CCTV, Cloud Based 4G Redeployable Cameras and Body Worn Video (BWV)

May 2023

Contents

Definitions

Cloud-Based 4G Redeployable Cameras: temporary Cloud-based IP cameras offering end-to-end encryption which record video material when activated. Any Cloud-based 4G redeployable camera used will allow for images to be recorded, stored and downloaded using end-to-end Cloud-based encryption.

Body Worn Video [BWV]: wearable body camera equipment which records audio, video, or photographic material as required. Any BWV used will allow for images and voice to be recorded and downloaded.

Data Controller: in this instance Linacre College (the "College") as defined in Article 3 of General Data Protection Regulation: Linacre College Student Privacy Policy.

Data Subject: as defined in Article 3 of General Data Protection Regulation: Linacre College Student Privacy Policy.

Personal Data as defined in Article 3 and 4 of General Data Protection Regulation: Linacre College Student Privacy Policy and any information (including a recording) which relates to an identified or identifiable individual.May include image and voice.

Recorded Material: any material recorded by, or as the result of, technical equipment, which forms part of the CCTV System, Cloud-based 4G redeployable cameras or is recorded by the BWV.

System Maintenance: IT Manager, Director of Estates

System Manager: IT Manager and Lodge Reception Manager

System Operator: Linacre College

System Owner: (of the CCTV System) Director of Estates on behalf of Linacre College

The System: A Closed-Circuit Television (CCTV) System in use at Linacre College and operated from 24/7 Lodge Reception

Introduction

Linacre College has a closed-circuit television system [CCTV] in place to provide a safe and secure environment for students, staff and visitors and to protect College property. The CCTV system runs 24 hours a day, 7 days a week. The cameras are strategically positioned to ensure minimal intrusion of privacy and prominent signs are displayed to inform employees, students, members of the public and other individuals that CCTV is in use. Linacre cameras cover the main College site but also all student residences owned by the college within Oxford including Stoke House in Headington. Access to CCTV footage or images will be restricted with clear guidelines on who can access the information.

This policy sets out how Linacre College uses CCTV, Cloud-based 4G redeployable cameras or BWV to ensure compliance with the General Data Protection Regulations, The Human Rights Act 1988 (HRA) and the Surveillance Camera Code Of Practice issued under the Protection Of Freedoms Act (POFA Code).

Context and Application of the Policy

Linacre College is located in the centre of Oxford City, within an area that is consistently busy with pedestrians and traffic. The Lodge Reception aims to be staffed 24/7. The main door of the college is locked on a door access system, but unlocked weekdays from 12pm to 1:30pm for visitors to access our dining hall for lunch. There are other entry points to the college with access being granted to those who possess an appropriate fob or card. All visitors, contractors and suppliers will be managed by the Lodge through our E-Visitor software system.

[redacted]

3.1 This Policy applies to all parties who seek to rely on CCTV, Cloud-based 4G redeployable cameras or BWV footage recorded on premises used by the University.

3.2 It sets out how CCTV, Cloud-based 4G redeployable cameras and BWV footage may be used within Linacre College. It explains when footage may be shared lawfully within the University and externally with third parties.

3.3 The System will be operated at all times and any Cloud-based 4G redeployable cameras and BWV footage will be recorded with due regard for the privacy of individuals being recorded (the Data Subjects).

Reasons for CCTV, Cloud-Based 4G Redeployable Cameras and why BMW Equipment May be Worn

These security measures are available to:

