Mae'r ddogfen hon hefyd ar gael yn Gymraeg

This document is also available in Welsh

SURVEILLANCE SYSTEM POLICY

Author	Director of Policy, Assurance and Compliance
Version	1.3
Status	Final
Date Approved	12th March 2026
Approved by	Audit and Risk Committee
Effective Date	12th March 2026
Date of Next Review	31st March 2028
Responsibility for Review	Director of Policy, Assurance and Compliance
Equality and Welsh Language Impact Assessment	Y
Health and wellbeing implications considered	Y

Version	Date	Description	Amended/Reviewed by
1.0	28.11.25	Draft Policy completed.	Director of Policy, Assurance and Compliance
1.1	12.03.26	Minor corrections to section numbering	Director of Policy Assurance and Compliance
1.2	12.03.26	Policy approved by Audit and Risk Committee	Director of Policy, Assurance and Compliance

Table of Contents

1. Scope and Purpose

1.1: **Purpose**

The purpose of this Policy is to set out the College's strategic approach to the responsible use of surveillance systems.

The College is the owner and operator of all surveillance systems deployed on its estate, including CCTV, ANPR and Body-Worn Video. The systems are installed, managed and governed by the College to support its statutory duties in relation to safety, safeguarding, security and the effective operation of the campus. All equipment, data and recordings are under the control of the College and are managed in accordance with this Policy, associated Procedures and the requirements of data protection law.

Surveillance will only be deployed where it is necessary, lawful, proportionate and targeted, in compliance with:

- UK GDPR and the Data Protection Act 2018
- Protection of Freedoms Act 2012
- Surveillance Camera Code of Practice (Home Office, 2021)
- Human Rights Act 1998 (Article 8 the Right to Private Life)

The Policy establishes the College's commitment to:

- Protecting the safety and security of its community.
- Safeguarding its premises and assets.
- Supporting legitimate investigations (safeguarding, disciplinary, security and incident reviews).
- Ensuring transparency and accountability in how surveillance data is used.
- Maintaining public confidence through clear governance, appropriate oversight and regular review.

1.2: **Scope**

This policy applies to all forms of surveillance operated by the College, including but not limited to:

- Fixed CCTV systems
- ANPR and vehicle access systems
- Body-worn Video
- Any future surveillance technologies approved through the College's Change Control process.

It applies to all staff, students, contractors, visitors and third parties who may appear in surveillance recordings.

The operational detail for implementing this policy is set out in the *Surveillance Systems Procedures*, including requirements for system operators.

1.3: **Links with related policies and procedures**

This policy aligns with and support a range of college policies and procedures to ensure a unified approach to data and records management. It should be read in conjunction with:

- Surveillance System Procedures
- The Data Protection Policy and Procedures

- Records management Policy and Procedures
- Data Breach Policy and Procedures
- IT Policy – Internal Systems
- Safeguarding and Child Protection Policy
- Health and Safety Policy
- Equality and Diversity Policy
- Examinations Policy and Procedures

1.4: **Relevant Legislation and regulatory frameworks**

This policy is designed to comply and be informed by key legislation, regulatory frameworks and government and industry guidance including:

- UK General Data Protection Regulation (UK GDPR)
- Data protection Act 2018
- Human Rights Act 1998
- Protection of Freedoms Act 2012
- Surveillance Camera Code of Practice
- ICO and Biometrics and Surveillance Camera Commissioner guidance

The College will have regard to relevant approved operational, technical and competency standards for surveillance systems (for example the BS EN 62676 series, BS7958 and BS8593) and, where proportionate and practicable, will work towards maintaining those standards in the design, operation and review of its systems.

2. Definitions

2.1: **Surveillance Systems:** Any fixed or mobile camera, or networks of cameras, used for monitoring or recording images or information for security, safety or operational purposes.

2.2: **Personal Data:** Information that relates to an identified or identifiable individual, captured through surveillance systems.

2.3: **Data Controller:** The College, as the organisation determining the purpose and means of operating surveillance systems.

