

Windale Primary School

CCTV Policy

Document Control	
Document Title	CCTV Policy
Summary of changes	No changes.
Date of original issue	14/07/2021
Name of Originator	Tina Arundell
Name of responsible Group	Windale H&S Committee
Next Review Date	May 2026

Declaration of Adoption

This document has been reviewed by the H&S committee and has been formally adopted

Contents

1. Introduction
2. CCTV system overview
3. Purposes of the CCTV system
4. Monitoring and recording
5. Compliance with Data Protection legislation
6. Applications for disclosure of images
7. Retention of images
8. Complaints Procedure
9. Monitoring compliance
10. Policy Review
11. Appendix 1 – DPIA
12. Appendix 2 – Map with camera location & view direction

1. Introduction

- 1.1 Windale Primary School has in place a CCTV surveillance system “the CCTV system” across its premises. This policy details the purpose, use and management of the CCTV system in the School and details the procedures to be followed in order to ensure that the School complies with relevant legislation and the current Information Commissioner’s Office Code of Practice.
- 1.2 The School will conform to the requirements of the Data Protection Act 2018, the General Data Protection Regulation (GDPR) and any subsequent data protection legislation, and to the Freedom of Information Act 2000, the Protection of Freedoms Act 2012 and the Human Rights Act 1998. Although not a relevant authority, the School will also have due regard to the Surveillance Camera Code of Practice, issued under the Protection of Freedoms Act 2012 and in particular the 12 guiding principles contained therein.
- 1.3 This policy is based upon guidance issued by the Information Commissioner’s Office, ‘In the picture: A data protection code of practice for surveillance cameras and personal information’ (“the Information Commissioner’s Guidance”).

<https://ico.org.uk/media/for-organisations/documents/1542/cctv-code-of-practice.pdf>

2. CCTV System overview

- 2.1 The CCTV system is owned by Windale Primary School, Windale Avenue, Oxford, OX4 6JD and managed by the School and its appointed agents. The data controller for CCTV images held by Windale Primary School is United Learning Trust (ULT). ULT is registered with the Information Commissioner’s Office (ICO). The registration number is Z7415170.

The Group’s Data Protection Officer is responsible for ensuring that ULT complies with the Data Protection Law. The Data Protection Officer can be contacted on company.secretary@unitedlearning.org.uk or 01832 864538.

The CCTV system operates to meet the requirements of the Data Protection Act 2018 and the Information Commissioner’s Guidance.

- 2.2 Windale Primary School’s designated Data Protection Lead and School Manager is responsible for the overall management and operation of the CCTV system, including activities relating to installations, recording, reviewing, monitoring and ensuring compliance with this policy.
- 2.3 The CCTV system operates across the School. Details of the number of cameras can be given on request.
- 2.4 Clearly visible signs are placed at all pedestrian and vehicular entrances to inform staff, pupils, parents, visitors and members of the public that CCTV is in operation.

The signage indicates that the system is managed by the School and a 24-hour contact number for the Security Control Centre is provided, if appropriate.

- 2.5 The Data Protection Lead is responsible for ensuring that adequate signage is erected in compliance with the ICO CCTV Code of Practice.
- 2.6 Cameras are sited to ensure that they cover School premises as far as is possible. Cameras are installed throughout the School's sites including roadways, car parks and externally in vulnerable public facing areas.
- 2.7 Cameras are not sited to focus on private residential areas. Where cameras overlook residential areas, privacy screening or software masking will be utilised.
- 2.8 The CCTV system is operational and capable of being monitored for 24 hours a day, every day of the year.
- 2.9 Any CCTV installation shall be subject to a Data Protection Impact Assessment. It will also comply with the policy and procedures within this document. The Data Protection Impact Assessment shall be appended to this policy and shared with Central Office Data Protection Officer

3. Purposes of the CCTV system

- 3.1 The Headteacher purposes of the School's CCTV system are as follows:
 - for the prevention, reduction, detection and investigation of crime and other incidents;
- 3.2 The CCTV system will be used to observe the school's buildings and areas under surveillance to identify incidents requiring a response. Any response should be proportionate to the incident being witnessed.
- 3.3 The school seeks to operate its CCTV system in a manner that is consistent with respect for the individual's privacy as outlined in the Privacy Impact Assessment.

