Dunottar School

CCTV Policy

Table of Contents

1. Introduction

1.1 Dunottar 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 Dunottar School, High Trees Road, Reigate Surrey RH2 2EL and managed by Dunottar School and its appointed agents. The data controller for CCTV images held by Dunottar School is United Church Schools Trust (UCST). UCST is registered with the Information Commissioner's Office (ICO). The registration number is Z533407X

The Group's Data Protection Officer is responsible for ensuring that UCST 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 Dunottar School's designated Data Protection Lead 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 provided 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 provides details of the contact email address.

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, buildings (internal and external), within buildings 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, except by prior agreement by local residents where it is at their request.

2.8 A surveillance camera is positioned along the public footpath outside the school, with footage accessible to both law enforcement and the public as needed. There is signage to inform the public and gives notice that images are being recorded for purposes of crime prevention and public safety in association with Surrey Police. The public can email the data controller of the scheme with any questions to spol.cctv@dunottarschool.com, which is monitored frequently.

2.9 The CCTV system is operational and capable of being monitored for 24 hours a day, every day of the year.

2.10 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 purposes of the School's CCTV system are as follows:

- for the prevention, reduction, detection and investigation of crime and other incidents;

- to ensure the safety of staff, children, visitors and members of the public; and

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 not routinely monitored in real time but are able to be in the IT Office on an as and when needed basis.

4.2 Images are recorded and stored centrally on a server located securely in the server room and are viewable in the IT office by all CCTV trained staff. Downloaded footage or snapshot images are securely stored on Microsoft 365 cloud storage in accordance with the process outlined in the retention of images section. All images recorded by the system remain the property and copyright of United Learning.

Additional staff may be authorised by the Headmaster to monitor cameras on a view only basis to support trained staff i.e. in identifying specific children.

Trained staff are as follows: Network Manager & IT Technician.

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 The use of cameras placed in classrooms W7 and W8 is primarily for the protection of IT assets and monitoring access into the IT server room. (will be carried out in accordance with Part 3 of the Employment Practices Code.

The monitoring of classrooms should be clearly identified in the Privacy Impact Assessment. This should cover:

- identifying clearly the purpose(s) behind the monitoring arrangement and the benefits it is likely to deliver
- identifying any likely adverse impact of the monitoring arrangement
- considering alternatives to monitoring or different ways in which it might be carried out
- taking into account the obligations that arise from monitoring
- judging whether monitoring is justified

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.

4.8 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. However, there are no cameras needed or placed in any of these areas mentioned above.

4.9 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 Headmaster and Director of People will be sought before the installation of any covert cameras. The Headmaster 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.

4.10 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.

https://ico.org.uk/media/for-organisations/documents/1064/the_employment_practices_code.pdf

5. Compliance with Data Protection Legislation

5.1 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; 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

e. 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.

7. Access to and disclosure of images to third parties

7.1 A request for images made by a third party should be made in writing.

7.2 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.

7.3 All unexpected requests for CCTV images by third parties, 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 request*s.

7.4 Where a suspicion of misconduct arises and at the formal request of the Investigating Officer, HR Manager/ Business Partner or a member of the SLT, the Headmaster may provide access to CCTV images for use in staff disciplinary cases.

7.5 The Headmaster or SLT may provide access to CCTV images to Investigating Officers when sought as evidence in relation to staff discipline cases.

7.6 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.

8. Retention of images

8.1 Unless required for evidential purposes, the investigation of an offence or as required by law, CCTV images will be retained for no longer than 30 days from the date of recording. Images will be automatically overwritten after this point.

8.2 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.

8.3 Where an image is required to be held in excess of the retention period referred to in 7.1, the Headmaster 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.

8.4 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.

8.5 Access to retained CCTV images is restricted to the Headmaster and SLT and other persons as required and as authorised by the Headmaster. These individuals are: Network Manager and IT Technician.

9. Complaints Procedure

9.1 Complaints concerning the School's use of its CCTV system or the disclosure of CCTV images should be made in writing to the Headmaster at Dunottar School, High Trees Road, Reigate, Surrey RH2 7EL. Any complaint will be handled in accordance with the school's complaints policy.

9.2 All appeals against the decision of the Headmaster should be made in writing to the Chair of the LGB.

10. Monitoring Compliance

10.1 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.

10.2 All staff with responsibility for accessing, recording, disclosing or otherwise processing CCTV images will be required to have undertaken United Learning Data Protection training.

