University of HUDDERSFIELD
Inspiring global professionals

POLICY FOR THE OPERATION OF CLOSED CIRCUIT TELEVISION

Contents

Introduction and Accountability

The University of Huddersfield has installed a comprehensive Closed Circuit Television (**CCTV**) surveillance system (the **System**) whereby cameras have been installed at the campus. Images are monitored by the security staff at the Control Room.

Using software and cameras located within buildings, data will be monitored by nominated staff within the faculty or department whose areas the cameras are designed to protect, as well as Security Control. A list of nominated staff is included at Appendix I of this Policy.

The System is owned by the University and operated by the Estate and Facilities Department. The Control Room is staffed by the University's security team, which comprises the University's security staff and Contract Security Staff.

This Policy is intended to act as guidance for Estates staff, the operators of the System and all members of the University community.

The Policy's purpose is to ensure that the System is used to create a safer environment for students, staff and visitors to the University, and to ensure that its operation is consistent with the obligations on the University imposed by the Data Protection Act 2018 (DPA 2018). The objectives of the Policy are outlined at paragraph 1.1 below. This Policy is designed to work with the University's Data Protection Policy, the provisions of which should be adhered to at all times.

Guidance published in 2018 by the Information Commissioner's Office (the **ICO**) can be found on the ICO's website or by using this link - ICO link to your data matters

Complaints

The Security Services Manager is responsible for the operation of the System, and, in the first instance, for ensuring compliance with this Policy. Breaches of the Policy by any member of staff may constitute a disciplinary matter under the relevant conditions of employment. It may also be a criminal offence. It is also recognised that other members of the University may have concerns or complaints in respect of the operation of the System. Any concerns in respect of the System's use or regarding compliance with this Policy should, in the first instance, be addressed to the Security Services Manager in writing or by email using the contact details below.

Contact details:

Security Services Manager	m.j.falsey@hud.ac.uk
Security Services Manager Telephone	01484 472632
Security Control Room	01484 472221

Policy

1. Objectives

1.1 The System has been installed by the University for the principal purposes of preventing and detecting crime. It is recognised, however, that ancillary benefits of operating CCTV for these purposes may include reduction of the fear of crime generally, the provision of a safer public environment for the benefit of those who work within the University or who visit and may assist with increasing the level of customer care. These objectives must, however, be consistent with respect for individuals' privacy.

1.2 The System will be monitored in accordance with these objectives and, accordingly, monitoring will be permitted only to:

- assist in the prevention and detection of crime;
- facilitate the identification, apprehension and prosecution of offenders in relation to crime and public order and as an aid to public safety;
- assist with the enforcement of University car parking regulations and to assist in the management of the car parks;
- provide and operate the System in a manner which is consistent with respect for the individual's privacy;
- assist with the provision of a safer public environment;
- assist with the promotion of the principles of customer care; and
- assist in work place monitoring where this relates to involvement in criminal activity or gross misconduct.

2. The System

2.1 The System is all internet protocol based, password protected and comprises a selection of fixed position cameras, monitors, recording facilities on designated CCTV University servers and public information signs. The cameras cover building entrances, car parks, perimeters, external areas and internal areas such as receptions, the library recreational spaces and teaching and study areas. They do not cover areas where individuals have a reasonable expectation of privacy, such as toilets and changing rooms.

2.2 The System encompasses Queensgate Campus and Southgate Campus. It will also include CCTV images that, in due course, are captured by the System and monitored at the twenty-four hour Control Room.

2.3 Details of the locations of any overt CCTV surveillance cameras operated by the University may be available on written request, subject to relevant exemptions. Requests should be directed to Security Services Manager in the first instance.

2.3 The System is operational and images are capable of being monitored for twenty-four hours a day, throughout the whole year.

2.4 The University's staff, students and the general public are made aware of the presence of the System and its ownership by compliant University signage prominently placed at the main entrances to and relevant areas on the Campus. This sets out the purposes for processing CCTV images (in accordance with paragraph 1.1 above) and identifies the University as the party responsible for processing those images.

