CCTV and Surveillance Schemes Policy

Document control			
Approved by	Full Trustees	Approved date	19 December 2019
Next Review	December 2020	Policy Level	GDPR
Published	https://www.dartmoormat.org.uk/policies-and-documents.html		

Version	*Date issued*	*Author*	*Update information*
V1.0	12/12/2018	N McDermott	First published version
V1.1	19/12/2019	N McDermott	Minor updates to aid reading ease. Compilation of schools' schedule. Addition of clause 3.6 and 3.7.
V 1.2	23/09/2020	N McDermott	Update to Appendix 1 Okehampton College specific details

1. Introduction

1.1. Dartmoor Multi Academy Trust is committed to safeguarding and the welfare of our pupils/students, staff, and visitors. This policy sets out the management, operation and use of CCTV surveillance systems in our schools.

1.2. **We use CCTV and Surveillance systems to**:

i. protect School buildings and their assets
ii. increase personal safety and reduce the fear of crime
iii. support the police in deterring and detecting crime
iv. assist in managing the School.

1.3. **The systems will not be used**:

i. to provide recorded images for the world-wide-web.
ii. to record sound other than in accordance with section 5 of this policy.
iii. for any automated decision taking

1.4. This policy will be reviewed annually.

2. Definitions

2.1. "the School" means member Schools of the Dartmoor Multi Academy Trust (DMAT)

2.2. "Data Controller" means the School's Data Controller (Headteacher or Head of School)

2.3. "Surveillance systems" includes CCTV systems and access control systems.

2.4. "Surveillance staff" means employees of the School, which may include senior leadership or administrators or premises staff, with the skills and permission to manage and operate surveillance systems.

3. Statement of Intent

3.1. Surveillance systems are registered with the Information Commissioner under the terms of the Data Protection Act 2018. The Dartmoor Multi Academy Trust will comply with the requirements both of the Data Protection Act and the Commissioner's CCTV Code of Practice. The Trust will treat all surveillance schemes and all information, documents and recordings obtained and used as data which are protected by the Act.

3.2. Warning signs, as required by the Code of Practice of the Information Commissioner will be placed at all access routes to areas covered by School CCTV.

3.3. Materials or knowledge secured as a result of CCTV or access control systems will not be used for any commercial purpose. Data will only be released for use in the investigation of a specific crime and with the written authority of the police. Data will never be released to the media for purposes of entertainment.

3.4. Systems are planned and designed to give maximum effectiveness, but it is not possible to guarantee that the system will cover or detect every single incident taking place in the areas of coverage. CCTV systems may include fixed or mobile cameras located around School sites.

3.5. Cameras will not focus on private homes, gardens and other areas of private property. Cameras will be positioned to avoid capturing the images of persons not visiting the premises.

3.6. Unless an immediate response to events is required, cameras will not be directed at individuals, their property or a specific group of individuals, without authorisation being obtained through an Application for the use of directed surveillance, as set out in the Regulation of Investigatory Power Act 2000. Authorising Officers for the Dartmoor Multi Academy Trust are the Chief Executive Officer (Daryll Chapman) and the Data Protection Officer (Nuala McDermott). Approval must be obtained from a Justice of the Peace in accordance with Home Office guidance.

3.7. CCTV systems which make use of wireless communication links (eg, transmitting images between cameras and a receiver) should ensure that these signals are encrypted to prevent interception.

3.8. CCTV systems which can transmit images over the internet (eg, to allow viewing from a remote location) should ensure that these signals are encrypted to prevent interception and also require some form of authentication for access (eg, a username and secure password).

3.9. Schools must ensure that cameras and systems produce clear images which law enforcement bodies (usually the police) can use to investigate crime and these can easily be taken from the system when required

4. Management of Surveillance systems

4.1. Surveillance systems will be administered and managed by the Data Controller, in accordance with the principles and objectives expressed in the code. The Data Controller is responsible for undertaking systematic checks of the management, operation and retention of data under this policy and recording such checks on the Surveillance Log.

