Data Protection Impact Assessment (CCTV)

Cotwall End Primary School operates a CCTV system. As such **Cotwall End Primary School** must consider the privacy implications of such a system. There are a number of other issues **Cotwall End Primary School** will also need to consider. The completion of the Data Protection Impact Assessment highlights some of the key implications.

A Data Protection Impact Assessment is also recommended by the Surveillance Camera Code of Practice which sets out the guiding principles that should be applied when CCTV systems are in place to ensure that privacy risks are minimized whilst ensuring the aims of the CCTV system are met.

The Data Protection Impact Assessment looks at the wider context of privacy taking into account Data Protection Law and the Human Rights Act. It considers the need for the CCTV system and the impact it may have on individual privacy.

The Data Protection Impact Assessment helps determine whether the proposed system can be justified as proportionate to the needs of the school. In undertaking this Data Protection Impact Assessment **Cotwall End Primary School** has considered its obligations under Data Protection Law.

Cotwall End Primary School recognizes that changes do occur and on this basis good practice recommends that the school review its Data Protection Impact Assessment. The school recognizes that it is good practice to undertake a Data Protection Impact Assessment before a system is put in place and follows the surveillance commissioner's passport to compliance.

The school also has a CCTV Policy.

A Data Protection Impact Assessment will typically consist of the following key steps:

1. Identify the need for a DPIA.
2. Describe the information flow.
3. Identify data protection and related risks.
4. Identify data protection solutions to reduce and eliminate the risks.
5. Sign off the outcomes of the DPIA.

Explain broadly what project aims to achieve and what type of processing it involves. You may find it helpful to refer or link to other documents, such as a project proposal. Summarise why you identified the need for a DPIA.

What is the aim of the project? – CCTV consistently delivers benefits in terms of improved health and safety and security within schools. It complements other security measures which are in place within the school.

CCTV aims to achieve the following:

- Improve the health and safety and security of pupils, staff, and visitors
- Protect the school buildings and internal infrastructure
- Improve pupil behavior
- Reduce vandalism
- Provide assistance in the detection and prevention of crime

Parents have the assurance that their children are safe whilst in school. Parents are aware that with CCTV there is the potential for behavior at school to improve. The Board of Governors are also of the opinion that this is the case

Step 2: Describe the processing

Describe the nature of the processing: how will you collect, use, store and delete data? What is the source of the data? Will you be sharing data with anyone? You might find it useful to refer to a flow diagram or other way of describing data flows. What types of processing identified as likely high risk are involved?

How will you collect, use, store and delete data? – The CCTV system will provide the school with both still and video pictures from 11 fixed based cameras located throughout the school and the images will be captured on a digital video recorder. The CCTV system is operational 24 hours a day, 7 days a week.

The images are transmitted to a video Digital Video Recorder which are housed within a secure communication room. Access to the communication room is restricted. The images are stored on the hard drive of the Digital Video Recorder.

The transmitted images can also be viewed live in the School's Office. School Admin Staff, Caretaker and Senior Leadership Team have access to the CCTV images. This helps to maintain site security, access control, pupil and staff safety.

What is the source of the data? – The CCTV system provides school video pictures, which are transmitted from cameras positioned in various locations throughout the school. All of the CCTV cameras are fixed on a particular scene. The location of the CCTV cameras are as follows:

1. Outside Y3/4 classroom, viewing the school side gate off the drive
2. Outside Headteacher's Office, viewing the playground for Y3/4
3. Outside Y5 classrooms, viewing walkway between Y5 and Y6 and field
4. Outside Y6 classrooms, viewing access to Y6 classrooms
5. Outside Main Entrance, viewing main entrance, and top of car park
6. Outside Main Gate, viewing pedestrian and vehicle access to drive
7. Outside KS1 boiler house, viewing Area of car park around caretaker's house, and access to rear of school
8. Outside KS1 stairway, viewing school drive and KS1 stairway
9. Outside KS1 entrance, viewing doorway and path to KS1
10. Outside Y2, viewing playground and field access from driveway.
11. Outside Reception playground, viewing gateway access to reception outdoor area.