4. Monitoring and Recording

- 4.1 Cameras are monitored in the main school office on a standalone hard drive unit.
- 4.2 Images are recorded securely on a standalone hard drive unit in the school main office and are viewable by all authorised CCTV staff.

Authorised Staff are as follows:

Headteacher
Deputy Headteacher
Assistant Headteacher
School Manager
Senior Admin Assistant & Data Protection Lead

- 4.3 A log shall be kept of requests to access recorded images by staff and whether any recorded images have been copied to support specific investigations. Information logged should include name of staff, time and date of viewing, time and date of

images reviewed, brief reason for viewing content (e.g. “incident in corridor”) but should not contain names, whether any images have been copied and where they have been copied to.

- 4.4 The cameras installed shall provide images that are of suitable quality for the specified purposes for which they are installed, and all cameras are checked regularly to ensure that the images remain fit for purpose and that the date and time stamp recorded on the images is accurate.
- 4.5 All images recorded by the CCTV System remain the property and copyright of United Learning. The recorded images are stored securely for 22 days on a standalone hard drive unit in the school main office. Downloaded footage used in investigations is securely stored onsite on an encrypted portable device in accordance with the process outlined in the retention of images section.
- 4.6 The CCTV system should not be used to carry out lesson observations.
- 4.7 The use of cameras in areas where one would normally expect a degree of privacy should be clearly identified on the Privacy Impact Assessment. This would include cameras placed in, or looking into, toilet or changing areas.
Cameras should only be used in toilet or changing areas where there are full height cubicles, never in areas where it is possible to see people using the toileting facilities (excluding hand washing) or changing.
- 4.8 The use of covert cameras will be restricted to rare occasions, when a series of criminal acts have taken place within a particular area that is not otherwise fitted with CCTV. A request for the use of covert cameras will clearly state the purpose and reasons for use and the authority of both the Headteacher and Director of People will be sought before the installation of any covert cameras. The Headteacher should be satisfied and be able to demonstrate that all other physical methods of prevention have been exhausted prior to the use of covert recording.
- 4.9 Covert recording will only take place if informing the individual(s) concerned would seriously prejudice the reason for making the recording and where there are reasonable grounds to suspect that illegal or unauthorised activity is taking place. All such monitoring will be fully documented and will only take place for a limited and reasonable period.

5. Compliance with Data Protection Legislation

- 5.1 From 25 May 2018, the School will also comply with the General Data Protection Regulation. Due regard will be given to the data protection principles contained within Article 5 of the GDPR which provide that personal data shall be:
 - a. processed lawfully, fairly and in a transparent manner;
 - b. collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes;

- c. adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
- d. accurate and, where necessary, kept up to date;
- e. kept in a form which permits identification of the data subjects for no longer than is necessary for the purposes for which the personal data are processed; and
- f. processed in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

5.2 All storage used for images, recorded or downloaded for investigations, must be in compliance with GDPR rules; on secure storage on premise or on cloud storage within the EEA.

5.3 The existence of the School's CCTV system must be recorded in the Record of Data Processing Activities using United Learning's Education Information Portal (EIP).

6. Applications for disclosure of images

Applications by individual data subjects

- 6.1 Requests by individual data subjects for images relating to themselves "Subject Access Request" should be submitted in writing.
- 6.2 In order to locate the images on the School's system, sufficient detail must be provided by the data subject in order to allow the relevant images to be located and the data subject to be identified.
- 6.3 Where the School is unable to comply with a Subject Access Request without disclosing the personal data of another individual who is identified or identifiable from that information, it is not obliged to comply with the request unless satisfied that the individual has provided their express consent to the disclosure, or if it is reasonable, having regard to the circumstances, to comply without the consent of the individual. Any decision to withhold the requested images must be referred to the Group's Data Protection Officer or his team as there are specific rules that must be adhered to when applying the exemptions contained in the Data Protection Act 2018.