2.5 To ensure privacy, wherever practicable, the cameras are prevented from focusing or dwelling on domestic accommodation and this will be demonstrated on request to local residents. Where domestic areas such as gardens are near those areas which are intended to be covered by the scheme, the Security Services Manager (or nominee) will consult with the owners of the domestic area to discuss what images may be recorded.

2.6 Images captured on camera are recorded on digital hard drive recording for use in accordance with this Policy. Persons monitoring the images at locations other than the Library, or the Security Control Room will not be permitted to view anything other than the live stream without the permission of the Security Services Manager. Any images recorded will be managed by the Security Services Manager for images recorded in the Security Control Room.

2.7 Although every effort has been made in the planning and design of the System to give it maximum effectiveness, it is not possible to guarantee that the system will detect every incident taking place within the area of coverage.

2.8 For the purposes of the Act, the Data Controller is the University and the University is legally responsible for the management and maintenance of the System.

2.9 In order to comply with the objectives of this Policy with regard to public safety (see paragraph 1.1) Control Room staff will monitor University car parks. Monitoring of car parks will also take place in order to assist colleagues with the enforcement of the University car parking regulations and the prevention and detection of crime.

3. The Library

3.1 Images captured by the System in the library shall be monitored by the library wardens during library opening hours.

3.2 The System monitors in the library shall have access granted only to those members of staff who need to monitor the system and who have been appropriately trained in accordance with this policy. No unauthorised access shall be permitted at any time.

3.3 Any incidents viewed on the library System shall be recorded by the library wardens on the Incident log maintained by the Security Services Manager as described in 5.1.

3.4 The designated nominees listed in Annex I shall have the ability to play back images captured by the System in the library when strictly necessary. The designated nominees shall be responsible for ensuring that all viewing of playback is logged on the central register in security control.

4. The Control Room

4.1 Images captured by the System will be monitored in the Control Room. The Control Room is a self-contained and secure room. The monitors in the Control Room cannot be seen from outside.

4.2 Access to the Control Room is strictly limited to the Security Services Manager, Senior Management and staff members specifically authorised by either the Security Services Manager, Assistant Security Services Manager or Senior Management.

4.3 No unauthorised access to the Control Room is permitted at any time. Police officers and any other person with statutory powers of entry may enter with the explicit consent of the Security Services Manager or nominee.

4.4 Persons other than those specified in paragraph 4.2 may be authorised to enter the Control Room on a case-by-case basis. Written or verbal authorisation is required and may only be given by the Security Services Manager or nominee. Each separate visit will require individual authorisation and will be supervised, at all times, by the Security Services Manager or nominee. Such visitors will not be given access to any data which falls within the scope of the Act.

4.5 In an emergency and where it is not reasonably practicable to secure prior authorisation, access may only be granted to persons with a legitimate reason to enter the Control Room by the officer on duty at that time. Such access will be recorded.

4.6 Before granting access to the Control Room, officers must satisfy themselves of the identity of any visitor and ensure that the visitor has the appropriate authorisation. All visitors will be required to complete and sign the visitors' log, which shall include their name, their department or the organisation they represent, the person who granted authorisation for their visit (if applicable) and the times of their entry to and exit from the Control Room. A similar record shall be kept of the officer on duty in the Control Room at any given time.

5. Control Room Administration and Procedures

5.1 An electronic operational incident log will be maintained in the Control Room and details of all incidents will be noted together with any action taken.

5.2 It is recognised that images of identifiable living individuals obtained by the system comprise personal data and are subject to the law on data protection including the provisions of the Act.

All copies will be handled in accordance with the procedures outlined in Appendix II of this Policy, which is designed to ensure the integrity of the system. The Security Services Manager will be responsible for the development of and compliance with the working procedures in the Control Room.

5.3 Recorded images will only be reviewed with the authority of the Security Services Manager or nominee. Copies of images are permitted only for the purposes of crime detection, evidence in relation to matters affecting safety, evidence for prosecutions, evidence for disciplinary proceedings in accordance with clauses 6 and 7 below, for the purpose of car park management or where otherwise required by law.