4.2. Surveillance systems will be operated 24 hours each day, every day of the year.

4.3. Surveillance system controls and hardware will only be accessed by Surveillance staff or authorised personnel. Full details of access must be recorded in the School's Surveillance log (see Appendices for template log).

4.4. Day-to-day management is the responsibility of designated Surveillance staff. Surveillance staff will:

- check and confirm the efficiency of the system regularly including checking that cameras are functional and not obscured, recording and overwrite functions are as designed
- ensuring appropriate technical, physical and organisational security of systems

- system maintenance is up to date

4.5. **CCTV footage will only be retained for a maximum of 30 days**. This means the right of erasure may not apply as erasure will happen automatically after 30 days. On occasion, we may need to retain data for a longer period, for example, where a law enforcement body is investigating a crime and asks for it to be preserved, to give them opportunity to view the information as part of an active investigation or where the school is investigating an incident. After this time, we will permanently delete the data through secure methods.

5. Covert and audio recording

5.1. The covert surveillance activities of public authorities are not covered here because they are governed by the Regulation of Investigatory Version 1.2 8 20170609 Powers Act (RIPA) 2000 and Regulation of Investigatory Powers (Scotland) Act (RIPSA) 2000. This type of recording is covert and directed at an individual or individuals (Example: The police using covert surveillance equipment to monitor and record the activities of a suspected drug dealer to identify if related offences are committed.

5.2. The use of audio recording, particularly where it is continuous, will, in most situations, be considered more privacy intrusive than purely visual recording. Its use will therefore require much greater justification.

5.3. Audio recording will only be used where:

5.3.1. The school has identified a need or issue which can be characterised as a pressing social need and can evidence that this need must be addressed.

5.3.2. The school has considered other less privacy intrusive methods of addressing the need.

5.3.3. Having reviewed the other less privacy intrusive methods, the school has concluded that these will not appropriately address the identified issue and the only way to address the issue is through the use of audio recording.

5.3.4. The school should ensure that at the point of purchase of the audio system all appropriate privacy by design methods have been incorporated into the system. If you have already bought the system, you should look to see if you can incorporate any privacy by design technologies.

5.3.5. If the school is using audio recording, they should ensure the system they have bought provides a high enough quality of recording to achieve the stated aim.

5.3.6. The school should make it clear to data subjects that audio recording is taking place, over and above any visual recording which is already occurring.

6. Data sharing

6.1. Release of data to the police or other authorised applicants will be recorded in the Surveillance Log.

6.2. Requests by the police can only be actioned under section 29 of the Data Protection Act 1998. Recordings will only be released to the police on the clear understanding that the recording remains the property of the School, and both the recording and information contained on it are to be treated in accordance with this code. The School also retains the right to refuse permission for the police to pass to any other person the recording or any part of the information contained thereon.

6.3. Applications received from outside bodies (for example solicitors) to view or release recordings will be referred to the Head teacher. In these circumstances data will normally be released where satisfactory documentary evidence is produced showing that they are required for legal proceedings, a subject access request, or in response to a court order.

6.4. The Data Protection Act provides data subjects (individuals to whom 'personal data' relate) with a right to data held about themselves, including those obtained by CCTV. Requests for data subject access can be made in accordance with the Trust's Subject Access Request Policy and must include the date, time and location where the footage is believed to have been captured. Where information of third parties is also shown with the information of the person who has made the access request, we will consider whether we need to obscure this information. In most cases the privacy intrusion to third party individuals will be minimal and obscuring images will not be required. However, consideration will be given to the nature and context of the footage.

6.5. Requests under the Freedom of Information Act will be considered following the guidance in the ICO's CCTV Code of Practice.

7. Breaches

7.1. Any breach of this policy will be investigated by the Headteacher and the Trust's Data Protection Officer in line with the Trust's Personal Data Breach Policy.

