period(s) does this request relate to?** |
| Please provide details of dates and times:  Click or tap here to enter text. |

1. **Purpose**

|  |
| --- |
| **What is the reason for the request?** |
| If you are investigating a criminal offence, or potential criminal offence, please state what this is and why this information is required for that investigation:  Click or tap here to enter text. |

1. **Necessity**

|  |  |
| --- | --- |
| **Is the information requested necessary for prevention or detection of an unlawful act?** | |
|  | **Yes**: Please include more detail here if not covered under question 2 above:  Click or tap here to enter text. |
|  | **No** |
|  | | |
| **Is the information necessary for reasons of substantial public interest?** | |
|  | **Yes**: Please explain why:  Click or tap here to enter text. |
|  | **No** |
|  | | |
| **Could this information be obtained in any other less invasive way and/or from an alternative source?** | |
|  | **Yes:** Please explain why this alternative source is not being used to obtain the information:  Click or tap here to enter text. |
|  | **No** |

1. **Proportionality**

|  |  |
| --- | --- |
| **What are the potential risks to the individual of us providing the requested information?** | |
| Click or tap here to enter text. | |
|  | |
| **Is there any reason why we should not contact the individual(s) to ask for their consent to share the requested information?** | |
|  | If yes, please explain why: Click or tap here to enter text. |

**INTERNAL USE ONLY: FOR COMPLETION BY UNIVERSITY OF CHICHESTER STAFF:**

**UK GDPR Article 6 Lawful basis for processing**

|  |  |
| --- | --- |
|  | **(a) Consent:** the individual has given clear consent for the University to process their personal data for a specific purpose. |
|  | **(c) Legal obligation:** the processing is necessary to enable the University to comply with legislation, e.g. Safeguarding (not including contractual obligations). |
|  | **(d) Vital interests:** the processing is necessary to protect someone’s life. |
|  | **(e) Public task:** the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law |
|  | **(f) Legitimate interests:** the processing is necessary for the legitimate interests of the University and/or the legitimate interests of a third party, and this is not overridden by the interests, rights and freedoms of the individual. If this lawful basis is relied upon please complete a brief legitimate interests assessment:  The purpose test (identify the legitimate interest):  Click or tap here to enter text.  The necessity test (consider if the processing is necessary):  Click or tap here to enter text.  The balancing test (consider the individual’s interests):  Click or tap here to enter text. |

**UK GDPR Article 9 Condition for processing (special category data only)**

|  |  |
| --- | --- |
|  | (a) Explicit consent |
|  | (c) Vital interests of the individual or of another natural person where the individual is physically or legally incapable of giving consent |
|  | (f) Legal claims or judicial acts |
|  | (g) Reasons of substantial public interest (with a basis in law)  6. Statutory and government purposes 7. Administration of justice and parliamentary purposes  10. Preventing or detecting unlawful acts 11. Protecting the public 12. Regulatory requirements  14. Preventing fraud 15. Suspicion of terrorist financing or money laundering  18. Safeguarding of children and individuals at risk |
|  | (i) Public health (with a basis in law) |

|  |  |  |
| --- | --- | --- |
| Approved | Yes | No |
| Rationale if refused: | Click or tap here to enter text. | |
| Decision made by: | Click or tap here to enter text. | |
| In consultation with:  *(if applicable)* | Click or tap here to enter text. | |
| Date: | Click or tap to enter a date. | |

# Appendix C: CCTV Retention Log

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Date Data Retained | Date of Data Captured | Time from – to | Reason for retention | Authorised by | Storage Method | Outcome | Date of Data Deletion | Method of Deletion | Name of Staff | Signature |
|  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |

**Appendix D: University Privacy Statement**

**PRIVACY NOTICE**

**How we use your information**

The University is committed to protecting the privacy of personal information in full compliance with Data Protection legislation.