6. Covert Recording

6.1 Covert cameras may be used only in the following circumstances and only with the written authorisation of, or upon the request of, the University Vice Chancellor or Deputy Vice Chancellor if:

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

6.2 Any covert recording will only be carried out for a limited and reasonable period of time. It must be consistent with the objective of making the recording and must only relate to the specific unauthorised activity.

6.3 The decision to adopt covert recording will be appropriately documented and will detail the issue rationale and decision as to why the use of covert recording was reached, the length of time it is to continue for and by whom.

7. Workforce Monitoring

7.1 The system may capture images of staff members during its operation. These images will only be viewed or used for workforce monitoring purposes if the University has reasonable suspicion of criminal activity, gross misconduct or behaviour which puts others at risk.

7.2 If images of staff members caught by the system are to be used either in disciplinary proceedings, criminal or civil proceedings then the footage will be retained until after these proceedings have concluded. Retention will be for such period as is necessary according to the purpose(s) for which the images were obtained or have been retained, in accordance with the Records Retention Schedule.

7.3 Staff members have the right to view any images of them which have been captured by the system and also have a right to respond to such images.

7.4 In addition to being informed in this Policy, there will also be signs placed at the entrance and at strategic points throughout the University, informing staff that CCTV is in operation.

8. Staff

8.1 All staff involved in the operation of the system will, by training and access to this Policy, be made aware of the sensitivity of handling CCTV images and recordings.

8.2 The Security Services Manager will ensure that all staff, including relief staff, are fully briefed and trained in respect of all functions, operational and administrative, arising from the system.

8.3 All staff using the system will be trained on the University's obligations, and its and their responsibilities, arising from the Act.

8.4 Operatives of the System not directly employed by the University (for example, contract security staff) will be required to hold a valid Security Industry Authority (SIA) licence before they are permitted to access the System.

9. Recording & Retaining

9.1 The System and local systems are supported by digital hard drive recording facilities. The digital recording facility is capable of retrieving images to a dedicated server or to an external device.

9.2 Images will be cleared automatically after holding for 28 days unless otherwise required to keep for evidential purposes or a Subject Access Request has been received before the images are due for deletion. However, the University recognises that, in accordance with the requirements of the Act, no images should be retained for longer than is necessary. Accordingly, some recorded images may be erased after a shorter period, for example, where it can be determined more quickly that there has been no incident giving rise to the need to retain the recorded images.

9.3 In the event of the disc or digitally recorded image being required for evidence or the investigation of crime it will be retained for a period of time until it is no longer required for evidential purposes or any investigation into a crime has been completed.

9.4 In order to comply with the standards set out in the ICO's Code of Practice:

- the medium on which images have been recorded will only be used once and
- where the system records, features of the camera and/or date and time reference, these will be checked for accuracy on a regular basis.

9.5 Where images are to be downloaded, the minimum number of copies necessary to achieve the purpose shall be created. Any such copies shall be destroyed once they are no longer required for the purpose. Due to improved camera/quality (higher data) all such copies shall be recorded onto suitable media USB, CD or DVD-R; or utilise Police 'Good Sam' system (Instant On Scene

(goodsamapp.org). Where other media are used, they shall be stored in accordance with Appendix II.

9.6 Hard copy prints of digital images are subject to the same controls and principles of Data Protection as other data collected in the Control Room. They will be treated using the same procedures (contained within Appendix II of this Policy) as digital images.

10. Monitoring Procedures

10.1 The Control Room will be staffed by authorised officers only. The officers are members of the University's Security Staff or Contracted Security staff.

10.2 The control of the system will always remain with the University but at the University's discretion the cameras may be operated in accordance with requests made by the police during an incident to:-

- monitor potential public disorder or other major security situations;
- assist in the detection of crime; and
- facilitate the apprehension and prosecution of offenders in relation to crime and public order.

