Policy number:	HS213	**Originator:**	IT Manager
SharePoint:	Policies and Procedures:		
EIA Meeting Date:	06 July 2017	**EIA Required:**	YES
Approved by:	SMT	**Date:**	13 March 2020
Review Frequency:	Annually		
Review Date:	November 2023 (reviewed Nov 22 minor changes)		
External Web Site appropriate:	YES		
Linked policies/College documents:	Data Protection Policy Information Security Policy		
Summary available:	NO		

CCTV Policy

This document can be made available in other formats, on request

The policy may not need to be reviewed annually but Appendix 2, The Checklist for Users of Limited CCTV Systems, will need to be completed annually in May each year before the ICO renewal in July.

Key Points

- Newbury College maintains internal video surveillance technology to deter and assist in the prevention or detection of crime, monitor security and identify actions which might result in disciplinary action.
- The operation of the systems must be consistent with individuals' rights to privacy.
- The external video surveillance technology is administered by MITIE, not Newbury College.
- Images are likely to be personal data as defined by the Data Protection Act 1998 (DPA) and so must be processed in accordance with the Act, kept secure and destroyed within the agreed retention period. The Information Commissioner's CCTV Code of Practice must be followed.
- Individuals have rights to access images of themselves.
- Third parties may request copies of images in specified circumstances. This is likely to be to law enforcement agencies, prosecution agencies and appropriate members of Newbury College staff.
- Signs must be prominently displayed informing people that monitoring is in use.
- The IT Manager is responsible for compliance with and implementation of this policy.
- The Data Protection Officer is responsible for advising on compliance with the DPA and other legislation in relation to surveillance technology.
- The Finance Director is accountable for ensuring compliance with the policy.

1. Purpose

1.1 This policy sets out the accepted use and management of video surveillance systems or any other surveillance technology including CCTV to ensure that Newbury College complies with its legal obligations and respect for individual privacy of its students, staff, contractors and visitors.

2. Scope and definitions.

2.1 This policy covers the use of surveillance technologies which record identifiable images of people on Newbury College premises.

2.2 CCTV is defined as: fixed cameras designed to capture and record images of individuals.

2.3 Surveillance System is defined as: any electronic system or device that captures images of individuals or information relating to individuals. This term is used in this policy to refer to any surveillance technology including CCTV. It includes any technology that may be introduced in the future for a similar purpose such as automatic number plate recognition (ANPR), body worn cameras or aerial surveillance.

2.4 Current Video Surveillance systems

2.4.1 Newbury College has in place video surveillance systems to provide a safe and secure environment for students, staff and visitors, and to protect college property.

2.4.2 Newbury College carries out Threat and Security Risk Assessments as required by British and European standards to identify where there is a requirement for video surveillance technology. Reasons for a decision to install may include but are not limited to the following:

- Deter crime
- Assist in prevention and detection of crime
- Assist with the identification, apprehension and prosecution of offenders
- Assist with the identification of actions that might result in disciplinary proceedings against staff and students
- Monitor security of campus buildings
- Identify vehicle movement problems around the campus. These cameras are the responsibility of MITIE.

2.5 Operation of the systems

- The systems will be provided and operated in a way that is consistent with an individual's right to privacy.
- The Internal Video surveillance systems operate during Standard opening hours of the building.
- Responsibility for management of the systems is with the IT Services Department.
- External Surveillance cameras are located at strategic points on the campus, principally at the entrance and exit point of sites and buildings. All cameras will be positioned to only capture images from the areas intended as detailed in site specific Security Risk Assessments (SRA). These cameras are the responsibility of MITIE.

- CCTV signs will be prominently placed at strategic points and at entrance and exit points of the campus to inform staff, students, visitors and members of the public that a CCTV installation is in use. These must state that monitoring is in use, the name of the organisation responsible, the reason for the monitoring and give contact details for any enquiries. External cameras are the responsibility of MITIE.