2.4: **Data Processor:** A third party acting on behalf of the College, responsible for installing, maintaining or managing surveillance equipment or data under contract.

2.5: **Data Protection Impact Assessment (DPIA):** An assessment that evaluates and mitigates privacy and human rights risks associated with surveillance activities.

2.6: **System Operator:** A member of college staff designated and trained to monitor, review or retrieve footage from surveillance systems in line with the College policy and Surveillance System Procedures.

3. Policy Statement

3.1: Key Principles

The College will operate all surveillance systems in line with the following principles:

- **Legitimacy and Lawfulness:** Surveillance will only be used for lawful clearly defined purposes i.e. safety and security and prevention and detection of crime.

- **Necessity and Proportionality**: Surveillance will not be used where a less intrusive means could achieve the same outcome.
- **Purpose Limitation**: Surveillance data will only be processed for the defined purposes listed in this policy, and any compatible purposes approved through a DPIA.
- **Transparency**: The College will communicate clearly about the presence, purpose and lawful basis for surveillance through signage and privacy notices.
- **Accountability**: Decisions relating to surveillance access, disclosure and retention will be fully traceable, recorded in the *Surveillance Asset Register* and subject to routine audit.
- **Data Minimisation**: Footage access is restricted to the minimum required for a defined, legitimate purpose.
- **Data Protection by Design:** Privacy and data protection will be embedded from the design stage of any new system or upgrade.
- **Retention and Security:** Data captured by surveillance systems will be retained only for as long as necessary and protected through appropriate technical and organisational measures.
- **Regular Review:** Surveillance systems will be reviewed periodically to ensure ongoing compliance, justification and effectiveness.

3.2: Key Commitments

The College makes the following commitments to ensure that surveillance activities remain lawful, accountable and proportionate in practice.

3.1(i) Legitimacy and Lawfulness

Surveillance systems will only be used for purposes that are lawful, fair and transparent as required under UK GDPR requirements.

- Each surveillance activity will be based on a clearly defined lawful basis under UK GDPR and recorded as part of the *IAR and ROPA Register*. Where surveillance captures special category data or criminal offence information an appropriate condition will also be recorded.
- The College will ensure signage and privacy information clearly communicate the presence and purpose of surveillance.

3.1(ii) Necessity and Proportionality

The College will ensure that any surveillance measure is necessary to achieve a clearly defined objective(s) and proportionate to the problem it seeks to address.

- Before modification and installation of new surveillance systems or functions, the College will assess privacy risks and seek to identify if there are less intrusive alternative to achieve the objective.
- Surveillance systems will only be deployed where no reasonable and less invasive means are available to achieve the same legitimate purpose.
- The scale, positioning and technical capabilities of the cameras will be proportionate to the identified risk, avoiding monitoring of areas where individuals have a higher expectation of privacy.
- The College will review justifications to ensure objectives remain relevant and proportionality is maintained.

3.1(iii) Purpose Limitation

The College will only use surveillance systems to monitor and record areas of the College site for the following purposes:

- For the safety and security of staff, students, visitors, contractors and other individuals who enter the College's premises.
- For the security of college assets
- For prevention, reduction, detection and investigation of incidents of crime
- To assist in the investigation of suspected breaches of the College's policies, procedures, regulations and codes of conduct.
- To monitor and manage vehicle access, traffic flow and delivery incidents

3.1(iv) Transparency and Accountability

The College will ensure that all surveillance activity is transparent and that accountability is demonstrable.

- Signage will be positioned clearly at entry points to monitored areas and include the College's identity, purpose of monitoring and surveillance query contact details.
- The College will maintain detailed records of DPIAs, asset inventories, access logs, disclosures and reviews in line with UK GDPR accountability principle.

3.1(v) Data Protection by Design and Default

The College will embed privacy and data protection into the design and configuration of all surveillance systems.

- Technical settings will ensure that only data necessary for the intended purpose is captured and retained.
- New systems or upgrades will not be implemented without a Data Protection Impact Assessment (DPIA).
- Camera positioning, resolution and recording features will be configured to avoid unnecessary or excessive collection of personal data.

