



# Wyton on the Hill Primary School

## CCTV Policy

### **Data Protection**

- Any personal data processed in the delivery of this policy will be processed in accordance with the school Data Protection policy.

### **1. Policy Statement**

1.1 Wyton on the Hill Primary School uses Close Circuit Television (“CCTV”) within the premises of the School. The purpose of this policy is to set out the position of the School as to the management, operation and use of the CCTV at the School.

1.2 This policy applies to all members of our Workforce, visitors to the School premises and all other persons whose images may be captured by the CCTV system.

1.3 This policy takes account of all applicable legislation and guidance, including:

- General Data Protection Regulation (“GDPR”);
- CCTV Code of Practice produced by the Information Commissioner;
- Human Rights Act 1998.

1.4 This policy sets out the position of the School in relation to its use of CCTV and should be read in conjunction with the School Data Protection Policy.

1.5 The system comprises of six external cameras and does not use any sound recording capability. The CCTV system is owned and operated by the School. The Data Protection Officer (“DPO”) or their representative has overall responsibility as delegated by the Data Controller (Board of Governors).

1.6 Access and viewing is restricted and all authorised operators with access to images will be aware of the procedures they are required to follow and their responsibilities under this policy. All employees will be aware of the restrictions in relation to access to, and disclosure of, recorded images. The further introduction of, or changes to, CCTV monitoring will be subject to consultation with staff where appropriate

### **2. Purpose of CCTV**

2.1 The School uses CCTV for the following purposes:

- To provide a safe and secure environment for pupils, staff and visitors;
- To protect the school buildings and assets;
- To assist in reducing the fear of crime and for the protection of private property;
- To assist in the prevention of crime and assist law enforcement agencies in apprehending offenders.

### **3. Policy Intent**

3.1 The school will:

- notify the Information Commissioners Office of its use of CCTV as part of the annual data

- protection registration;
- complete a CCTV Privacy Impact Assessment (“PIA”) (Appendix A) for the use of surveillance CCTV and will update this as appropriate when the system is upgraded or significantly modified;
  - treat the system and all information processed on the CCTV system as data which is covered by the Data Protection Act/GDPR;
  - use cameras to monitor activities within the school grounds to identify potential criminal activity for the purpose of securing the safety and well-being of the school;
  - not direct cameras outside of the school site at private property, an individual, their property or a specific group of individuals. The exception to this would be where an authorisation was obtained for Directed Surveillance to take place, as set out in the Regulation of Investigatory Power Act 2000;
  - display CCTV warning signs will be clearly and prominently placed in the school grounds;
  - not guarantee that a system will or can cover or detect every single incident taking place in the areas of coverage;
  - not use materials or knowledge for any commercial purpose. Recorded materials will only be released for use in the investigation of a specific crime and with the written authority of the Police and in accordance with the Data Protection Act/GDPR.

#### **4. Siting Cameras**

Cameras will be sited so they only capture images relevant to the purposes for which they are installed (described above) and care will be taken to ensure that reasonable privacy expectations are not violated. The school will ensure that the location of equipment is carefully considered to ensure that images captured comply with the Data Protection Act/GDPR requirements

4.1 Covert Monitoring will cease following completion of an investigation.

4.2 Cameras sited for the purpose of covert monitoring will not be used in areas which are reasonably expected to be private, for example toilets.

#### **5. Storage and Retention of CCTV images**

5.1 Recorded data will not be retained for longer than is necessary. While retained, the integrity of the recordings will be maintained to ensure their evidential value and to protect the rights of the people whose images have been recorded.

5.2 All retained data will be stored securely.

5.3 Recordings are kept for up to 28 days. Specific recordings which the school wishes to retain after this time will be logged (see Appendix B).

5.4 An electronic file is held on a secure server where specific CCTV image/recordings are retained. Access by staff to specific recordings are outlined below in section 6.

