



Data Protection & CCTV

Policy 2026-27

GDPR Manager

Publication: August 2026

Review: August 2027| Version No 1.0

1. Policy Statement

- 1.1. City of Wolverhampton College needs to ensure the safety and security of students, staff, visitors, and resources. To this end the College uses CCTV technology to provide image-based monitoring of its Estates and facilities operates a Closed-Circuit Television (CCTV) system to promote a safe and secure environment for students, staff, visitors, and property. This policy ensures the CCTV system is used lawfully, transparently, and proportionately in accordance with UK General data Protection Regulations, Data Protection Act 2018, Information Commissioner Office (ICO) CCTV code of Practice.

2. Purpose

- 2.1. The purpose of this policy is to ensure that City of Wolverhampton College meets its legal, statutory and regulatory requirements under the data protection laws and to ensure that all personal and special category information is processed compliantly and, in the individuals, best interest.
- 2.2. The purpose of this CCTV Policy is to ensure that City of Wolverhampton College operates its CCTV systems in compliance with data protection laws and in a way that protects the rights, freedoms, and privacy of individuals. The policy sets out how CCTV footage is collected, used, stored, and shared, and ensures that all processing of personal data captured by CCTV is lawful, fair, transparent, and carried out in the best interests of the College community for purposes including security, crime prevention, and safeguarding.
- 2.3. The Policy is specifically to inform staff and users of Wolverhampton College premises and facilities of the arrangements for the placement and management of CCTV. In addition, this Policy provides information about the retention of CCTV images where the College has responsibility for the systems in use.
- 2.4. This Policy informs staff, students, visitors, and other users of City of Wolverhampton College premises about the arrangements for the deployment, operation, and management of the College's CCTV systems. It also sets out how CCTV images are collected, used, stored, and retained in accordance with data protection legislation, and clarifies the College's responsibilities as the data controller for CCTV systems under its control.
- 2.5. CCTV has been installed in our server rooms to assist in deterring crime, and also the prevention and detection of crime. The implementation of CCTV technology is intended to assist with the identification, apprehension and prosecution of offenders, and the identification of actions that might result in disciplinary action.

- 2.6. CCTV has been installed in the College's server rooms to deter crime and to support the prevention and detection of unauthorised activity, anti-social behaviour, incidents and misconduct. The use of CCTV in these areas is intended to assist in the identification, apprehension, and prosecution of offenders, as well as to identify actions or behaviours that may lead to disciplinary proceedings.
- 2.7. The existence and position of CCTV will help to deter any unauthorised access to server rooms, protect college property and assets, and assist law enforcement when legally required.

3. Scope

- 3.1. This policy applies to individuals working for or acting on behalf of City of Wolverhampton College (meaning permanent, fixed term, and temporary staff, any third-party representatives or sub-contractors, agency workers, volunteers, interns and agents engaged with City of Wolverhampton College).
- 3.2. Compliance with this policy is mandatory and failure to adhere to the requirements set out in this Policy may result in disciplinary action, contract termination, or other appropriate measures.
- 3.3. The policy covers Camera operation, Recording and storage, Access to footage, Disclosure of recording and Data retention.

4. Introduction

- 4.1. City of Wolverhampton College uses CCTV for the purposes of the prevention and detection of crime and to recognise and identify individuals with a view to taking appropriate action where necessary.
- 4.2. This document sets out the accepted use and management of CCTV equipment and images to ensure that Wolverhampton College complies with the Data Protection Act 2018 and other relevant legislation. We process personal data in line with our Data Protection Policy.
- 4.3. City of Wolverhampton College will also be cognisant of the Guiding Principles of the Surveillance Camera Code of Practice as published by the Home Office and updated in 2021.
- 4.4. This policy and procedure apply to all Wolverhampton College Campuses, Sites and Facilities.

5. Legal Basis for Processing

- 5.1. The City of Wolverhampton college consider CCTV images as personal data where individuals can be identified. The college processes CCTV data under the lawful basis of:
 - Legitimate interests (security and crime prevention)

- Legal obligations where disclosure to authorities is required

5.2. The college ensures that the use of CCTV is necessary and proportionate and that less intrusive alternatives have been considered.

5.3. A Data Protection Impact Assessment (DPIA) or Legitimate impact assessment (LIA) will be conducted before installing or significantly expanding CCTV systems.