- If an awarding body stipulates the use of CCTV as part of their regulations, we will put temporary cameras in place for exams. These recordings will be kept for the same duration as all other CCTV recordings unless a longer duration is specifically required by the awarding body.

2.6. The systems will not be used to:

- Provide images to the world wide web
- Disclose to the media

3. Legislative framework

3.1 Relevant legislation is:

- The Data Protection Act 1998 (DPA). This covers the rights of individuals (data subjects) in respect of their personal data. Identifiable images of individuals are personal data.

- The Human Rights Act 1998 (HRA) enshrines "respect for private and family life."

3.2 Newbury College has produced this policy in line with the Information Commissioner's (ICO) CCTV Code of Practice 2015.

3.3 Digital images

If images show a recognisable person, they are personal data and are covered by the Data Protection Act 1998. Newbury College's Data Protection Policy, should be adhered to at all times. It is overseen by the Data Protection Officer.

3.4 Newbury College is required to register its processing of personal data (including images) with the Information Commissioner's Office (ICO). The College's ICO notification registration number is Z6979501, renewed annually in July.

3.5 Where new cameras are to be installed on college premises the following assessment will include the following:

- The appropriateness of and reasons for using video surveillance will be assessed and documented;

- The purpose of the proposed surveillance system will be established and documented;

3.6 Responsibility for

- Day-to-day compliance with this policy will be established and documented;

- Consultation with the Data Protection Officer is required to ensure that the video surveillance system is covered by the College's Notification with the Information Commissioner's Office (ICO);

- Where new uses are proposed for video surveillance systems, these should be subject to a Privacy Impact Assessment (PIA) in accordance with the ICO Code of Practice on Privacy Impact Assessment.

3.7 Individual access rights (Subject Access Requests)

3.7.1 The Data Protection Act 1998 gives individuals the right to access personal information about themselves, including images.

3.7.2 All requests for access to a copy of video footage by individuals should be made via the CCTV Authorisation Request on SharePoint.

3.7.3 Requests for access to CCTV images must include:-

- The date and time the images were recorded
- Information to identify the individual, if necessary
- Proof of identity
- The location of the camera

3.7.4 The College will respond promptly and at the latest within 40 calendar days of receiving the £10 request processing fee and sufficient information to identify the images requested.

3.7.5 If the College cannot comply with the request, the reasons will be documented.

3.7.6 The requester will be advised of these in writing, where possible.

3.7.7 It may be necessary to involve a third party contract to obscure footage. This could be internal (Media Technician) or external. A written contract will be detailed and signed to provide explicit security.

3.8 Access to images by third parties

3.8.1 Unlike Data Subjects, third parties who wish to have a copy of CCTV images (i.e. images not of the person making the request) do not necessarily have a right of access to images under the DPA, and care must be taken when complying with such requests to ensure that neither the DPA, HRA or the CCTV Policy are breached.

3.8.2. Routine access to images will be restricted to those staff that need to have access in accordance with the purposes of the system.

3.8.3 Disclosure of recorded material will only be made to third parties in strict accordance with the purposes of the system and is limited to the following:-

- Law enforcement agencies (where the images recorded would assist in a specific criminal enquiry, and at the College's discretion).

- Prosecution agencies.

- Appropriate members of Newbury College staff (such as Human Resources and the Student Conduct, Complaints and Appeals team) in the course of staff or student disciplinary proceedings (including prospective proceedings) to ensure compliance with the college's regulations and policies.

- People whose images have been recorded and retained (unless disclosure to the individual would prejudice criminal enquiries).

3.8.4 All third party requests for access to a copy of video footage should be made in writing to the Data Protection Officer. If a law enforcement or prosecution agency is requesting access they should make a request under Section 29 of the Data Protection Act 1998.

3.8.5 Images that have been recorded may be viewed on site by the individual, or a copy provided for a law enforcement or prosecution agency. A record of the request will be recorded on the IT Services Department ticket system.