On each occasion that the Police obtain assistance with their operations, a report setting out the time, date and details of the incident must be recorded on operational incident log and brought to attention of the Security Services Manager.

11. Digital Recording Procedures

11.1 Control and management of digital recordings

Media handling procedures are in place to ensure the integrity of the image information held (see paragraph 9).

11.2 Third party access to recordings

Requests by persons outside the University for viewing or obtaining digital recordings will be made via the University's Data Protection (handling Subject Access Requests).

Access to recorded images will only be granted where it is consistent with the obligations placed on the University by the Act, the University's Data Protection Policy and, in particular, with the purposes set out in paragraph 1.1 of this Policy.

12. Standards

12.1 It is important that access to, and disclosure of, the images recorded by the system is restricted and carefully controlled, not only to ensure that the rights of individuals are preserved, but also to ensure that the chain of evidence remains intact should the images be required for evidential purposes. Users of the System will also have to ensure that the reasons for which they may disclose copies of the images are compatible with the reasons or purposes for which they originally obtained those images. The University use of CCTV is in accordance with the ICO's Code of Practice. By following the principles of the Code it ensures the University's compliance by respecting an individual's privacy, having clearly defined rules and guaranteeing images recorded are for a specified purpose or for law enforcement. Regular reviews ensure its use is reasonable and proportionate and the data is only used for the purposes for which it was collected.

12.2 All Control Room staff will be made aware of the restrictions set out in this Policy in relation to access to, and disclosure of, recorded images.

12.3 Access to recorded images will be restricted to staff who need to have access in order to achieve the purposes of using the system.

12.4 All access to the medium on which the images are recorded (disc or digital) will be documented.

12.5 Disclosure of the recorded images to third parties will be made only in the following limited and prescribed circumstances, and only to the extent required or permitted by law:

- law enforcement agencies where the images recorded would assist in a specific criminal inquiry;
- prosecution agencies;
- relevant legal representatives;
- where it is deemed necessary by the Security Services Manager or nominee to identify a victim, witness or perpetrator in relation to a criminal incident. Images from the system may be circulated via the University e-mail system to selected staff on a targeted basis.; and
- where disclosure is required by virtue of the Act.

12.6 When Disclosure to a third party is granted, the University will ensure:

- arrangements are in place to restrict disclosure of images in a way consistent with the purposes set out in paragraph 1.1 of this Policy;
- consideration is given to whether images of individuals need to be obscured to prevent unwarranted identification or distress;
- the images are disclosed in a way that is secure to ensure they are only seen by the intended recipient; and

- appropriate records are maintained.

12.7 All requests for access or for disclosure will be recorded. The Security Services Manager or nominee will make decisions on access to recorded images by persons other than police officers. Requests by the police for access to images will not normally be denied provided that they are accompanied by a request for disclosure information form signed by a police officer of appropriate seniority, who must indicate that the images are required for the purposes of a specific criminal enquiry in sufficient detail to enable the University to identify that the request meets the requirements of the Act.

12.8 If access or disclosure is denied by the Security Services Manager, the reasons will be documented and filed.

If access to or disclosure of the images is allowed, then the following will be documented on Appendix IV:

- the date and time at which access was allowed and/or the date on which disclosure was made;
- the reason for allowing access or disclosure;
- details of who the images have been provided to (name of the individual and the organisation (where applicable);
- the extent of the information to which access was allowed or which was disclosed;
- the Security Services Manager or nominee, using the appropriate forms will document routine disclosure to the police (Appendix III)

See paragraph 13 for access by data subjects.

13. Access by Data Subjects

13.1 All individuals whose images are recorded have a right to request to view the images of themselves held by the University and, unless they agree otherwise, to be provided with a copy of the images in most circumstances (a **Subject Access Request**); the individual will need to contact the University, by either:

- Using the form on UoH website (Data Protection - University of Huddersfield)
- Emailing: data.protection@hud.ac.uk
- Write to Data Protection, Vice-Chancellor's Office, University of Huddersfield, Queensgate. Huddersfield. HD1 3DH.

