[INSERT SCHOOL LOGO]

Surveillance Camera Systems Policy

[School Name].

Version 1 – 2024

Document Control:

Organisation	[School Name]
Title	Surveillance Camera Systems Policy
Author	[Head Teacher] in conjunction with Information Compliance at Powys County Council
Owner	[Head Teacher]
Protective Marking	No protective marking
Version	1
Review Date	N/A
Publication Date	2024

Revision History:

Revision Date	Revision	Previous Version	Description of Revision
V0.1	Draft	N/A	Development of Policy
V1	Approved	V0.1	Approved by relevant groups referred to below.

Policy Document Approvals:

This document has obtained the approval from the following Groups:

Sponsor Approval:	Date Approved:
(Powys County Council) Corporate Information Operational Governance Group	**30/04/2024**
(Powys County Council) Unions	**17/05/2024**
(Powys County Council) Corporate Information Governance Group	**18/07/2024**
Add school-related groups if appropriate	

Policy Contents:

1. Policy Introduction & Statement

1.1. For the purposes of this policy, surveillance camera systems include Closed-Circuit Television (CCTV), body worn cameras, drones, vehicle cameras (including internal and external fixings), mobile phones, and any other device that has the capability of capturing:

- visual and/or
- audio and/or
- Location data.

1.2. This policy governs the implementation, modification, and operation of surveillance camera systems to ensure the implementation of such meets their given purpose, lawfully.

1.3. A list of key definitions and acronyms is set out at Section 11.

2. Policy Purpose

2.1. [SCHOOL NAME] will, when implementing or modifying surveillance camera systems, aim to achieve compliance with:

- Data Protection legislation,
- Information Request legislation,
- The Human Rights Act 1998,
- The Regulation of Investigatory Powers Act 2000,
- The Protection of Freedoms Act 2012,
- The Home Secretary's Surveillance Camera Code of Practice, and
- The Information Commissioner's Office ('ICO') CCTV Code of Practice.

2.2. The consequences of failing to abide by this policy may result in a risk of non-compliance with legislation set out in 2.1., which could result in increased complaints, loss of public confidence, reputational damage and in some cases, regulatory action taken against [SCHOOL NAME].

2.3. For this policy to be effective, [SCHOOL NAME] employees must ensure that they have read and understood its key messages before implementing new, or modifying existing, surveillance camera systems.

3. Policy Scope

3.1. This policy applies to anyone in [SCHOOL NAME] and third-party processors involved in the procurement, implementation, modification, and/or operation of surveillance camera systems.

4. Assessing Surveillance Camera Systems

4.1. Staff responsible for [SCHOOL NAME] initiatives that involve the use of surveillance camera systems will, in accordance with Article 35 (1) of the UK GDPR, conduct a Data Protection Impact Assessment (DPIA) before such initiatives enter the implementation phase, since the processing of personal data using such systems will be considered "likely to result in [a] high risk to [the] rights and freedoms [of individuals]"

4.2. All DPIAs should be reviewed regularly, and particularly when a surveillance camera system is modified at a later stage.

4.3. Through the undertaking of a DPIA, [SCHOOL NAME] will determine whether deployment is lawful, fair, and the levels of intrusion acceptable. The DPIA itself will also act as a record of how [SCHOOL NAME] has considered and addressed any risks or wider concerns about the initiative.

4.4. The use of camera surveillance systems, including the field of vision, must be proportionate to the identified need.

4.5. The ICO & the Biometrics and Surveillance Camera Commissioner have jointly produced a Data Protection Impact Assessment (DPIA) template and associated guidance which focuses specifically on surveillance camera systems which should be used. The most up to date template and guidance can be obtained by contacting information.compliance@powys.gov.uk

5. Managing Data Captured through Surveillance Camera Systems

5.1. *Storage and retention*:

5.1.1. Personal data captured through surveillance camera systems that is no longer required will be deleted.

5.1.2. CCTV systems operated by [SCHOOL NAME] shall normally retain footage for no longer than 30 days. Where footage is required for the purposes of prosecution of an offence or to defend against legal claims, a copy should be made and stored securely.

5.2. *Access*:

5.2.1. Personal data captured through surveillance camera systems and retained by [SCHOOL NAME] will be accessible on a limited basis, to authorised individuals only, and will not be made widely available or distributed without consideration as to the purpose of access/disclosure.

5.2.2. Monitors displaying live images being captured by surveillance camera systems should only by seen by staff authorised to use the equipment.

5.2.3. Retrospective viewing of images captured by surveillance camera systems should take place in a restricted area to which other employees or third parties will not have access to whilst viewing occurs.

5.2.4. If the surveillance camera systems supplier (or other 3rd party support) is required to provide technical assistance with any operational element of a surveillance camera system, and through doing so will require access to repositories where personal data resides, then [SCHOOL NAME] will ensure that only limited and specific personal data is accessible, where possible.

5.2.5. [SCHOOL NAME] ensures that Data Processing Agreements (DPAg) are in place between them and the surveillance camera systems supplier or supporting organisation should any processing, including access, of personal data be required.