- Reassure those on College premises that in the event of an incident, CCTV, Cloud-based 4G redeployable cameras or possibly BWV footage may be available to support any subsequent investigation
- Act as a deterrent to any such incidents happening and contribute to a safe environment
- Help to identify, apprehend and prosecute or sanction offenders. Footage may provide the police and others with supporting evidence to enable criminal and civil proceedings to be actioned (including where specific police operations are underway)
- Support the investigation of incidents where conduct of staff, students or others has not been in line with: College or University policy, regulations or their contract of employment, or where there is otherwise apparently unacceptable behaviour, or is contrary to law or Government Guidelines
- Be relied upon by the college in negligence proceedings, where there is a recording of an accident or incident, , including in support of an insurance claim.
- Ensure that the college premises are in good order
- Support an investigation which is not directly relevant to the College save it may have been recorded on or close to College premises
- Support Data Protection Subject Rights Requests (including access)
- Support investigations or enquiries carried out by relevant stakeholders (such as contractors or other employers working on site) with a view to achieving these same aims
- Any other purpose which is broadly equivalent to these aims, as determined by the Director of Estates

The CCTV, Cloud-based 4G redeployable cameras and BWV will not be used for entertainment purposes or on a day-to-day basis to monitor the work of employees, conduct of students or to check if they are complying with the policies and procedures set by the College. Images from the system will not be disclosed to third parties (except for reasons set out below). The CCTV system does not record sound.

Statements of Purpose & Principles of the CCTV, Cloud-Based 4G Redeployable Cameras and BWV Policy

4.1 Purpose

The purpose of this Policy is to set out how CCTV recordings, Cloud-based 4G redeployable cameras and BWV will be used within the College and to meet the objectives and principles outlined in sections 3 and 4. Forms are available in the appendices which are to be completed to document the release of information.

4.2 Principles of operation of CCTV, Cloud-based 4G redeployable cameras and BWV:

CCTV

4.2.1 The CCTV system will operate in accordance with any applicable legislation, Guidance, Regulation Codes of Practice or Conduct and relevant Policies. See: https://www.gov.uk/government/publications/update-to-surveillance-camera-code/amended-surveillance-camera-code-of-practice-accessible-version

4.2.2 There must be signage highlighting clearly that CCTV is in use.

4.2.3 The CCTV System uses a digital operational recording facility securely located throughout the college. A list of recording facilities is kept securely in the Lodge Reception. Those operating or downloading CCTV will be authorised by the Director of Estates, Bursar, the Domestic Operations Manager, or their representative to do so.

4.2.4 The Lodge Manager is to maintain an up-to-date inventory of all camera locations (CCTV, Cloud-based 4G redeployable cameras) and a list of those trained in their use which can be reviewed by the Director of Estates, the Domestic Operations Manager, or delegated nominee. Generally:

4.2.5 Strategic responsibility for security management rests with the Director of Estates, with day-to-day operational management delegated to the Domestic Operations Manager, supported by the Lodge Manager and Head of Maintenance.

4.2.6 Recognisable images of people and recordings constitute Personal Data, as prescribed in Data Protection law. Personal Data must be processed with due regard to the Principles in SS 86-91 Data Protection Act 2018 which requires that processing must be (as paraphrased here):

- Lawful, fair and transparent
- Collected for specified, explicit and legitimate purposes
- Adequate, relevant and limited to what is necessary
- Accurate and where necessary kept up to date
- Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which those data are processed
- Processed in a manner that ensures appropriate security of the personal data
- Destroyed in accordance with the College requirements

4.2.7 Copyright and ownership of any footage will remain with the college as the Data Controller.

4.2.8 The University's Data Protection Policy can be found here: https://www.linacre.ox.ac.uk/about-linacre/policies-bylaws

4.2.9 All breaches of information security, technical assurance or near misses involving the processing of personal data involving BWV equipment, Cloud-based 4G redeployable cameras or CCTV must be reported to the Data Protection Officer (College Principal) by email. Any incidents must be investigated in accordance with the Information Security Policy and Disciplinary Rules and Procedures for Staff which can be found here: https://www.linacre.ox.ac.uk/about-linacre/policies-bylaws.The sharing of information about a person's protected characteristics [age, disability, gender reassignment, marriage and civil partnership, pregnancy and maternity, race, religion or belief, sex, and sexual orientation] learnt through CCTV, is a breach of the Equality Act 2010.