Will you be sharing data with anyone? – The information is used to ensure the health and safety and security of pupils, staff and visitors. They can be used to detect unauthorized visitors, and are used for protection of damage to school assets. The information may be shared with Senior Leadership Team and the Police for investigation and enforcement purposes should a criminal act be suspected.

Disclosure of data is covered by the school's internal processes which are fully compliant with relevant legislation and Codes of Practice.

What types of processing identified as likely high risk are involved? – Recording of images. Storage of images securely. Appropriate data retention applied to the images.

Data Management controls include passwords to the CCTV system.

Individuals can request copies of CCTV data which contains their personal information by submitting a subject access request.

Describe the scope of the processing: what is the nature of the data, and does it include special category or criminal offence data? How much data will you be collecting and using? How often? How long will you keep it? How many individuals are affected? What geographical area does it cover?

What is the nature of the data? – The CCTV data captured is both still images and video recordings.

Special Category data? – By default the CCTV may be picking up special category data including race/ethnic origin and the health of an individual

How much data is collected and used and how often? – The CCTV is operational 24 hours per day, 7 days per week.

How long will you keep the data for? – Images will be retained for 31 days (28 to 30 days best practice) unless requested as part of an incident and then stored on archive for 12 months. The Data Management System automatically deletes the information after 31 days. Please see the school's Data Retention Policy.

Scope of data obtained? – The CCTV images are obtained within the confines of the school's grounds and not outside.

Describe the context of the processing: what is the nature of your relationship with the individuals? How much control will they have? Would they expect you to use their data in this way? Do they include children or other vulnerable groups? Are there prior concerns over this type of processing or security flaws? Is it novel in any way? What is the current state of technology in this area? Are there any current issues of public concern that you should factor in? Are you signed up to any approved code of conduct or certification scheme (once any have been approved)?

What is the nature of your relationship with the individuals? – The school provides education to its students on a term time basis with staff delivering the National Curriculum. The school may receive a number of visitors on a daily basis including contractors, inspectors, support and agency staff, etc.

How much control will they have? – The school does inform pupils, staff and visitors that CCTV is in use by installing signs detailing the scheme and its purpose, along with a contact telephone number.

The CCTV system is capable of identifying individuals from the system and the images can be used in both criminal and civil court cases.

If a Subject Access Request is made data may be downloaded or copied for release to the data subject or a third party (in the case of a Data Protection request).

Each request for data must be requested via a signed data release form. In the case of the Police this can be authorized by a person at the rank of Sergeant or above using a WA170 form.

Do they include children or other vulnerable groups? – Cameras are located in areas where pupils and staff have access. Cameras are not located in any areas where privacy is expected. There are no cameras in interior areas of the school, toilet areas, and there are no cameras aimed at private areas such as residents' houses, etc.

Are there prior concerns over this type of processing or security flaws? – The school has a CCTV Policy. The system is operated in line with relevant legislation and the Surveillance Camera Code of Practice. Staff operating/using the system have undertaken Data Protection and Information Security training.

Describe the purposes of the processing: what do you want to achieve? What is the intended effect on individuals? What are the benefits of the processing – for you, and more broadly?
The CCTV system is proportionate and justified. It is also achieves for the school the following benefits: 1. demonstrates a duty of care to its pupils, staff, and visitors   2. protects the fabric of the school both externally and internally   3. as a consequence of this, budgets can be reduced/deferred to other school projects   4. provides assistance in the detection and prevention of crime   5. to assist in managing the school   The CCTV system is referenced in the school's Privacy Notice (Pupil)(Workforce)

Step 3: Consultation process

Consider how to consult with relevant stakeholders: describe when and how you will seek individuals' views – or justify why it's not appropriate to do so. Who else do you need to involve within your organisation? Do you need to ask your processors to assist? Do you plan to consult information security experts, or any other experts?
The views of students, staff and the Board of Governors will be obtained. Once reviewed the views of stakeholders (including parents) will be taken into account   The view of YourIG has also been engaged to ensure CCTV compliance.