8. Complaints

8.1. Any complaints about the School's Surveillance systems can be made via the Trust's Complaints Policy.

9. Appendices

1. Individual School CCTV schedule (and schematic for Okehampton College)
2. CCTV Signage (print on yellow paper) or ensure similar signage is displayed
3. Surveillance Systems Access Log

CCTV and Surveillance Sch

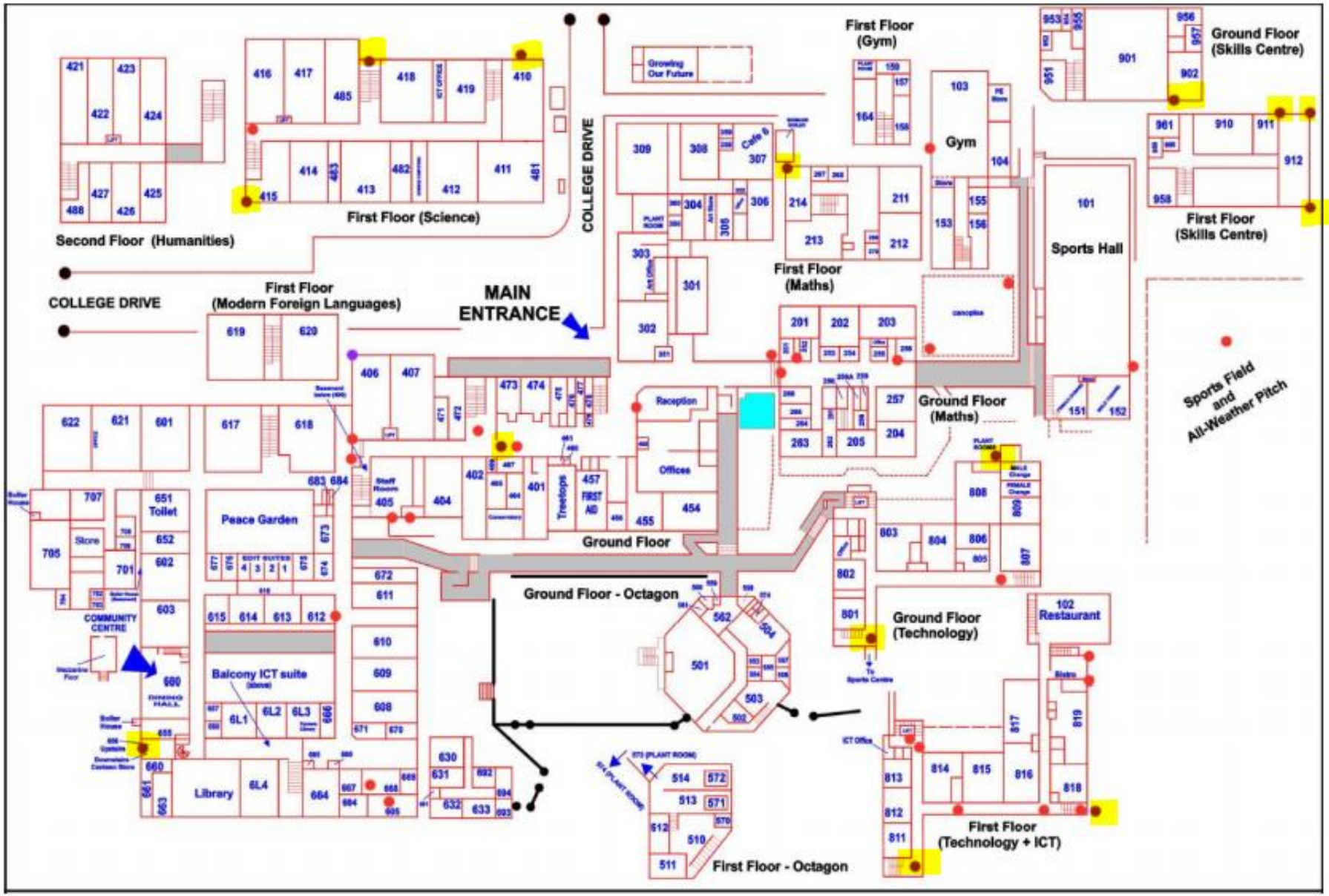
Dartmoor MULTI ACADEMY TRUST

SCHOOL NAME	CCTV	Number Cameras	Named individual responsible for system	Named roles with authority to view images on CCTV [1]	Location of cameras	Record function	Storage location	Image retention period	Service and Maintenance Contractor
Black Torrington Primary	No								
Bradford Primary	No								
Bridgerule Primary	**Yes**	2	Ian Warn	HCC Site Supervisor IT support SLT	Schematic in HCC Site Supervisors Office	Continuous	School	14 days max	Independent Fire and Security
Bridestowe Primary	**Yes**	2	Mark Butler	Head of School IT Support	Barn Owls Class. Owlets outside area	On motion	Remote	30 days max	Hub IT System Manager
Boasley Cross Primary	No								
Chagford Primary	**Yes**	1	John Coundon	Head of School IT Support Executive Headteacher	Reception foyer	On motion	School	30 days max	TBC
Exbourne Primary	No								
Highampton Primary	No								
Holsworthy Community College	**Yes**	61	Ian Warn	HCC Site Supervisor IT support SLT	Schematic in Site Supervisors Office	Continuous	School	14 days max	Independent Fire and Security
Lydford Primary	No								
Northlew Primary	No								