Access to and disclosure of images to third parties

- 6.4 A request for images made by a third party should be made in writing.
- 6.5 In limited circumstances it may be appropriate to disclose images to a third party, such as when a disclosure is required by law, in relation to the prevention or

detection of crime or in other circumstances where an exemption applies under relevant legislation.

- 6.6 All unexpected requests for CCTV images by a third party, including requests made by the police, should be referred to the School's Data Protection Lead in the first instance and if not available to the Group's Data Protection Officer or their team, who will advise on the application of any appropriate exemptions. Any third-party request should be added to the EIP in the GDPR area under *third party requests*.
- 6.7 Where a suspicion of misconduct arises and at the formal request of the Investigating Officer or HR Manager/ Business Partner, the Headteacher may provide access to CCTV images for use in staff disciplinary cases.
- 6.8 The Headteacher may provide access to CCTV images to Investigating Officers when sought as evidence in relation to staff discipline cases.
- 6.9 A record of any disclosure made under this policy will be held on the CCTV management system, itemising the date, time, camera, requestor, authoriser and reason for the disclosure.

7. Retention of images

- 7.1 Unless required for evidential purposes, the investigation of an offence or as required by law, CCTV images will be retained for no longer than 22 days from the date of recording. Images will be automatically overwritten after this point.
- 7.2 The automatic deletion of data after the defined retention period should be checked on a half termly basis. This should be logged on a half termly basis.
- 7.3 Where an image is required to be held in excess of the retention period referred to in 7.1, the Headteacher or their nominated deputy will be responsible for authorising such a request. A record of these stored images will be kept within the CCTV viewing log.
- 7.4 Images held in excess of their retention period will be reviewed on a three-monthly basis and any not required for evidential purposes will be deleted. The CCTV monitoring log will provide evidence of the images which have been held and where they are kept. When deleted this should be recorded in the CCTV monitoring log.
- 7.5 Access to retained CCTV images is restricted to the Headteacher and other persons as required and as authorised by the Headteacher.

These individuals are:

Deputy Headteacher
Assistant Headteacher
School Manager
Senior Admin Assistant & Data Protection Lead

8. Complaint's procedure

- 8.1 Complaints concerning the School's use of its CCTV system, or the disclosure of CCTV images should be made in writing to the Headteacher at Windale Primary School, Windale Avenue, Oxford, OX4 6JD. Any complaint will be handled in accordance with the School's complaints policy.
- 8.2 All appeals against the decision of the Headteacher should be made in writing to the Chair of Governors.


9. Monitoring Compliance

- 9.1 All staff involved in the operation of the School's CCTV System will be made aware of this policy and will only be authorised to use the CCTV System in a way that is consistent with the purposes and procedures contained therein.
- 9.2 All staff with responsibility for accessing, recording, disclosing or otherwise processing CCTV images will be required to have undertaken United Learning Data Protection training.


10. Policy review

- 10.1 The School's usage of CCTV and the content of this policy shall be reviewed annually by the Headteacher with reference to the relevant legislation or guidance in effect at the time. Further reviews will take place as required.

Headteacher

Name	Katie Geran-Haq
Signature	
Date	28/5/24

Governor for Health & Safety

Name	Susan Armstrong
Signature	
Date	24/5/2024

11. Appendix 1

Data Protection Impact Assessment for CCTV

If your school has uses CCTV you will need a DPIA in place. The DPIA will need to be reviewed if the system is updated and the update results in changes in its functionality, or if more cameras are added to the system.