13.2 All staff involved in monitoring or handling image data will proceed in accordance with the following protocol in respect of a Subject Access Request.

13.3 Data subjects must make their request in writing in sufficient detail to allow for identification of the information they require including:

- Dates and times of the footage they are requesting and their location, for example which specific area or building in sufficient detail to allow the University to identify relevant footage;

- Two photographs of themselves - one full face and one side view with the completed form;

- Proof of their own identity e.g. a utility bill, a driving licence or a passport.

13.4 Upon receipt of a Subject Access Request, the Security Services Manager may contact the requestor to discuss the request and shall, in responding to any such requests, give due consideration to the rights and freedoms of third parties captures in the images. In particular, the Security Services Manager shall consider whether:

a) still images can be provided instead of film footage
b) it is possible to remove or redact third party data
c) it is possible to arrange for the data subject to attend the University premises to view the footage without providing a copy.

Where appropriate, these options will be discussed with the requestor to determine whether it is possible to provide the information they are seeking.

Where the University cannot comply with the request without disclosing information relating to another individual who can be identified from the footage, then the University may refuse the request unless that other individual has consent to the release of the information or it is reasonable in all the circumstances for the University to provide the information without their consent.

13.5 The Security Services Manager shall respond to all requests under this section within one calendar month of receiving the request, either providing the data or explaining why the data cannot be released to the individual.

13.6 Copies of Subject Access Requests must be sent to the University's Data Protection Officer for audit and record-keeping purposes.

14. Request to Prevent Processing

14.1 An individual has the right to request a prevention of processing where this is likely to cause substantial and unwarranted damage or distress to that or another individual.

14.2 All such requests should be addressed in the first instance to the Security Services Manager, who will provide a written response within 20 working days of receiving the request, setting out their decision. A copy of the request and response will be retained.

Appendix I

Nominated Staff who may view and download live stream CCTV

Name	Job Title
Martin Falsey	Security Services Manager
	Assistant Security Services Manager
Gary Skyrme	Estates &Facilities IT Systems Development and Support Analyst
Contracted Control Room CCTV Operatives SIA Licenced	Contracted, SIA Licenced Control Room CCTV Operatives

Nominated Staff who may view live stream CCTV

Name	Job Title
Heather Kerrick	Assistant Director, Estates and Facilities
Various nominated	Campus Support Officers
Various nominated	Library Wardens (Library cameras only)
Claire White	Executive Office Manager – Vice-Chancellor's Office (VCO cameras only)
David Bray	Team Leader – Computing and Engineering (SCE cameras only)
Darren Sugden	Technical Services Manager – Computing & Engineering (SCE cameras only)

Nominated Staff who may playback CCTV (Library cameras only)

Name	Job Title
Vince Deer	Library Support Officer
Wayne Winterbottom	IT Support Manager
Paula Clover	Library Services, Customer Services Manager

Appendix II

Policy the Operation of CCTV

PROCEDURES FOR THE HANDLING OF CCTV IMAGES

Computer Disks-Still photographs

All computer disks containing CCTV images, or any still photograph or printed image, shall be marked with a unique number and securely stored within filing cabinet in Security Control Hub. A log will be maintained by the Security Services Manager or nominee containing details as to the dates when the disk/photograph was introduced into the system or created and when it was disposed of. Computer disks, still photographs and hard copy prints will be disposed of as confidential waste. Such erasure and disposal will be logged.

Disclosure of images to third parties

In this section "Authorised Data Handler" means, the Security Services Manager or nominee.

Disclosure to the Police

Where a police officer requests access to CCTV footage, they must provide an appropriate request for disclosure of information form, setting out the information required, and the reasons for the request. The form must identify the requesting officer and be countersigned by an appropriate signatory in accordance with police protocols.

When such a request is received, the Authorised Data Handler shall consider it and, if appropriate, arrange for the release of data. A copy of the form shall be retained by the Authorised Data Handler, who shall arrange for a copy to be provided to the Data Protection Officer.