6. Location Of Cameras

6.1. The City of Wolverhampton college may install cameras in appropriate areas such as Building entrances and exits, Corridors and common areas, Car parks, Reception areas, External campus spaces.

6.2. The City of Wolverhampton college will not be installed in areas where individuals reasonably expect privacy, including Toilets, changing rooms, Prayer rooms, Private offices (unless exceptional circumstances apply).

7. Signage And Transparency

7.1. The city of Wolverhampton College has display clear signage across the campus to inform individuals that CCTV is in operation. Signage will include Notification that recording is taking place, The purpose of CCTV monitoring, Contact details for further information.

7.2. This ensures transparency in line with requirements set by the UK Data Protection Act 2018 and the Information Commissioner's Office (ICO).

8. Management Responsibilities for CCTV System

8.1. The Estates Department has overall responsibility for the maintenance of the system. They will periodically check the equipment and arrange for the suppliers to carry out periodic maintenance checks.

8.2. The Security Team will ensure that images are deleted in accordance with the retention policy. Members of the Security Team and ADT will have access to the recorded images during the maintenance of the systems but will under no circumstances routinely view, disclose or retain copies of the recorded images.

8.3. Members of the Security Team and Estates department will be trained in the operation of the CCTV system and will be aware of the data protection compliance requirements in line with the Code of Practice.

9. Auditing The System's Operation, Access to and Disclosure of Images

- 9.1. The Data Protection Officer (in conjunction with the Funding and Compliance Team) is responsible for ensuring that this policy and its implementation is compliant with Data Protection Legislation and will audit the system's use on a periodic basis.
- 9.2. The College's Security Manager and Data Protection Officer are responsible for dealing with and responding to any requests for access to images made by CCTV Policy. Any requests received into the College for access to images must be forwarded to the College's Security Manager (cc'd to the Data Protection Officer) to be progressed using existing procedures.
- 9.3. The Security Manager, or delegated managers within their department, is responsible for viewing images when investigating an incident or suspected incident.
- 9.4. Images may also be accessed by the relevant Investigating Manager, if necessary, as part of a disciplinary investigation. Images may then be disclosed as part of the evidence assembled by the Investigating Manager in the event of a disciplinary hearing.
- 9.5. The College access to CCTV recordings is strictly limited to authorised personnel only, including Data Protection Office, Facilities or Security Manager, Senior management where required for investigation. All access to CCTV footage must be logged and auditable. Unauthorised access, copying, or sharing of CCTV footage is strictly prohibited and may result in disciplinary action.
- 9.6. The College may also disclose CCTV footage when necessary and lawful. Disclosure may occur to Law enforcement agencies investigating criminal activity, Regulatory authorities where legally required, Individuals making a Subject Access Request (SAR) under data protection law.
- 9.7. Requests from external organisations must be authorised by the Data Protection Officer.
- 9.8. Any request for the release of CCTV footage to law enforcement must be submitted through a formal DP1 request, and no images will be disclosed unless this process is completed and validated by the Data Protection Officer.

10. Secure Storage and Retention of Images

- 10.1. Images will be stored on the recording equipment which will be securely protected. The Security Team have responsibility for ensuring that the equipment and the routinely recorded images have the necessary security. Images are routinely retained for one month but may be retained longer in the event that they are required as part of an investigation.

- 10.2. The City of Wolverhampton College will on retain CCTV recordings for as long as necessary. The college will normally retain CCTV for 30 days unless required incident
- 10.3. Investigation, Legal proceedings, Police request. Footage required for investigations will be securely stored until the case is closed.
- 10.4. Where images have been retained for an investigation the Security Team will take responsibility for the secure storage of those images. This will be done in liaison with an appointed Investigating Manager where necessary for disciplinary purposes.

11. CCTV Data Security

- 11.1. The City of Wolverhampton College has implemented appropriate security to protect CCTV recordings, including Restricted system access, Secure servers or encrypted storage, Password-protected systems, Controlled viewing areas.
- 11.2. CCTV systems will be maintained regularly by the College IT Team to ensure security and functionality.

12. Individual Rights

- 12.1. The College understands individuals have rights under the UK General Data protection Regulation including:
- The right to request access to their personal data
 - The right to request erasure where appropriate
 - The right to raise concerns about surveillance
- 12.2. The College will respond to requests, queries, and requests for information. All Subject Access Requests (SARs) must be submitted to the Data Protection Officer via email at dataprotection@wolvcoll.ac.uk.