5.5 The Data Protection Act/GDPR does not prescribe any specific minimum or maximum retention periods that apply to all systems or footage. Rather, retention should reflect the organisation’s purposes for recording information, which should be informed by the purpose for which the information is collected, and how long it is needed to achieve this purpose. Storage availability is also a factor to be considered in the ability to retain recordings.

#### **6. Disclosure of Images to Data Subjects (Subject Access Requests)**

6.1 Any Individual recorded in any CCTV image is a data subject for the purposes of the Data Protection Legislation, and has the right to request access to those images.

6.2 Any individual who requests access to images of themselves will be considered to have made a subject access request pursuant to the Data Protection Legislation. Such a request should be

considered in the context of the School's Subject Access Request Policy.

6.3 All requests should be made in writing to the Head Teacher or Data Protection Officer or their representative. Individuals submitting requests for access will be asked to provide sufficient information to enable the footage relating to them to be identified. For example, date, time and location.

6.4 When such a request is made a member of the CCTV system administrator will review the CCTV footage, in accordance with the request.

6.4.1 If the footage contains only the individual making the request then the individual may be permitted to view the footage. This must be strictly limited to that footage which contains only images of the individual making the request. The CCTV system administrators must take appropriate measures to ensure that the footage is restricted in this way.

6.4.2 If the footage contains images of other individuals then the School must consider whether:

6.4.2.1 The request requires the disclosure of the images of individuals other than the requester, for example whether the images can be distorted so as not to identify other individuals;

6.4.2.2 The other individuals in the footage have consented to the disclosure of the images, or their consent could be obtained; or

6.4.2.3 If not, then whether it is otherwise reasonable in the circumstances to disclose those images to the individual making the request.

6.5 The school reserves the right to refuse access to CCTV footage where this would prejudice the legal rights of other individuals or jeopardise an ongoing investigation.

6.6 A record must be kept (see Appendix), and held securely, of all disclosures which sets out:

6.6.1 When the request was made;

6.6.2 The process followed by the CCTV system administrators in determining whether the images contained third parties;

6.6.3 The considerations as to whether to allow access to those images;

6.6.4 The individuals that were permitted to view the images and when; and

6.6.5 Whether a copy of the images was provided, and if so to whom, when and in what format.

## **7. Disclosure of Images to Third Parties**

7.1 The School will only disclose recorded CCTV images to third parties where it is permitted to do so in accordance with the Data Protection Legislation.

7.2 Third parties acting behalf of a duty subject will be handled in accordance with the School's Subject Access Request Policy.

7.3 CCTV images will only be disclosed to law enforcement agencies in line with the purposes for which the CCTV system is in place.

8.3 If a request is received from a law enforcement agency for disclosure of CCTV images then the School must follow the same process as above in relation to subject access requests. Detail should be obtained from the law enforcement agency as to exactly what they want the CCTV images for, and any particular individuals of concern. This will then enable proper consideration to be given to what should be disclosed, and the potential disclosure of any third party images.

8.4 The information above must be recorded in relation to any disclosure (see Appendix).

8.5 If an order is granted by a Court for disclosure of CCTV images then this should be complied with. However very careful consideration must be given to exactly what the Court order requires. If there are any concerns as to disclosure then the Data Protection Officer should be contacted in the first instance and appropriate legal advice may be required.

## **8. Access to CCTV Images**

8.1 The ability to view live and historical CCTV is only possible through the computer dedicated to the task in the School office.

8.2 Data from CCTV may be used within the school's' discipline and grievance procedures as required, and will be subject to the usual confidentiality requirements of those procedures.

## **9. Complaints**

- Complaints and enquiries about the operation of CCTV within the school should be directed to the Head Teacher or Data Protection Officer in the first instance.

## **10. Further Information**

For further information on CCTV and its use please see below:

- Data Protection Act 1998
- General Data Protection Regulation (GDPR)
- CCTV Code of Practice (ICO website <https://ico.org.uk/for-organisations/guide-to-data-protection/key-dp-themes/guidance-on-video-surveillance-including-cctv/>)

## Privacy Impact Assessment

This document will assist in recording the PIA process and results. The document should be completed prior to any project commencing and should be updated throughout the course of a projects life.