Disclosure to Other Person/Third Party

Where information is requested by someone other than the police or the data subject, (a "third party"), for example HR, Registry, H&S, that third party shall make the request on the Third Party Request Form in Appendix III. The Authorised Data Handler shall review the request and may only release the information if they are satisfied that there is a legal basis for doing so, and that it is reasonable in the circumstances for the information to be disclosed.

The Authorised Data Handler shall complete, sign and date Part C of the form confirming details of the data released (if any). The Authorised Data Handler may consul the Data Protection Officer when considering whether it is appropriate to release the data. If the University considers that the release

of data would prejudice the rights and freedoms of individuals, or that the third party had not provide a sufficiently clear legal basis for releasing the information, such request for data may be refused.

Other persons may also include law enforcement agencies (other than the police), solicitors, private individuals.

(An example of a private individual being given access to the data would be where a victim of a theft, is permitted to view a recorded image to point out to an investigator the exact location where an item subject to theft was located. This would allow the investigator to view the images and concentrate their attention on that location).

The Security Services Manager or nominee shall retain the completed form for evidential purposes and shall send a copy to the Data Protection Officer for auditing and record keeping purposes.

Appendix III

REQUEST FOR DISCLOSURE OF INFORMATION

Request to external organisation for disclosure of personal data (Form replacing DP7 and DP9)

West Yorkshire Police (WYP) request access to the specified information for the purpose outlined below. This request is made for the purpose(s) specified below, under one or more of the following legal powers:

- DPA 2018 Schedule 2 Part (2); Schedule 8 Parts (1), (2), (3), (6), (7) & (8); Section 8 (a) & (c)
- The Police Act 1996, MOPI 2005
- Crime and Disorder Act 1998
- Coroners and Justice Act 2009 Part 3

1. Information held by:	
Name	Click or tap here to enter name of recipient.
Position	Click or tap here to enter their position in their organisation.
Organisation	Click or tap here to enter name of their organisation.
Email address	Click or tap here to enter Email address.
Postal address	Click or tap here to enter address of their organisation.

2. This request is necessary of the purpose of:	
The prevention, investigation, detection or prosecution of criminal offences	☐
The execution of criminal penalties	☐
Safeguarding against and the prevention of threats to public security	☐
Other – please state other purpose below:	☐

The data subject is deceased and information is required for a valid policing purpose	☐
To determine questions of fitness to be interviewed, *Mens Rea* etc. (See guidance for healthcare requests below - it is unlikely that information supporting these purposes is routinely collected during treatment; however the current clinician may be able to support this need via an appropriate report).	☐

3. Data subjects details:	
Name	Click here to enter Name.
Alias	Click here to enter Alias Name.
Date of Birth	Click here to enter a Date.
Date of Death (if applicable)	Click here to enter a Date.

4. Police investigation details:	
Offence Reference	Click here to enter text..
Date of Offence	Click here to enter Date.
Details of Offence	Click here to enter text.

Address (including previous address if relevant)	Click here to enter text.

5. Information required:	
State brief summary of the criminal investigation or proceedings to which this request relates (e.g. crime type). Indicate in general terms (e.g. Suspect, Victim, Witness) how the individual named is linked to the investigation. **Only provide the minimum information - be careful not to disclose any third party personal data or information that would be excessive.**	Click here to enter text.
Information required, e.g. medical records, social care records, statements etc. (if known)	Click here to enter text.
Date or dates between if specific date is not known	Click here to enter text.
The information sought is needed to: Insert brief details to show that the requested information: • cannot be obtained by other means or from other sources • will be of substantial value to the investigation	Click here to enter text.

6. Informing the Individual of the request:	
Please indicate whether telling the individual would harm the investigation Telling the individual about this request will harm the police investigation **If YES – Go directly to 8.** **IF NO – Go to 7 – the police must tell the individual about this request and provide them with the privacy information referenced.**	Choose an item.