3.9 Requests to prevent processing

3.9.1 In addition to rights of access, Data Subjects also have rights under the DPA to prevent processing (i.e. monitoring and recording CCTV images) likely to cause substantial and unwarranted damage to that person, or prevent automated decision taking (i.e. through the use of visual recognition software) in relation to that person.

3.9.2 Should a Data Subject have any concerns regarding the operation of the CCTV systems, the following procedure must be complied with:

- The Data Subject should be directed to the Data Protection Officer to determine whether the Data Subject is making a request to prevent processing or automated decision making. If the Data Protection Officer determines that the Data Subject is instead making a Subject Access Request, the procedure will be followed.

- The Data Protection Officer will consider the request to prevent processing or automated decision making in consultation with appropriate staff.

3.9.3 The Data Protection Officer will normally provide a written response within twenty-one days of receiving the request to prevent processing or automated decision making, setting out their decision on the request. A copy of the request and response will be retained.

3.10 Retention and disposal

3.10.1 Unless required for evidential purposes or the investigation of crime or otherwise required by law, recorded images will be retained for no longer than 21 days from the date of recording.

3.10.2 At the end of their useful life all images stored in whatever format will be erased securely and permanently and where in physical form, for example tapes or discs, disposed of as confidential waste. All still photographs and hard copy prints also will be securely disposed of as confidential waste.

3.11 Covert monitoring

3.11.1 Covert monitoring (where the individual is not aware the monitoring is taking place) will only be justifiable in exceptional circumstances where there are grounds to suspect criminal activity or extremely serious malpractice. If such monitoring is undertaken:

- It must be with the authorisation of the College Principal;
- The decision to adopt covert recording will be fully documented and will set out how the decision to use covert recording was reached and by whom;
- It 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;
- The risk of intrusion on innocent workers is considered;
- Areas where a high level of privacy is expected remain private;
- Only limited numbers of people will be involved in the monitoring.

3.12 Access to images by staff

3.12.1 Access will be restricted to those staff that need to have access in accordance with the purposes of the system.

4. Accountability and Responsibility

4.1 The Internal CCTV surveillance system is owned by Newbury College.

4.2 Data Governance and Strategy Group are responsible for approving and reviewing this policy.

4.3 The Policy Lead is the Data Protection Officer.

4.4 The Finance Director is responsible ensuring compliance with this policy.

4.5 Authorisation for new CCTV camera installations or other installation or use of surveillance technologies must be given in writing by the Finance Director.

4.6 The Finance Director is accountable for ensuring compliance with the policy.

4.7 The Data Protection Officer is responsible for advising on compliance with the DPA and other legislation.

5. Encryption

5.1 Digital storage is not encrypted but located in a secure, controlled environment.

6. Monitoring

6.1 This Policy will be reviewed annually or when the law or guidance changes.

6.2 The Data Protection Officer is responsible for:

- Maintaining this policy
- Providing expert guidance on the application of the DPA
- Providing guidance regarding subject access requests and third party requests for access to footage.
- Providing guidance, support and training
- Liaison with the Information Commissioner's Office, including annual notification to the ICO

7. Documentation

7.1 Appendix 2, Checklist for Users of Limited CCTV Systems, must be re-completed annually prior to the annual payment to the ICO

7.2 If additional surveillance cameras are added a Privacy Impact Assessment (PIA) (Appendix 1) and CCTV Risk Assessment (Appendix 4) must be completed to confirm the eligibility of the requirement. The map, Appendix 3, showing the camera locations must also be updated.

8. Associated policies and guidance

- Data Protection Policy
- In the picture: a data protection code of practice for surveillance cameras and personal information. ICO, 2015 (https://ico.org.uk/media/1542/cctv-code-of-practice.pdf)
- Information Security Policy

Date: July 2017
Reviewed: May 2018, March 2020, November 2022
Review Date: November 2023