CCTV System Use, Cloud-Based 4G Redeployable Cameras and BMW Operation

5.1. Every person involved in the management and operation of CCTV, Cloud-based 4G redeployable cameras or BWV must be provided with access to this Policy by their line manager.

5.1.2 No member of staff may use any of the equipment until they have received suitable training and they are familiar with this Policy and other relevant requirements brought to their attention by their line manager.

5.1.3 Members of the College who are involved with the monitoring, provision and use of any footage by whatever means are doing so in accordance with the requirements of any explicit or implied terms relating to confidentiality in their contract of employment. They are required to sign the Declaration of Confidentiality (Appendix 2) confirming that they have received suitable training; that they are aware of their responsibility under the terms of this Policy as well as their contract. This Declaration must be retained in their personnel file and be available on request. These staff are bound by any implied or explicit contractual obligations to keep information confidential.

5.1. 4 Any CCTV, Cloud-based 4G redeployable cameras or BWV user found to have unlawfully, wilfully or negligently compromised the privacy of individuals in breach of this policy may be subject to the disciplinary procedures of the College, and may be reported to the authorities (e.g., the Police or appropriate regulator). Non-compliance by third parties will be subject to contractual penalties may face criminal charges by the authorities or other appropriate sanctions. Nothing in this policy should inhibit lawful whistleblowing which is carried out in accordance with relevant procedures.

5.1.5 A list of authorised persons to monitor and download CCTV, Cloud-based 4G redeployable cameras or BWV images will be kept up-to-date by the Lodge Reception Manager and the IT Manager will review it annually to make sure it is up-to-date.

5.1.6 No recorded CCTV, Cloud-based 4G redeployable cameras or BWV material, whether recorded digitally, in analogue format or as a hard copy video print, will be released from the Control Room unless it is in accordance with this Policy and the prerequisite authority to release has been secured, save in an emergency (see Appendix 3).

5.1.7 A CCTV, Cloud-based 4G redeployable camera and BWV data release log(s)will be kept up-to-date by the Lodge Manager for audit trail purposes.

5.1.8 Where a person seeks to exercise their Data Subject Rights (see Ss 45-50 Data Protection Act 2018) such as seek a copy of footage of themselves, the Data Subject should contact the Principal as the Data Protection Officer. If the request is received by a third party (such as the contracted Security Services), any request should be forwarded promptly so that it can be dealt within the legal time limit.

5.1.9 Where a control centre requires operators to be licensed, in accordance with the law, no member of staff may operate cameras subject to the legislation without a Public Space Surveillance (CCTV) licence. It is for the College to ensure that it is current and valid.

5.1.10 The College CCTV System shall be maintained by the IT Manager and Lodge Reception Manager to ensure compliance with the Information Commissioner's Office (ICO) CCTV Code of Practice and that images recorded continue to be of appropriate evidential quality. The maintenance programme will make provision for regular/periodic service checks on the equipment, which will include cleaning of any all-weather domes or housings, checks on the functioning of the equipment, and any minor adjustments that need to be made to the equipment settings to maintain picture quality. The maintenance will also include regular periodic overhaul of all the equipment and replacement of equipment, which is reaching the end of its serviceable life.

5.2 BWV Operation

5.2.1 Any BWV worn must be to the security specification as agreed by the College.

5.2.2 BWV may only be worn and used by suitably trained and designated staff. This may be worn by private security hired by the College should they risk assess an event to require BWV.The hired private security company are responsible for ensuring that all staff are trained to requisite standards.

5.2.3 The BWV user will declare that they are recording as they respond to an incident, with a view to highlighting who will be in receipt of said footage. The BWV user must wear clothing that displays that they areusing this equipment. Recording must not be covert.

5.2.4 College does not operate BWV as a matter of routine. It may be deployed at major events, for example by external security companies operating to College's security specification.