1. School	Windale Primary School
2. Name of the person completing the DPIA.	Tina Arundell

3. Is this a new system or an expansion of an existing system?	<input checked="" type="checkbox"/> new system <input type="checkbox"/> expansion of an existing system
--	---

4. Why do you need CCTV? What are the benefits to the organisation and or data subjects?	For the prevention, reduction, detection and investigation of crime and other incidents during out of school hours. The benefits are to ensure the safety of the school site during school closure times.
5. Who are the data subjects?	<input type="checkbox"/> Students <input type="checkbox"/> Parents <input type="checkbox"/> Teachers <input type="checkbox"/> Visitors NA – CCTV only records during out of school hours
6. What are location types where the cameras are in place (tick all that are in place) You will need to list all cameras in appendix 1 .	<input type="checkbox"/> Corridors <input type="checkbox"/> Inside classrooms <input type="checkbox"/> Toilets <input checked="" type="checkbox"/> Playgrounds <input checked="" type="checkbox"/> Car Park <input checked="" type="checkbox"/> Other, please state: External gate entrances, external areas of quod & walkway from quod to main playground
7. Are any of the cameras located in areas where privacy would be expected?	<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No If yes, please consult with the Data Protection Team.
8. What is your lawful basis? Explain the rationale for your chosen lawful basis.	<ul style="list-style-type: none"> • Out of Hours activity on site • To assist the police in their investigation if school reported a crime.
9. Consider whether you will be processing special categories of data. If so, you will need an Article 9 condition for processing.	CCTV only captures within site perimeter. CCTV on site signs are visible and can be found around the school site

Question	Response	Further Action (if required)
10. How will you ensure that the use of the data is limited to the purpose outlined above?	The school's CCTV Policy states clearly what CCTV is used for. Use and access of the installed system is limited to strategic members of school staff.	No
11. What other less intrusive solutions have been considered?	Higher perimeter fencing. Out of hours security service	No

12. Are you consulting with relevant stakeholders? If not, please explain why not. See appendix 2 to record consultation.	The school would only share images to the police to help with their investigations of crimes against the school.	No
13. Confirm that the following are in place:	<input type="checkbox"/> The CCTV is stated within the school's privacy notice <input checked="" type="checkbox"/> The CCTV policy is published on the school's website Clear and adequate signage is in place: <input checked="" type="checkbox"/> when you enter the premises <input type="checkbox"/> where the cameras are located.	No
14. Is the processing covered by the record of data processing activities?	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No	No
15. Provide the information flow, from initial capture to eventual destruction. You may want to attach a diagram at appendix 3 .	CCTV images are retained for no longer than 22 days. The system automatically deletes recordings after 22 days.	No
16. Where is downloaded data stored? What is the process for securing and maintaining retention schedules on downloaded data, <i>If data is being accessed or disclosed you will need to follow the relevant policies:</i> <ul style="list-style-type: none"> • CCTV policy • Disclosure SAR • Disclosure 3rd party 	The school does not download any data from the CCTV recordings,	No
17. How long is data stored? Policy states 30 days (can be extended to 60 over school summer holiday but should be stated here if that option is going to be used). If your retention period differs from policy, even is less, please state reason.	Data is stored on the drive for up to 22 days,	No
18. Tick the retention procedure in place:	<input checked="" type="checkbox"/> Data automatically deleted after retention period <input type="checkbox"/> System operator required to initiate deletion	No
19. How will the school manage SARs for CCTV footage?	The school will inform the person requesting this, that it needs to be in writing on headed paper with specific instructions of what they are requesting and who the request is from. The request is passed to the schools DPL for processing.	No

20. Does the system have the capability to blur 3 rd parties out in the event of a SAR?	<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No	No
21. How will you ensure the security and integrity of the data? Consider the location of the data storage. <u>storage</u> . Is it held in a physical location within the school that protects it from theft? If the is hosted by a 3rd party you will need to complete a cyber security questionnaire.	CCTV unit is in the School Manager's office, which has security fob access only during school opening hours. Out of hours period, office door is locked. Headteacher, School Manager & Senior Admin Assistant are the only people with security fob access & keys to office.	No
22. If monitors are in place which enable the live viewing of the footage, where are the monitors located? <i>They should not be able to be seen inadvertently by unauthorised persons.</i>	As above. Monitor is only turned on in the event of looking back at recordings & when recording timings need to be changed for school break 24-hour coverage.	No
23. Who has access to the system. Do any external 3 rd parties have access to the data?	Headteacher, School Manager & Senior Admin Assistant are the only people with security fob access & keys to office.	No
24. Are the images recorded of adequate quality to fulfil the purpose?	Yes	No
25. Is the system's coverage adequate for the purposes stated?	Yes	No
26. How will you ensure the accuracy of the system? See audit checklist appendix 5 .	School Manager makes a termly check.	No
27. Are cameras positioned to avoid any capture of private land? If repositioning is not possible, please explain what other measures are in place to avoid excessive data processing?	Yes	No
28. Are there any automated or AI driven parts of the system? If yes, please explain what is in place and what the purpose is and liaise with the Central Office data protection team.	No	No
29. Where is the data held?	<input checked="" type="checkbox"/> Onsite <input type="checkbox"/> Externally hosted by 3rd party	No