7. Privacy Information **Only complete this section with the individual if you are informing them of the request**	
Data Subject's Acknowledgement I confirm that I have been advised that my personal data will be processed for the purpose(s) as set out above and that I can obtain more information about my data rights at: **https://www.westyorkshire.police.uk/advice/our-services/your-data/privacy-information-notice/privacy-information-notice**	Choose an item.

I understand that the information provided will be held confidentially and used solely for the purpose(s) outlined above, unless otherwise required or permissible by law.	
Print name:	Click here to enter text.
Signature:	
Capacity* **Please state your capacity for requests involving vulnerable adults and children under the age of 13 years** (e.g. Parent, Guardian, Appropriate Adult or Other Representative)	Click here to enter text.
Date:	Click here to enter Date.
Address:	Click here to enter text.
Date of Birth*	Click here to enter Date.
*DPA / GDPR indicate that a parent / guardian may act on behalf of a child under 13, whereas consideration of the capacity of the child to consent in their own right is appropriate for older children.	

8. Requested by:	
Officer in the Case:	Click here to enter Rank - Number - Name.
Authorising Officer: only needed if you are not telling the individual about the request	Click here to enter Rank - Number – Name.
Requesting Officer:	Click here to enter Rank - Number – Name.
Contact details: Station, Address, Email, Telephone	Click here to enter text.
Request Date:	Click here to enter Date.
I confirm that the information requested is needed for the purposes indicated above and a failure to provide that information would harm the police investigation	

Notes:

- It is mutually agreed between the police and those to whom the request is addressed that no charges will be made in respect of this request.
- WYP confirm that the information requested is for the purpose stated above and any failure to provide it will, in the view of the Requesting Officer, be likely to prejudice the police investigation.
- WYP confirm that the information will be held confidentially and used solely for the purpose(s) outlined above, unless otherwise required or permissible by law.
- WYP will securely dispose of the information when no longer required.
- In the case of ORIGINAL records, WYP will return the records when no longer required.

REMOVE from completed form BEFORE submission

Guidance for Police

This form replaces DP7 and DP9. It is used by the police to make formal requests to other organisations for personal data where the information is needed for a policing purpose. It places no compulsion on the recipient to disclose the information, but should provide the necessary assurance that a disclosure for these purposes is appropriate and in compliance with the Data Protection Act 2018 or other legislation or legal powers. The information provided on the form should provide the recipient with sufficient information to allow them to locate the information sought.

NOT telling the individual about the request (previously form DP7)
If the police investigation would be harmed by telling the individual about the request then you do not need to tell them.

The request must however be countersigned by an Inspector or police staff equivalent or above, and both you and the Authorising Officer must sign the form at Section 8.

Telling the individual about the request (previously form DP9)

If **NO** harm would occur to your police investigation then you **MUST** inform the individual (or their representative if vulnerable or under 13 years) of the request and refer them to the West Yorkshire Police Privacy Information Notice at:

https://www.westyorkshire.police.uk/advice/our-services/your-data/privacy-information-notice/privacy-information-notice

The individual (or their representative) must then sign the form at Section 7.

The request must then be signed by the requesting officer at Section 8 – there is no need for a counter-signature.

Officers must:

- **Retain a copy of the completed form and attach it to the source system e.g. NICHE**
- **Send a completed copy to the relevant external organization**

Further guidance on the use of this form may be obtained from the force Data Protection Officer.

Guidance Relating to Health Records

Uninformed Disclosure – where you cannot tell the data subject about the request because this would compromise the police investigation: These disclosures are common when the subject is the alleged perpetrator of crime, although also for use when the subject is a victim or witness but not co-operative, or lacks capacity. Requests for healthcare information / medical records will be reviewed and authorised by an appropriate senior officer within healthcare organisations, usually in the role of Data Protection Officer and / or Caldicott Guardian. So as not to prejudice the enquiry, the subject will not be informed of the request for disclosure. Although the DPA does not define "serious crime", the GMC definition will generally be considered.

Informed Disclosure – where you can inform the data subject about the request: The typical approach when the subject is co-operating with the police – e.g. a witness or victim of alleged crime. Informed disclosures are processed on the basis that the police have provided the relevant privacy information to the subject.