5.3. *Disclosure*:

5.3.1. Disclosure of personal data, captured through surveillance camera systems and retained by [SCHOOL NAME] will only be made in accordance with the purpose(/s) for which the surveillance camera system is being used, or when law allows.

5.3.2. All requests for disclosure of footage shall be made in writing explaining fully why the disclosure is required and shall be submitted to the service area responsible for the footage.

5.3.3. [SCHOOL NAME] may disclose non-personal identifying data captured through surveillance camera systems in response to a Freedom of Information or Environmental Information request unless the information is found to be exempt from disclosure.

5.3.4. [SCHOOL NAME] will disclose personal identifiable data to a requester who submits a Subject Access Request (SAR) but will remove data that identifies other individuals unless it is reasonable not to do so.

5.4. *Security*:

5.4.1. The security of surveillance camera systems will be assessed to ensure adequate protection of personal data, and that it meets appropriate security standards.

6. Training

6.1. All individuals, including [SCHOOL NAME] members of staff or third parties responsible for the operation of surveillance camera systems must ensure that all necessary training surrounding the use of equipment is undertaken.

6.2. [SCHOOL NAME] will ensure that staff are sufficiently skilled and competent to use the equipment to minimise inappropriate data handling incidents.

6.3. Training should be revisited regularly especially when any surveillance camera system is modified to include additional functionality.

6.4. All [SCHOOL NAME] employees undertake mandatory Cyber Security and GDPR training on an annual basis.

7. Audit

7.1. All data captured through surveillance camera systems must remain on school-approved systems.

7.2. Should any data captured through surveillance camera systems be required to be removed from school systems and placed onto, for example, removeable media devices, then the staff will ensure that the sharing of personal data is lawful and secure.

7.3. Those operating the surveillance camera system(/s) will ensure that the system is capable of producing audit logs that may be accessed and viewed locally.

7.4. If surveillance camera systems are not capable of producing audit logs, then measures will be put in place to ensure audit logs are taken via alternative methods (such as maintaining a simple Excel spreadsheet) as to when relevant actions (including downloading, copying, removing, deleting, altering, etc.) are performed.

8. Individual Rights

8.1. All surveillance camera systems that [SCHOOL NAME] operate will not in any way affect the rights afforded to a data subject under data protection legislation, particularly the right to be informed and the right of access.

8.2. "Right to be Informed":

8.2.1. [SCHOOL NAME] will ensure that privacy notices will be in place. For example, CCTV notices will be displayed in prominent locations that will obviously indicate to any individual that CCTV is in operation. The use of CCTV systems and other recording systems will be supported by [SCHOOL NAME]'s privacy notice which is accessible here [INSERT PRIVACY NOTICE LINK].

8.3. "Right of Access":

8.3.1. Members of staff acquiring any surveillance camera systems will ensure that the software, or by the very least, their processes, is/are capable of extracting and redacting images appropriately to allow [SCHOOL NAME] to respond to a Subject Access Request (SAR).

8.3.2. SARs for personal data captured through surveillance camera systems will require the data subject to detail the date and time images were recorded, and the location of the camera.

9. Complaints & Contacts:

9.1. General complaints and enquiries about the operation of [SCHOOL NAME]'s surveillance camera systems must be addressed to [INSERT CONTACT]

9.2. Data protection complaints surrounding [SCHOOL NAME]'s surveillance camera systems must also be addressed to [INSERT CONTACT].

10. Policy Review:

10.1. The surveillance camera systems policy will be reviewed every 5 years, unless required to review due to changes in legislation or regulatory guidance.

11. Definitions

11.1. Data Protection Legislation: UK General Data Protection Regulations ('UK GDPR')/Data Protection Act 2018 ('DPA 2018') – In effect, these are regulations that lay down rules relating to the protection of natural persons with regard to the processing of their personal data, and provide individuals with rights associated with the use of their personal data, for example, a Subject Access Request ('SAR'), which allows an individual to request copies of their personal data held by a controller.

11.2. Information Request Legislation: Freedom of Information Act 2000 ('FOIA')/Environmental Information Regulations 2004 ('EIR') – In effect, these regulations provide individuals with the right to request non-personal information from public authorities, including Local Authorities & Schools.

11.3. Personal Data – Any information relating to an identified or identifiable natural person ('data subject'); [directly or indirectly identified], in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

11.4. Controller – The body which, alone or jointly with other bodies, determines the purposes and means of the processing of personal data.

11.5. Processor – The body which processes personal data on behalf of the controller.

11.6. Processing – Covers a wide range of operations performed on personal data, including by manual or automated means. It includes the collection, recording, organisation, structuring, storage, alteration, retrieval, consultation, use, disclosure, erasure or destruction of personal data.

11.7. Data Protection Officer (DPO) – An individual appointed by the controller to assist a controller monitor internal compliance, inform and advise of a controller's data protection obligations, provide independent advice regarding Data Protection Impact Assessments and act as a contact point for data subjects and the Information Commissioner's Office.