



CCTV Policy

This policy is available to parents and prospective parents on the school's website and by request from the School Office. If you require a copy of this document in large print or audio format, please contact the School Office.

Policy Review Schedule

| | | |
|-------------------------------------------|---------------------------------|-------------------------------------------------------------------------------------|
| Policy Name | DPA CCTV Policy | |
| Review Frequency | Every 3 years | |
| Statutory Policy | No | |
| Policy Owner | Office and Finance Manager | |
| Lead Reviewer | Office and Finance Manager | |
| Approver and date of last approval | Executive Principal: 02/09/2024 | |
| Key review dates | | |
| Changes made | | |
| 15/11/2017 | B Gorsuch | |
| 01/05/2018 | B Gorsuch | Reviewed to ensure policy is compliant with GDPR regulations |
| 01/03/2020 | B Gorsuch | Email address added for SAR requests |
| 01/09/2020 | B Gorsuch | Policy updated to reflect new method of system access |
| 01/09/2022 | B Gorsuch | Staffing updated |
| 02/09/2024 | R Kozłowska | Visitor's sign in system update and staffing update (Premises Manager out of hours) |



CONTENTS

| | | |
|-----------|------------------------------------------------------------|----------|
| 1. | INTRODUCTION..... | 4 |
| 2. | OBJECTIVES OF THE CCTV SYSTEM | 4 |
| 3. | STATEMENT OF INTENT | 4 |
| 4. | SYSTEM MANAGEMENT | 5 |
| 5. | SIGNAGE | 5 |
| 6. | LIASON | 5 |
| 7. | DOWNLOAD MEDIA PROCEDURE | 5 |
| 8 | VIEWING OF LIVE IMAGES | 6 |
| 9 | DATA STORAGE/RETENTION | 6 |
| 10 | ASSESSMENT OF THE SYSTEM AND CODE OF PRACTICE | 6 |
| 11 | SYSTEM MAINTENANCE | 6 |
| 12 | COMPLAINTS | 7 |
| 13 | ACCESS BY THE DATA SUBJECT | 7 |
| 14 | PUBLIC INFORMATION | 7 |
| 15 | SUMMARY OF KEY POINTS | 7 |

1. INTRODUCTION

- 1.1 The purpose of this Policy is to regulate the management, operation and use of the CCTV system (Closed Circuit Television) at Didcot Primary Academy, hereafter referred to as 'the Academy'.
- 1.2 The system comprises of 15 PTZ (pan-tilt-zoom) cameras located in and around the school site. All cameras are monitored from the School Communications Room and images are only available to selected authorised staff (School Principal and School Office Staff). The system is also accessible from selected designated staff laptops and desktops (Senior Leadership Team and Office Staff). These devices are password protected and locked when not in use. Images are available only when devices are on the school premises.
- 1.3 This Policy follows Data Protection Act and General Data Protection Regulation guidelines.
- 1.4 The School Policy will be subject to review annually to include consultation as appropriate with interested parties.
- 1.5 The CCTV system is owned by the Academy.

2. OBJECTIVES OF THE CCTV SYSTEM

- 2.1 To protect pupils, staff and visitors.
- 2.2 To increase personal safety and reduce the fear of crime.
- 2.3 To protect the Academy's buildings and assets.
- 2.4 Without prejudice, to protect the personal property of pupils, staff and visitors.
- 2.5 To support the police in preventing and detecting crime.
- 2.6 To assist in identifying, apprehending and prosecuting offenders.
- 2.7 To assist in managing the Academy.

3. STATEMENT OF INTENT

- 3.1 The CCTV system will seek to comply with the requirements of the Data Protection Act and General Data Protection Regulations.
- 3.2 The Academy will treat the system, all information, documents and recordings (both those obtained and those subsequently used) as data protected under the Act.
- 3.3 Cameras will be used to monitor activities within the Academy and its grounds to identify criminal activity actually occurring, anticipated, or perceived. It will be used for the purpose of securing the safety and wellbeing of the pupils, staff and Academy together with its visitors.
- 3.4 The system has been designed to deny observation on adjacent private homes, gardens and other areas of private property.
- 3.5 Materials or knowledge secured as a result of CCTV will not be used for any commercial purpose.
- 3.6 Images will only be released to the media for use in the investigation of a specific crime with the written authority of the police.
- 3.7 Images will never be released to the media for purposes of entertainment.
- 3.8 The planning and design has endeavoured to ensure that the system will give maximum effectiveness and efficiency but it is not possible to guarantee that the system will cover or detect every single incident taking place in the areas of coverage.
- 3.9 Warning signs will be clearly visible on the site.

4. SYSTEM MANAGEMENT

- 4.1 The system will be administered and managed by the Academy (Office Manager and Principal) who will act as the Data Controller, in accordance with the principles and objectives expressed in the policy.
- 4.2 The day-to-day management will be the responsibility of both the Principal and the Office Manager who will act as the System Manager.
- 4.3 The system and the data collected will only be available to the Data Controller, the Principal and the System Manager. The data storage PC and Monitor will be kept in a locked room at all times. The system is accessible on designated laptops and desktops (Senior leadership team and Office Staff). Premises Manager will be able to access outside of school hours (from 5.30pm till 8am the following day and during the school holidays) when necessary. These designated devices are password protected and locked when not in use. Images are available only when devices are on the school premises.
- 4.4 The CCTV system will be operated 24 hours each day, every day of the year.
- 4.5 The System Manager will check and confirm the efficiency of the system daily and in particular that the equipment is properly recording and that cameras are functional.
- 4.6 Unless an immediate response to events is required, cameras will not be directed at an individual, their property or a specific group of individuals, without authorisation in accordance with the Regulation of Investigatory Power Act 2000.
- 4.7 The System Manager must satisfy themselves of the identity of any person wishing to view images or access the system and the legitimacy of the request. Where any doubt exists access will be refused.
- 4.8 Details of **ALL** visits and visitors will be recorded in the InVentry system. A log will be kept of any CCTV system access including the time/data of access and details of images viewed.
- 4.9 Any visit may be immediately curtailed if prevailing operational requirements make this necessary.

