Data Protection Impact Assessment (CCTV)

The **Hales Valley Trust (Hurst Hill Primary School)** operates a CCTV system. As such **Hales Valley Trust** I must consider the privacy implications of such a system. There are a number of other issues **Hales Valley Trust** 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 **Hales Valley Trust** has considered its obligations under Data Protection Law.

Hales Valley Trust 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.

Step 1: Identify the need for a 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. **Hales Valley Trust** has updated its Privacy Notice for its CCTV system. The Privacy Notice highlights what personal information is used and the lawful basis for using this personal information. It also highlights who the school will share the personal information with and how long the information will be kept. The Privacy Notice (Pupil) and Privacy Notice (Workforce) documents what rights an individual has regarding their personal information. Reference should is made to the CCTV system in the school's Information Asset Register.

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 pictures from 4 fixed based cameras located throughout the school and the images will be transmitted/captured on a digital video recorder (DVR). The CCTV system is operational 24 hours a day, 7 days a week.

The images are transmitted to a digital video recorder which is housed in a locked office of the school. Access is restricted via a locked door. Access to the school is via a secure door entry system. The school reception is manned throughout the school day. The images are stored on the hard drive of the digital video recorder. The DVR is located within a locked room.

The transmitted images can be viewed in the event of an incident. The images can be viewed form the front office computer.by the Headteacher, Senior Leadership Team and site manager. This is documented in the school's CCTV Policy. This helps to maintain site security, access control, pupil and staff safety. Images are deleted automatically after 30 days. Data is only viewed in the event of an incident.

What is the source of the data? – The CCTV system provides still/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:

- 2 cameras are located in the school playground
- 2 additional cameras are located around the perimeter of the building

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, pupils with poor behavior/internal truancy, and protection of

damage to school assets. The information may be shared with Senior Leadership Team and the Police for investigation and enforcement purposes.

Disclosure of data is covered by the school's internal processes which are fully compliant with relevant legislation and Codes of Practice (please see the school's CCTV Policy).

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.

The digital video recorder is located in the Server Room within a locked cabinet. Access to the images is password protected.

Data Management controls include passwords to the CCTV system. (see comment above)

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 are still 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 a day 7 days a week.

How long will you keep the data for? – Images will be retained for 30 days unless requested as part of an incident and then stored on archive for the period of the investigation process or for 12 months whichever is the lesser. The Data Management System automatically deletes the information after 30 days. This needs to be included in **Hales Valley Trust** Data Retention Policy. YourIG would recommend data retention meets industry standards (28 to 31 days)

Scope of data obtained? – The CCTV images are obtained within the confines of the school.

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 their presence. One is located to the front of the school and two to the rear of the school. Recommendation that these signs contain details of who the data controller is (i.e. Hurst Hill Primary School) and the school's contact telephone number. The CCTV signage needs to be located on entry to the school site (car park and pedestrian access). It also needs to be located to the rear of the site. 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 areas where privacy is expected. There are no cameras in toilet areas, changing rooms, and there are no cameras aimed at private areas such as residents' houses, etc. CCTV signage should be clearly visible from the street. **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 (consideration respecting data retention). Recommendation by YourIG that staff operating/using the system must 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 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. encourages improvement pupil behavior 5. provides assistance in the detection and prevention of crime 6. to assist in managing the school CCTV system is be 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 CCTV system was installed in 09/09/2013. The system has 4 cameras. If the School is looking to upgrade its system with additional cameras. The school will need to consider the CCTV Passport to Compliance guidance prior to implementation. The decision to install and expand the CCTV system would be agreed by **Hurst Hill** Board of Governors. This will be communicated to parents and pupils via the school's CCTV Privacy Notice. This will be published on the school website. 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). The lawful basis 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)

Does the processing achieve your purpose? – Cameras are located in areas where pupils and staff have access. Cameras are not located in 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 will be contained in the school's Privacy Notice (CCTV). 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 consider developing a separate data retention policy which identifies data retention periods for CCTV. However, the school will note data retention periods against CCTV as documented in the Information Asset Register. The school will continue to be compliant with its CCTV Policy.
What information will you give the individuals? – The school will 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 school does have a Privacy Notice for its CCTV.
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.

Step 5: Identify and assess risks

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**
Appropriate CCTV signage in place which conforms to industry standards	Possible	Minimal	**Low**
Training not undertaken by those using CCTV Privacy Notice (Pupils); (Workforce)	Possible	Significant	**Medium**
Noncompliance when upgrading the school's CCTV system	Possible	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	Maintenance contract in place with Security Services	**Reduced**	Low	Yes
CCTV Policies & Procedures	Policies and Procedures insitu	**Reduced**	Medium	Yes
Training	Undertaken in GDPR and Information Security	**Reduced**	Low	Yes
Privacy Notices	Update the Privacy Notices to include reference to CCTV	**Reduced**	Low	Yes
CCTV Passport to Compliance	Upgrade CCTV using guidance from CCTV Passport to Compliance	**Reduced**	Low	Yes

Step 7: Sign off and record outcomes

Item	Name/date	Notes
Measures approved by:	**Chief Operations Officer**	Integrate actions back into project plan, with date and responsibility for completion
Residual risks approved by:	**Chief Operations Officer**	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: Recommend that signage is put in place which meets industry standards (name of Dawley Brook Primary School; contact telephone number) Include in **Hales Valley Trust**Information Asset Register Working towards CCTV Passport to Compliance when updating CCTV		
DPO advice accepted or overruled by:	Yes	If overruled, you must explain your reasons
Comments:		
Consultation responses reviewed by:	**Chief Operations Officer**	If your decision departs from individuals' views, you must explain your reasons
Comments: **[Comments provided]**		
This DPIA will kept under review by:	**Your IG**	The DPO should also review ongoing compliance with DPIA