5.3 Cloud-based 4G redeployable cameras

Covert Cloud-based 4G redeployable cameras will be used on rare occasions when a serious or persistent criminality is taking/has taken place and all other physical methods of prevention have been exhausted.

5.3.1 Any Cloud-based 4G redeployable cameras must be to the security specification as agreed by the Director of Estates. This may be used by private security hired by the College should they risk assess an event to require Cloud-based 4G redeployable cameras. The hired private security company would be responsible for ensuring that all staff are trained to requisite standards and that the necessary license is gained from the local council.

5.3.2 Cloud-based 4G redeployable cameras must only be installed and used by suitably trained and designated staff, and with agreement from the Director of Estates.

5.3.3 This equipment is a temporary measure and strict installation periods must be agreed by the Director of Estates or Bursar, recorded and adhered to. If a longer-term solution is required, an application must be made to the Director of Estates for the installation of fixed CCTV.

5.3.4 There must be signage highlighting clearly and visibly that CCTV is in use.

5.3.5 The use of Cloud-based 4G redeployable cameras to obtain photographic images and data on or over the Linacre College estate must comply with the General Data Protection Regulations and CCTV Codes of Practice cited in this document.

5.4 Privacy Notices

The Contracted Security Services and the College will ensure that the use of Cloud-based 4G redeployable cameras, BWV and CCTV is noted on Privacy Notices. The privacy notice explains what personal information is collected, what it is used for and who it is provided to as explained in this policy. The notice also describes why we require your data, and the legal basis on which we do this, again, as explained in this policy. The CCTV privacy notice is also informed by the College's Data Protection Policy, Health and safety Policy, Information Security Policy, Student Privacy Policy. This notice is to be published on the College's website under the section Policies and By Laws.

5.5 Access Arrangements and Security of Central Control Room (the lodge)

Access and security arrangements to central Control Room shall as a minimum comply with the following:

- Access to the CCTV system is strictly controlled and only those persons on legitimate business are allowed access as set forth in section 4 of this policy.

- A detailed record will be maintained by the Lodge and access will only be maintained after formal identification has taken place and authorised by the Director of Estates, Bursar or Domestic Operations Manager.
- Visitor acess will only be permitted by the authorisation process described above.
- A logbook of access to the System is maintained by the Lodge. This book contains details of the individual and organisation, date, time and purpose of visit.

5.5.1 Request to prevent access to images:

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

All such requests should be addressed in the first instance to the Principal who will provide a written response within 21 days of receiving the request setting out their decision.. A copy of the request and response will be retained.

5.6 Management of Recorded CCTV, Cloud-based 4G redeployable cameras and BWV Material

5.6.1 The management of recorded evidence will be compliant with ICO CCTV Code of Practice (the Code of Practice), which can be found at: https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/cctv-and-video-surveillance/

5.6.2 Any images obtained from the System must be treated in accordance with this policy and the Code of Practice from the moment they are received by the Lodge Reception until final destruction. All transfers of data must be evidenced in the appropriate log. Access to and the use of recorded material will be strictly for the purposes defined in Section 4 of this Policy.

5.6.3 All requests for a download of CCTV, Cloud-based 4G redeployable cameras or BWV footage should be authorised by the Director of Estates or the Domestic Operations Manager. Where another party (such as the Police, University Security Services or an onsite contractor) seeks access to footage, that party is required to complete the relevant form (Appendix 3) which can be obtained either from the Lodge Reception or from the IT Team. The third party is required to set out why access is required and how any footage will be used. The College will respond within 30 calendar days of receiving the request. Third parties can be categorised as follows:

- Law enforcement agencies including the police
- Prosecution agencies
- Oxford University Proctors or Oxford University Security Services

- An authorised member of the College as part of a formal investigation, where there is a legitimate expectation that the images requested may inform the matters under investigation and that no irrelevant breach of subject privacy will occur.