Access to Deceased Records: The Data Protection Act only has jurisdiction over information relating to living individuals. Although the confidentiality of medical & other records may continue post-mortem, their disclosure for policing or other official purposes is permissible.

Fitness to be interviewed, *Men's Rea* etc.: Largely specific to Mental Health records. Healthcare records are maintained to support treatment. Questions relating to fitness to be interviewed, to stand trial, or criminal intent when an alleged offence was committed are rarely recorded in healthcare records. When this is the aim, healthcare providers will signpost the police to an appropriate clinical contact to commence a dialogue and potentially draft an appropriate report.

Healthcare Professional: Before healthcare records are disclosed, they will be reviewed by an appropriate healthcare professional – usually someone who is / was involved in a professional capacity with the data subject - to consider any information which is likely to cause harm or distress to the data subject or a 3rd party. Should such information be identified WYP will be informed, with a view to agreeing its sensitive handling.

Original (Paper) Records: Copies of records will ordinarily be provided. Originals will be provided where justifiable, retaining a copy to maintain the integrity & accessibility of the records until the originals are returned. Records are increasingly wholly electronic. Hard copy will be provided.

Information required (Section 5): This section frames the request so that both parties understand the nature of the investigation and intent of the disclosure. Data Controller organisations are obliged to consider the request for disclosure against the Duty of Confidence under which records are held. The detail provided will help to balance the confidentiality of records with the public interest in disclosure. Be as descriptive as possible in these areas. Although full disclosure is permissible, records are often large in volume. Specifying the request, e.g. for specific content, date range etc. will help to reduce scope. Requests should be confined to relevant information when this is understood and known.

Appendix IV

Third Party Data Request

Section A. Third Party Requesting Information

Name……

Position *(if applicable)* ……

Business/Agency *(if applicable)* ……

Business/Agency/Home address (*whichever is applicable)* ……

Telephone Number/Email address……

Signature……Date……

Reference No……

Section B Data Required

Date & Time of footage……

Location of Cameras……

Reason for Request……

Requested Format ☐I want to view the footage ☐ I want printed images ☐I need a copy of the footage

(Note: Whilst your request will be taken into account, if the University releases data, it will do so in the least intrusive way possible, at its own discretion)

Legal Basis for Request

I have the consent of the Data subject (please attach a copy) ☐

I need this information for the purpose of safeguarding national security ☐

I need it for reasons of public interest (please state these reasons) ☐

……

I need this in connection with legal proceedings and I have a court order (please attach) ☐

(Note: If you do not yet have your court order, you can submit the form and we will not erase any relevant data, but unless it is reasonable to do so, we will not release the data without it)

I am relying on another basis for release (please state the legal basis, including reference to legislation where appropriate) ☐

……

……

……

Section C University Authorisation

Disclosure Made: ☐Viewing only ☐still images provided ☐Copy footage given ☐No disclosure made

Name…… Position…… Date……

Policy Sign Off and Ownership Details

Document name:	Policy for the Operation of Closed Circuit Television
Version Number:	2.0
Equality Impact Assessment:	Not required – the impact of the activity of CCTV capturing images is fair, transparent, and consistently applied for all.
Approved by:	Senior Leadership Team
Date Approved:	08 July 2022
Date for Review:	July 2024
Consulted with:	University Secretary
Author:	Assistant Director of Estates and Facilities
Owner (if different from above):	Director of Estates and Facilities
Document Location:	https://www.hud.ac.uk/media/policydocuments/CCTV-Policy.pdf
Compliance Checks:	Annual audit of CCTV usage
Related Policies/Procedures:	Data Protection Policy

REVISION HISTORY

Version	Date	Revision description/Summary of changes	Author
V2.0	July 2022	First draft of policy - no major changes.	Assistant Director of Estates and Facilities
V1.0	July 2019	First draft of policy under new Policy Framework	Assistant Director of Estates and Facilities