Step 4: Assess necessity and proportionality

Describe compliance and proportionality measures, in particular: what is your lawful basis for processing? Does the processing actually achieve your purpose? Is there another way to achieve the same outcome? How will you prevent function creep? How will you ensure data quality and data minimisation? What information will you give individuals? How will you help to support their rights? What measures do you take to ensure processors comply? How do you safeguard any international transfers?

What is the lawful basis for processing? – The lawful basis for processing is contained in the school's Privacy Notice (Pupil). It includes the following:

- Article 6 and Article 9 (Special Category Data) under Data Protection Law
- The Common Law Duty of Care
- Health and Safety at Work Act
- Safeguarding Vulnerable Groups Act
- Working together to Safeguard Children Guidelines (DfE)
- Keeping Children Safe in Education (DfE)
- DfE Risk Protection Arrangement Risk Assessment guidance

Does the processing achieve your purpose? – Cameras are located in external areas where pupils and staff have access. Cameras are not located in any internal areas of the school, or areas where privacy is expected.

Is there another way to achieve the same outcome? – To support school security a locked in school policy has been adopted along with improved lighting and other improvements have been put in place.

How will you prevent function creep? – The lawful basis for processing is contained in the school's Privacy Notice (Pupil). Where there have been material changes to the way CCTV is used, the school will undertake a review of its CCTV system to ensure compliance and mitigate against 'function creep.'

How will you ensure data quality and data minimisation? – Consider the source of the data. The school will continue to be compliant with its CCTV Policy.

What information will you give the individuals? – The school does inform pupils, staff and visitors that CCTV is in use by installing signs detailing the scheme and its purpose, along with a contact telephone number.

How will you help them support their rights? – The school has a Subject Access Request

procedure in place to ensure compliance with Data Protection Law. CCTV signage states a contact telephone number. The school will continue to be compliant with its Data Protection Policy.

Describe source of risk and nature of potential impact on individuals. Include associated compliance and corporate risks as necessary.	Likelihood of harm	Severity of harm	Overall risk
	Remote, possible or probable	Minimal, significant or severe	Low, medium or high
Positioning of CCTV cameras at entrance points to the school and the issue of privacy	Remote	Minimal	Low
Housing of CCTV cameras outside and ingress of water	Possible	Significant	Medium
Ongoing maintenance of CCTV equipment preventing breakdowns, etc	Possible	Significant	Medium
CCTV policies and procedures not in place leading to inconsistencies, etc	Probable	Significant	Medium

Step 6: Identify measures to reduce risk

Identify additional measures you could take to reduce or eliminate risks identified as medium or high risk in step 5

Risk	Options to reduce or eliminate risk	Effect on risk	Residual risk	Measure approved
		Eliminated reduced accepted	Low medium high	Yes/no
CCTV & ingress of water	Use of waterproof enclosures	Reduced	Low	Yes
CCTV Maintenance	Hiring of a maintenance company	Reduced	Low	Yes
CCTV Policies & Procedures	Policies and Procedures in situ	Reduced	Medium	Yes

Step 7: Sign off and record outcomes

Item	Name/date	Notes
Measures approved by:	**Kieron Underhill**	Integrate actions back into project plan, with date and responsibility for completion
Residual risks approved by:	Claire Williams	If accepting any residual high risk, consult the ICO before going ahead
DPO advice provided:	Yes	DPO should advise on compliance, step 6 measures and whether processing can proceed

Summary of DPO advice:

CCTV Policy

Amend Privacy Notice

CCTV Checklist / Passport to compliance

DPO advice accepted or overruled by:	Kieron Underhill, accepted	If overruled, you must explain your reasons

Comments:

All complete 17th April 2025

Consultation responses reviewed by:	Kieron Underhill	If your decision departs from individuals' views, you must explain your reasons

Comments:

To be reviewed

This DPIA will kept under review by:	Kieron Underhill / DPO	The DPO should also review ongoing compliance with DPIA