The college's legal advisor will determine whether release is lawful. In the event of a refusal to release footage, the third party can ask the Vice-Principal to review that refusal. Where the College is unable to comply with a subject access request without disclosing the personal data of another individual who is identifiable, it is not obliged to comply with the request unless satisfied that the individual(s) has given consent to the disclosure. However, if it is deemed reasonable to release the images under the circumstances then the College will comply without having consent from the individual(s). Footage may be released in the absence of the completion of the form in an emergency, for example an ongoing police incident. Such release must be authorised by the Director of Estates (or delegated nominee) or the Domestic Operations Manager. The manager authorising release in this situation is responsible for ensuring that the form be completed retrospectively.

5.6.4 In the interests of processing information only as necessary and in accordance with relevant Data Protection law, the College may direct the requester to view the footage, rather than receive a copy, if appropriate and practical to do so.

5.7 Retention of Recorded CCTV, Cloud-based 4G redeployable cameras and BWV Material

5.7.1 CCTV, Cloud-based 4G redeployable cameras or BWV recordings will be retained on (re-usable if appropriate) media for one calendar month save where a request has been made to retain them by the College, the Police or a third party who has made a request for the footage to be kept. In this case, the footage will be kept until it has been copied and supplied to the party requesting it. There may be specific instructions to keep the footage for an indefinite period pending for example a police investigation, where source material is required. The material should be kept until advised otherwise.

5.7.2 Before reuse or destruction, media will be erased in full accordance with the manufacturer's requirements. Digital recording will be set to overwrite automatically. At the conclusion of their life-span recorded material used within the CCTV System will be destroyed responsibly.

5.7.3 Each discrete item of recorded material (CD, DVD, USB stick etc.) will be registered and monitored from the time it is produced, until it is destroyed, whilst it is within the Lodge Reception. Recorded material will be retained for 1 month from its creation unless there has been a recorded

incident in which this footage may be required. In this case, the footage must be kept for 6 months from the closure of the incident, after which it will be destroyed.

5.7.4 If recorded material is released in accordance with this Policy, a record must be kept which identifies the basis for that release and to whom it has been released to. Records will be retained for at least three years.

Complaints

Complaints about the CCTV system should be made in writing to the Director of Estates at the College.

Equality Impact Assessment

Linacre College is committed to ensuring provided services, recruitment and treatment of staff reflects individual needs, promotes equality and does not discriminate unfairly against any particular individual or group. The Equality Impact Assessment for this policy has been completed by Dr Clara Barker on the 26 May 2023.

Appendix 1

List of Responsible System Managers

Governing Body: The Governing Body has the responsibility to ensure that there is a clear written policy statement that outlines how the College complies with CCTV regulations and delegate the management of the system to the Director of Estates.

Director of Estates: The Director of Estates has overall responsibility for the CCTV System and is the person responsible for ensuring the objectives and principles set out in this policy are upheld.

Domestic Operations Manager: The Domestic Operations Manager is responsible for ensuring that that the CCTV system is operated according to this policy and that the Lodge Reception staff are fully trained and operating the CCTV system.

Lodge Reception Manager: The Lodge Reception Manager has day-to-day responsibility for the monitoring, operation and evaluation of the CCTV system, daily maintenance and cleaning of all cameras, implementation of this policy and maintaining records of the incidents dealt with including CCTV access requests. Further, the Lodge Manager will act as the contact point for all staff, students, visitors or members of the public wishing to enquire about the system. On request enquirers will be provided with a copy of this policy, which is also accessible on our website.

IT Manager: The IT Manager is responsible for the maintenance and repair of the CCTV systems, negotiating the terms of contracts with the CCTV equipment supplier and other related security companies.

Principal: The Principal is the Data Protection Officer for the College.

Appendix 2

Declaration of CCTV Confidentiality

I confirm that my employer [name of employer] has provided me with Information Security Awareness Training relevant to my employment as: [Position]:

I am aware of my potential personal liability and implications for my employer from any negligent or malicious actions when processing data on behalf of the College.