30. Is the system hosted or maintained by a third party? If so, you will need a processing agreement compliant with Article 28.	No	No
31. Can the system be accessed remotely via cloud/internet-based systems or remote standalone devices?	No	No

Identify the risks

32. Identify and evaluate the risks to the rights and freedoms of individuals relating to your system. Assess both the likelihood and the severity of any impact on individuals.				
Ref.	Describe the risk	Likelihood of harm <i>Remote, possible or probable</i>	Severity of harm <i>Minimal, significant or severe</i>	Overall risk <i>Low, medium or high</i>
1.	Potential for CCTV images to be misused	<i>Remote</i>	<i>Significant</i>	<i>Low</i>
2.	Right of access for CCTV not recognised	<i>Possible</i>	<i>Significant</i>	<i>Medium</i>
3.	Inadequate signage informing persons CCTV cameras are in operation	<i>Possible</i>	<i>Significant</i>	<i>Low</i>

Address the risks

Identify additional measures you could take to reduce or eliminate risks identified as medium or high risk					
Ref	Options to reduce or eliminate risk	Effect on risk <i>Eliminated, reduced, accepted</i>	Residual risk <i>Low, medium, high</i>	Measure approved? <i>Yes, no</i>	Responsible person for action.
1.	Limited access for staff to access the CCTV and trained to use the system	Reduced	Low	Yes	Headteacher
2.	Signs are placed on outside walls of building visible to persons entering the school grounds	Reduced	Low	Yes	School Manager

Note that [appendix 1](#) allows you to record mitigations and safeguards particular to specific camera locations and functionality.

Authorisation

This section should be filled in by the school Data Protection Lead

Risk of harm to data subjects /school / United Learning



NONE



LOW



MEDIUM



HIGH

A **HIGH** risk is one where it is more likely than not that the processing will cause serious harm. In such circumstances, a more robust Impact Assessment should be conducted in consultation with the Group Data Protection Officer's team and possibly involving consultation with data subjects and other stakeholders: processing should not begin until this is completed.

Detail the reasons why you have come to this conclusion.

Cameras records externally and out of school hours only (5.30pm – 7am Mon – Fri (term time), weekends & school breaks 24 hours).

Signed



Name

Zoe Barrett

Position

Senior Admin Assistant & DPL

Date

28/08/2022

Receipt & review by the Group Data Protection Officer's team

Comments

Signed

Name

Date

Agreed review date.

The processing activities documented in this DPIA will be reviewed to ensure that they continue to reflect the information documented above during the month of July 2025.

Camera Locations

Use this table to record the location and scope of your surveillance camera system and the steps you've taken to mitigate risks particular to each location. If cameras cover toilet areas, this would need to be recorded as private.