To apply for a Car Parking Permit, you will need to complete an application form and as part of the application process you will be asked to provide personal information to enable your application to be processed. This information will be stored and processed securely by the University and third parties, as indicated below, acting on behalf of the University, for the purposes of managing parking applications and enforcement. Data is stored on local and cloud-based servers that are hosted in the UK. All data stored and processed is subject to stringent and appropriate security measures and reviews.

The University is the controller for this service and Parking Eye Limited, trading as Car Parking Partnership, are the processors acting on behalf of the University.  Applications for permits, appeals against a permit decision, renewals and amendments are managed by the University.  The personal data we collect will be processed for the purposes of sending automated alerts and emails relating to the issue, management, maintenance and renewal of parking permits. Enforcement of parking regulations will be automated via ANPR cameras. Images captured will detail all vehicles entering and exiting University property and may include occupants. This data will be stored and processed securely by Parking Eye acting as processor on behalf of the University for the purpose of enforcement.

Applicants will arrange payment for parking by payment card and will be directed to the Cardsave payment portal (part of WorldPay) integrated with the Car Parking Permit Application system. Payment card data is not saved within the permit system.

Please note that limited information, such as the name and contact number of the registered keeper of a vehicle may be shared with the University Car Parking Contractor to support the University’s Parking Policy Enforcement Procedure. Data such a place of work will be stored for statistical purposes.

**Lawful basis for processing personal data**

By registering on the University Car Parking Permit Application system, you will be accepting our terms and conditions, as part of entering a contact with the University for supply of a parking permit.

In the course of completing your application we may require your explicit consent to sharing special category data, which is relevant to your application e.g. information relating to a health condition you may have.  Where you have consented to provide such information, this will only be processed to assess your eligibility for a permit and will not be used for any other purpose.

**Retention periods for personal data**

The Universitywill retain any information supplied, as part of your application, including documents uploaded to the database, or any relevant details from such documents, for the duration of your permit.  We will not ask you for more information than we need, and we will not keep your information for any longer than necessary.

The Car Parking Permit Application system is automated to delete your data after set periods, dependent upon the status of your permit as set out below:

* For approved permits: data will be deleted 1 calendar month after permit expiry.
* For applications that are incomplete: data will be deleted 3 calendar months after the last change or action.
* For applications that are declined, retired, awaiting verification, awaiting approval or awaiting payment: data will be deleted 12 calendar months after the last change or action.
* For applications that have been appealed: data will be deleted 12 calendar months after the last appeal submission.
* Records of sent emails will not be deleted if they are less than 3 months old. This is to ensure records of emails sent near the end of a permit’s life are still available while relevant.

**Personal data that will be deleted**

All data submitted in applications, including personal data such as contact details (name, address, email) and vehicle registration will be deleted. In additional any history relating to emails sent, appeal submissions, appeal decisions and all other information stored in the permit system regarding charges and payments will also be deleted, other than where required to meet any statutory obligations.

Basic anonymous permit information such as Permit Reference, Approval State, Permit Type, Zone, Term, Start and End Date will be retained for statistical purposes for the duration of the University’s use of the Car Parking Permit Application system.

**My rights as a data subject**

As a data subject you have rights under data protection legislation including for example the right of to access information held about you, the right of rectification of any incorrect or incomplete data, and the right of erasure of your data (right to be forgotten) when it is no longer necessary for the purposes it was collected and processed.

To find out more about how the University complies with data protection legislation and your rights as a data subject you can access our Privacy Standard and Privacy Notices here: <https://www.chi.ac.uk/about-us/policies-and-statements/data-protection/>.

If you wish to raise a complaint on how we have handled your personal data, you can contact our Data Protection Officer at [DPOfficer@chi.ac.uk](mailto:DPOfficer@chi.ac.uk).

If you are not satisfied with our response or believe we are not processing your personal data in accordance with data protection legislation you can complain to the Information Commissioner’s Office (ICO) <https://ico.org.uk/concerns/>.