I have familiarised myself with the following policies:
[List the policies]

I have undertaken the following Information Security Awareness Training programmes:
[Date / title of programme / training provider]

Name:

Signature:

Appendix 3

Internal CCTV, Cloud-Based 4G Redeployable Camera and BWV Data Download Request Form

*This form should be completed to facilitate the identification of activities and the collection of evidence, which might warrant disciplinary proceedings being taken against staff or students

1. Requester

First name(s):	Last name:
Job title:	Faculty / Directorate:
Email:	Telephone:

2. Specific information required

Date and time of incident (please use 24 hr clock or mark am/pm):
Exact location:
Description of incident / Reason for Request:

3. Data subject (if applicable)

First name(s):	Last name:
Address: Other identifying information:	

4. Information provision

If we hold information, how would you like the information to be provided?

☐ Electronically using encrypted documents (sent via email with decryption passwords relayed by telephone call)

☐ ect in person (proof of identification required when collecting)

☐ Exchanged digitally by encrypted means

5. Declaration and authorisation

I certify that:

- Non-disclosure would prejudice the case
- I understand information given on this form is correct
- I understand that if any information given on this form is incorrect I may be committing an offence under Section 170 of the Data Protection Act, 2018

Signed:	Date:

6. Authorising line manager*

*this must be a College representative in a sufficiently senior position to authorise this request, normally at a Director's or Bursar's level

First name(s):	Last name:
Job title:	Faculty / Directorate:
Email:	Telephone:

Where to send your request

Please note: If the form has not been fully or properly completed and authorised you will be asked to re-submit your application. Send this form to:

E-mail:

Postal address:

Linacre College Use Only

Release Authorisation Information approved for release:

Yes No

First name(s):	Last name:
Job title:	Department:
Email:	Telephone:

Appendix 4

Disclosure Request Form (Data Protection Act)

Data Protection Act (2018) Request for Disclosure in accordance with Schedule 2 Part 1(2) or Part 1(5)
1. Requestor First name(s): Last name: Job title: Organisation: Address: Postcode: Telephone: Email:
2. Data subject (if known) Current details First name(s): Last name:

Address:
Other identifying information (including date of incident and location)
3. Specific information required
4. Reason for requesting disclosure
Offence(s) or suspected offence(s) (please explain why if this information cannot be provided)
6. Purpose

State the purpose for requesting disclosure of personal information about the data subject specified in section 2 of this form. Please specify the statutory powers you rely on here:
Select one option ☐ **Prevention or detection of crime** ☐ **Apprehension or prosecution of offenders** ☐ **Assessment or collection of tax, duty or imposition of a similar nature** ☐ **for the purpose of, or in connection with, any legal proceedings (including prospective legal proceedings** ☐ **for the purpose of obtaining legal advice**
7. Information provision If we hold information how would you like the information to be provided? ☐ Electronically using Encrypted Documents or by encrypted transfer* *Encrypted documents will be sent via email and decryption passwords will be relayed by telephone call. ☐ Collect in person (Proof of identification required when collecting) We will notify you if we do not hold information or your request for disclosure is refused

8. Declaration and authorisation

The authorising officer must be of the rank of police inspector or higher, or for other 'relevant bodies' a senior officer/manager.

Declaration

I certify that:

- Information requested is compatible with the stated purpose (section 4) and will not be used in anyway incompatible with that purpose

- Non-disclosure could prejudice the case

- The information given on this form is correct and complete to the best of my knowledge

I understand that if any information given on this form is incorrect, I may be committing an offence under Section 170 of the Data Protection Act, 2018

Requestor

Signed:

Date:

The College requires a wet signature

Authorising Officer (Requesting Organisation)*

***this must be an officer of the organisation, in a sufficiently senior position to authorise this request: rank of Sergeant or above

First name:

Last name:

Job title:

Signed:

Date:

The College requires a wet signature