### **Step 1: Identify the need for a Privacy Impact Assessment**

*Explain what the project aims to achieve, what the benefits will be to the organisation, to individuals and to other parties. Summarise why the need for a Privacy Impact Assessment was identified (draw on answers from the screening questions).*

The project aims to enhance safeguarding and security of Wyton on the Hill Primary School The project with use a network of CCTV cameras and a recording device on which video images are stored. All cameras will be located in spaces at the school to which staff, students can all access but will also capture some adjoining public footpaths and roads.

Due to potential concerns about the collection of images this PIA is being completed.

### **Step 2: Describe the information flows**

*The collection, use and deletion of personal data should be described. You may want to refer to a flow diagram to explain the data flow. You should say how many individuals are likely to be affected by the project.*

1. The cameras will be installed and activated when the school is built in February 2019.
2. They will constantly (24hours) record.
3. The cameras will cover a large portion of the external part of the school.
4. The cameras will all be visible.
5. The cameras will provide an image of sufficient quality to mean that individuals and their actions will be clearly identifiable.
6. The cameras will be recorded, but not constantly monitored 'live'.
7. Signs will be clearly displayed close to the cameras highlighting their presence and purpose.
8. All recordings will become the property of Wyton on the Hill Primary School and will be kept for 28 days or longer if the school sees fit.
9. The recordings may be provided to outside agencies such as social workers or the police if the content is relevant to an investigation. This provision is to occur solely under the strict instruction of the Designated Safeguarding Lead for the school.

### Step 3: Consultation requirements

*Explain what practical steps you will take to ensure that you identify and address privacy risks. Who should be consulted, internally and externally? How will you carry out the consultation?*

1. This Privacy Impact Assessment (PIA) will be available to everyone via our website.
2. All current staff, students and parents will be informed about the project, the reasons for it and its implications
3. A thorough network of signage will be clearly displayed to ensure that anyone who may subject to recording is fully aware.

### Step 4: Identify privacy solutions

*Describe the actions you could take to reduce the risks, and any future steps which would be necessary, e.g. the production of new guidance or future security testing for systems.*

<b>Risk</b> (as identified above)	<b>Solution(s)</b> eg. training, policy update, agreement/contract NB: There may be more than one possible solution for each risk	<b>Result</b> Is the risk eliminated, reduced or accepted?
Intrusion of privacy	Installation of signage Proper communication of purpose	Risk is reduced
Loss of data	Storage resilience The footage will be kept for a maximum amount of time of 28 days on the school system. Access to these files will only be allowed to specified members of staff. The system will be a closed network without external access.	Risk is reduced

**Step 5: Sign off and record the PIA outcomes**

*Who has approved the privacy risks involved in the project? Which of the solutions identified above need to be implemented?*

<b>Risk (as identified above)</b>	<b>Approved solution</b>	<b>Approved by</b>
Intrusion of privacy	Communication to all parents, staff and students.	Head teacher
Loss of data	Hardware and software purchased from CCTV specialists based on advice from the County Council	School Business Manager

**Step 6: Integrate the PIA outcomes back into the project plan**

*Who is responsible for integrating the PIA outcomes back into the project plan and updating any project management paperwork? Who is responsible for implementing the solutions that have been approved? Who is the contact for any privacy concerns which may arise in the future?*

<b>Action to be taken</b>	<b>Date for completion of actions</b>	<b>Responsibility for action</b>
Future privacy concerns / project developments	As required	School Business Manager

**Appendix B – External Requests  
Subject Access & Third Party Request Disclosure Log**

**NB: Please follow the Subject Access Request Policy procedures before disclosing any data**

Date request received and from whom (name & organisation)	Date referred to DPO	Subject Access Request or Third Party Request	State the reason (if third party)	Date & nature of disclosure (viewing or copy of image)	Images viewed/sent (state location, date, time of original image/s and internal image reference)	The outcome if applicable