5. SIGNAGE

- 5.1 Signs will be positioned at entrances where CCTV operates. These signs will indicate that CCTV monitoring and recording are in use on the premises.

6. LIASON

- 6.1 Liaison meetings may be held with all bodies involved in the support of the system.

7. DOWNLOAD MEDIA PROCEDURE

- 7.1 To maintain and preserve the integrity of the data (and to ensure their admissibility in any legal proceedings) any download media used to record events from the hard drive must be prepared in accordance with the following procedures:
 - 7.1.1 Each download media must be identified by a unique mark.
 - 7.1.2 Before use, each download media must be cleaned of any previous recording.
 - 7.1.3 The System Manager will register the date and time of download media insertion, including its reference.

- 7.1.4 Download media required for evidential purposes must be sealed, witnessed and signed by the System Manager, then dated and stored in a separate secure evidence store. If a download media is not copied for the police before it is sealed, a copy may be made at a later date providing that it is then resealed, witnessed and signed by the System Manager, then dated and returned to the evidence store.
- 7.1.5 If download media is archived the reference must be noted.
- 7.2 Images may be viewed by the police for the prevention and detection of crime and authorised Securipol Staff (the Academy's designated key holding service).
- 7.3 A record will be maintained of the release of any download media to the police or other authorised applicants.
- 7.4 Viewing of images by the police must be recorded in writing.
- 7.5 Should images be required as evidence, a copy may be released to the police under the procedures described in this policy. Images will only be released to the police on the clear understanding that the download media (and any images contained thereon) remains the property of the Academy, and download media (and any images contained thereon) are to be treated in accordance with Data Protection legislation. The Academy also retains the right to refuse permission for the police to pass the downloaded media (and any images contained thereon) to any other person. On occasions when a Court requires the release of a downloaded media this will be produced from the secure evidence store, complete in its sealed bag.
- 7.6 The police may require the Academy to retain the downloaded media for possible use as evidence in the future. Such downloaded media will be properly indexed and securely stored until they are needed by the police.
- 7.7 Applications received from outside bodies (e.g. solicitors) to view or release images will be referred to the Omnia Learning Trust Legal department.

8 VIEWING OF LIVE IMAGES

- 8.1 Display equipment used to view the images from CCTV camera are located in the School Communication Room and will not be visible to other staff, pupils or members of the public.

9 DATA STORAGE/RETENTION

- 9.1 CCTV images are held on site for a maximum period of 30 days. Any data shared with the police to assist with the detection/prevention of criminal activity will be held for the period identified in the police force's data retention schedule in accordance with their specific privacy notices.

10 ASSESSMENT OF THE SYSTEM AND CODE OF PRACTICE

- 10.1 Performance monitoring, including random operating checks, may be carried out by the Principal or the Data Controller.

11 SYSTEM MAINTENANCE

- 11.1 Display equipment and recordings may be viewed by personnel authorised to undertake installation and maintenance of the CCTV system. Such viewing will be restricted to that necessary for system work.

12 COMPLAINTS

12.1 Any complaints in relation to the Academy's CCTV system should be addressed to the Principal.

13 ACCESS BY THE DATA SUBJECT

13.1 The Data Protection Act and General Data Protection Regulations provide Data Subjects (individuals to whom "personal data" relate) with a right to data held about themselves, including those obtained by CCTV.

13.1.1 Requests for Data Subject Access should be made to the Omnia Learning Trust Data Protection Officer Bethan Gorsuch by email to: admin@omnialearningtrust.org

13.1.2 Individuals submitting requests for access will be asked to provide sufficient information to enable the footage relating to them to be identified.

13.1.3 The Academy reserves the right to refuse access to CCTV footage where this would prejudice the legal rights of other individuals or jeopardise an on-going investigation.

14 PUBLIC INFORMATION

14.1 Copies of this policy will be available to the public from the school office.

15 SUMMARY OF KEY POINTS

15.1 This Policy will be reviewed annually.

15.2 The CCTV system is owned and operated by Didcot Primary Academy.

15.3 The CCTV system and images are not available to visitors except under circumstances as outlined in this policy.

15.4 Liaison meetings may be held with the police and other bodies if required.

15.5 Downloaded media will be used properly indexed, stored and destroyed after appropriate use, in accordance with the Data Protection Act.

15.6 Images may only be viewed by authorised School/Securipol Staff and the police.

15.7 Downloaded media required as evidence will be properly recorded witnessed and packaged before copies are released to the police.

15.8 Downloaded media will not be made available to the media for commercial or entertainment purposes

REFERENCES INFORMATION

The Data Protection Act

http://www.ico.org.uk/for_organisations/data_protection/topic_guides/~media/documents/library/Data_Protection/Detailed_specialist_guides/ICO_CCTVFINAL_2301.pdf