North Tawton Primary	No								
South Tawton Primary	No								

[1] **or authorise others to view for identification.**

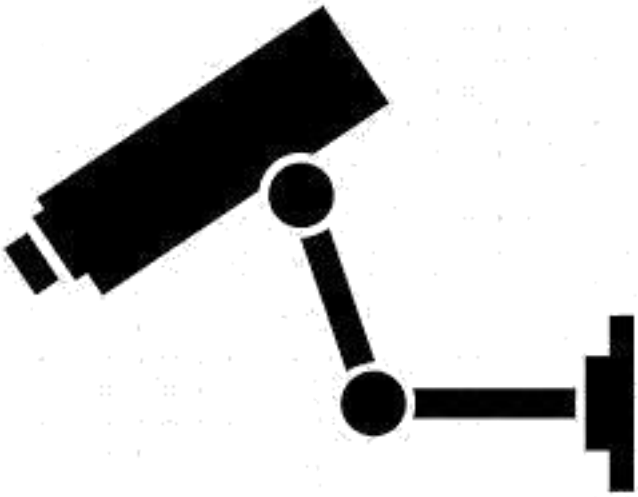
Okehampton Primary School	Yes	10	Sarah Godbeer	Headteacher, Deputy Headteacher, Assistant Headteacher, Administrator, Caretaker	See below	Continuous	School	30 days max	Metcalfe Allen
					1. Inside school reception. 2. Outside school reception 3. Outside dinner hall. 4. Outside Raven Tor. 5. Outside Hare Tor. 6. Outside Staff Room. 7. Outside Staff Room. 8. Outside Conservatory. 9. Outside Conservatory. 10. Outside Nursery				
Okehampton College	Yes	43	Carol Newman	Headteacher SLT IT Manager IT Support (IP only) Estates Team (JS, MG, DG) Behaviour Support	See Appendix 1. IP cameras in red, Analogue highlighted yellow	Internal: on motion External: continuous	School	30 days max	Hub IT System Manager
Tavistock College	Yes	TBC	L Coe	Premises Manager, Caretaker/ Electrician, Senior Leadership Team	Schematic in Premises Manager Office		School		IFS

OKEHAMPTON COLLEGE SCHEMATIC



Surveillance Systems Access Log

Name of person accessing system	Purpose of access	Date	Time	Identity checked by	Visit approved by	Notes To include details of any data removed



CCTV

Images are being monitored for the purpose of public safety, crime prevention, detection and the prosecution of offenders.

This scheme is controlled by

Dartmoor Multi Academy Trust

For further information please see
https://www.dartmoormat.org.uk/gdpr.html