3.1(vi) Retention, Security and Integrity

The College will maintain appropriate security and retention controls to safeguard surveillance data.

- Footage and associated data will be stored securely with restricted access, encryption and multi-factor authentication where possible.
- Retention periods will be defined in the Records Retention Schedule.
- Secure deletion will be applied when retention periods expire. Deletion will be automated unless the data is marked as evidential where it will be manually deleted in line with the Records Retention Schedule.
- Any data breach involving surveillance information will be managed under the College's Data Breach Policy.

3.1(vii) Rights of Individuals

The College recognises and upholds the rights of individual in relation to surveillance data.

- The College will managed data subject rights in relation to surveillance systems under the Data Protection Policy and Procedures.
- Requests to access surveillance data will be assessed to balance privacy, safeguarding and legal obligations.

3.1(viii) Regular Review and Continuous Improvement

The College will ensure that surveillance systems are regularly reviewed for compliance, necessity and proportionality as required by the Surveillance Code of Practice.

- Annual system reviews will be conducted and actions identified implemented as required.
- DPIAs will be updated when systems change or new risks emerge.

4. Responsibilities

4.1: **Governors**

- Provide strategic oversight and supports a culture of accountability.
- Receives reports on the operation and compliance of surveillance system.

4.2: **Senior Leadership Team (SLT)**

- Approves the strategic purpose and scope of surveillance systems.
- Ensures compliance within their areas of responsibility.

4.3: **Director of Policy, Assurance and Compliance (and the DPO)**

- Lead on the development, implementation and review of surveillance policies and procedures.
- Ensure DPIAs are conducted and reviewed.
- Advise on compliance with data protection and human rights obligations.
- Serve as the point of contact for the ICO and Biometrics and Surveillance Camera Commissioner.

4.4: **Head of IT**

- Ensure the technical security of surveillance systems, including access control and system integrity.
- Support investigation and recovery in the event of a data breach.

4.5: **System Operators**

- Operate surveillance system in accordance with this policy and Surveillance System Procedures.
- Ensure accurate recording and secure handling of footage and associated data.
- Immediately report any suspected misuse, unauthorised access or system malfunction to the Director of Policy, Assurance and Compliance and the Head of IT.

4.6: **Deans, Directors, Departmental Managers and Learning Area Leads**

- Ensure compliance with Surveillance System Policy and Procedures within their areas.

4.7: **All Staff**

- Understand and comply with this policy and the Surveillance System Procedures.
- Report any concerns, suspected misuse or data protection issues promptly to the Director of Policy, Assurance and Compliance and the Vice Principal Systems Development & Funding.

5. Complaints

Individuals who have concerns about the College's use of surveillance systems, the handling of their personal data or decisions made in response to data subject right requests or freedom of information requests should email dataprotection@stdavidscollege.ac.uk in the first instance who will review the matter in accordance with the College's Data Protection Procedures, Surveillance System Procedures and Freedom of Information Procedures. If the individual remains dissatisfied after the College's

internal review, they have the right to raise their concerns with the Information Commissioner's Office (ICO).

6. Equality and Welsh Impact Assessment Statement

An Equality and Welsh Language Impact Assessment has been completed. Overall, the surveillance Policy and accompanying Procedures have a predominantly positive or neutral impact across all protected characteristics. The measures in place strengthen safety, support fair and unbiased investigations and deter discriminatory behaviour. Strong governance, the *Justified Access Test*, annual reviews and redaction processes ensure no protected group is disproportionately targeted or affected. In relation to Welsh Language Standards, the impact is positive or neutral. Bilingual signage, privacy information and communication routes ensure Welsh speakers are not disadvantaged. The system operates in a language neutral way while enabling compliance with statutory requirements.

7. Communication and Storage

7.1: This policy and relating procedures will be available to staff on the 'Every' platform.

7.2: This policy will be published on the website.

7.3: This policy will be available in Welsh.