Ref.	Location of camera	Is this location considered private or intrusive?	Justification for use of camera	Any measures in place to reduce impact of privacy
1.	Front of school	No	To prevent criminal damage & unauthorised access during school closure times	NA
2.	Main playground facing Ox Hub garden	No	To prevent criminal damage & unauthorised access during school closure times	NA
3.	Foundation stage playground	No	To prevent criminal damage & unauthorised access during school closure times	NA
4.	Walkway from Courtyard to main playground	No	To prevent criminal damage & unauthorised access during school closure times	NA
5.	Main playground	No	To prevent criminal damage & unauthorised access during school closure times	NA
6.	Courtyard Zone 4 – Foundation stage	No	To prevent criminal damage & unauthorised access during school closure times	NA
7.	Courtyard corner of Zone 2 & 3	No	To prevent criminal damage & unauthorised access during school closure times	NA
8.	Front playground	No	To prevent criminal damage & unauthorised access during school closure times	NA
9.	Walkway to parent gate 3	No	To prevent criminal damage & unauthorised access during school closure times	NA
10.	Courtyard walkway from cleaning room to SLT corridor	No	To prevent criminal damage & unauthorised access during school closure times	NA

Consultation

Use this table to record any consultations and their outcomes.

Stakeholder consulted	Method	Views raised	Measures taken

Data Flow

Use this section to record the data flow of CCTV data. Consider the process from the when it is recorded, how it is stored, when it is viewed, when it is shared, when and how it is deleted.

Implementation Checklist

Use this checklist when installing a CCTV system, or to review the compliance of the current system.

Action	Status
The quality of the picture adequate to fulfil its purpose – i.e. can you identify individuals from the footage?	<input checked="" type="checkbox"/>
A processing agreement is in place for any third-party hosting.	<input type="checkbox"/> NA – no 3 rd party host
If the system has the capacity to capture audio, this should be switched off.	<input checked="" type="checkbox"/>
If covering a private area, the Data Protection Team have been consulted.	<input type="checkbox"/> NA – external site only
Those with authorised access have been documented in an access matrix	<input checked="" type="checkbox"/>
Responsibility has been assigned for reviewing the system to ensure accuracy is maintained and remains fit for purpose	<input checked="" type="checkbox"/>
There is a documented procedure for the use of the system locally. Including data extraction in the case of a SAR or other request for information. If the system has the capability to mask or blur, ensure those processes are recorded.	<input checked="" type="checkbox"/>
Privacy notices have been updated to reflect the use and published	<input checked="" type="checkbox"/>
Appropriate signage is in place	<input checked="" type="checkbox"/>
Is there a logbook in place to record access to the system?	<input checked="" type="checkbox"/>
CCTV is logged on the Records of Processing Activities	<input checked="" type="checkbox"/>

Audit checklist

Use this to record regular checks on the system.

Date – 04/09/2023	Response
Name of person completing the audit:	Tina Arundell
Is the date and time stamp accurate?	Yes
Is the system fit for purpose?	Yes
Are the cameras pointing to where they should?	Yes

Is any in-camera masking still obscuring appropriate areas?	NA
Is the access matrix up to date?	Yes
Is the logbook being used to record access to the data?	Yes
Where data has been downloaded, has the process for storing and deleting the data been followed appropriately?	NA
Have any new cameras or upgrades been reflected within the DPIA?	NA
Any further observations:	None
Date of next audit:	Sept 2024

Date – 03/09/2024	Response
Name of person completing the audit:	Tina Arundell
Is the date and time stamp accurate?	Yes
Is the system fit for purpose?	Yes
Are the cameras pointing to where they should?	Yes
Is any in-camera masking still obscuring appropriate areas?	NA
Is the access matrix up to date?	Yes
Is the logbook being used to record access to the data?	Yes
Where data has been downloaded, has the process for storing and deleting the data been followed appropriately?	NA
Have any new cameras or upgrades been reflected within the DPIA?	NA
Any further observations:	None
Date of next audit:	Sept 2025

Date	Response
Name of person completing the audit:	
Is the date and time stamp accurate?	
Is the system fit for purpose?	
Are the cameras pointing to where they should?	
Is any in-camera masking still obscuring appropriate areas?	
Is the access matrix up to date?	
Is the logbook being used to record access to the data?	
Where data has been downloaded, has the process for storing and deleting the data been followed appropriately?	
Have any new cameras or upgrades been reflected within the DPIA?	
Any further observations:	
Date of next audit:	

13. Appendix 2

Camera location & view area