11. Policy review

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

Version number:	1.		Target Audience:	Data Protection Leads and Head Teachers
UCST/ULT/Both:	Both		Reason for version change:	UK GDPR Review cycle
Date Authorised:	September 2018		Name of owner/author:	Alison Hussain
Authorised by:	FIC		Name of individual/department responsible:	Alison Hussain, Company Secretary and Data Protection Officer
Date reviewed:	March 2024			
Reviewed by:	IGSC			
Date of next review:	March 2025			
			Governor responsible for Policy:	Mr Dan Hawker
			Reviewed by:	John Weiner/Tom Stevens

Appendix A - Data Protection Impact Assessment Procedure

Data Protection Impact Assessment template

If the screening questions in Appendix A have identified the need for a DPIA use the following template to record your DPIA process and results. Please refer to the guidance in appendix C.

Step 1: Describe the nature of the data processing

Answer all questions in this section.

Department(s)	Whole School but mainly Estates and IT

Q1: Brief description of the processing	CCTV cameras will cover the school grounds and public areas around the external boundary of the school.
Q2: Why do you need to undertake this processing?	The reason for this deployment of CCTV is for the security and protection of students, staff, stakeholders and the property. The CCTV cameras covering the external boundary is due to a number of incidents including potential drug dealing.
Q3: Types of personal data that will be processed	
	Special category personal data? □ Yes ✕ No
Q4: Whose personal data is it?	The data subjects whose personal data will be processed by the CCTV system will include staff, parents, visitors and members of the public including children and vulnerable groups of people. The scope of the CCTV system on the external boundary is for crime prevention and public safety.
Q5: What IT (software packages) are used in processing the personal data?	Fixed CCTV cameras are installed (Networked)
	Is this new to the users? □ Yes ✕ No

Q8: Do you share the personal data outside of United Learning?	□ Yes ✕ No
	If yes are you sharing the data with a □ data controller or a □ data processor?
	Name of organisation(s) who you will be sharing the data with: Potentially only the Surrey Police, but no requests have been made.

Step 2: Establishing the lawfulness of the processing

Please indicate which of the legal basis you are relying on to process the personal data.		
(a) the data subject has given consent to the processing of his or her personal data for one or more specific purposes;		If yes state how you will collect consent and where you will record it. It is the Users choice to sign up if they wish – this is not a compulsory app.
(b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;		If yes, what type of contract are you referring to? □ Employment □ Independent school parent contract □ Other contract (please specify) _____
(c) processing is necessary for compliance with a legal obligation to which the controller is subject;		If yes please specify the legal obligation
(d) processing is necessary in order to protect the vital interests of the data subject or of another natural person;		If yes please specify what you consider the vital interests to be
(e) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child		□ The processing is an ordinary part of running a school? (Independent Schools) □ The processing is for the purpose of keeping in touch with alumni □ The processing is for another purpose (please specify) _____

2b) Will you be processing any of the following special categories of personal data?

- Racial and ethnic origin
- Political opinions
- Religious or philosophical beliefs
- Trade union membership
- Health data
- Sex life
- Sexual orientation
- Genetic data
- Biometric data for the purpose of uniquely identifying a natural person

If yes please indicate which of the following legal basis you are relying on to process the data.		
GDPR article 9 (a)the data subject has given explicit consent to the processing of those personal data for one or more specified purposes,		If yes state how you will collect consent and where you will record it.
GDPR article 9 (b) & DPA 2018 Sch 1 part 1 s1 processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law in so far as it is authorised by Union or Member State law		If yes please state which laws are applicable
GDPR article 9 (f) processing is necessary for the establishment, exercise or defence of legal claims;		
GDPR article 9 (h)) & DPA 2018 Sch 1 part 1 s2 processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee,		
DPA 2018 Sch 1 part 1 s5 Processing is necessary for statutory and government purposes		
DPA 2018 Sch 1 part 1 s8		

Necessary for identifying or keeping under review the existence or absence of equality of opportunity or treatment		
DPA 2018 Sch 1 part 1 s16 Support for individuals with a particular disability or medical condition		
DPA 2018 Sch 1 part 1 s17 Processing necessary for the provision of confidential counselling advice or support where the consent of the data subject cannot be obtained		
DPA 2018 Sch 1 part 1 s18 Necessary to protect an individual from neglect or physical, mental or emotional harm or to protect the physical, mental or emotional wellbeing of an individual		
DPA 2018 Sch 1 part 1 s20 Necessary for insurance purposes and is in the substantial public interest		
DPA 2018 Sch 1 part 1 s21 Necessary for the purpose of making a determination in connection with eligibility for, or benefits payable under, an occupation pension scheme Where the data subject is a relative of a member of the scheme.		

Step 3: Assessing Compliance

3 (a) lawfulness, fairness and transparency

Question	Response	Further action if required
Q1. Is the processing covered by the school's privacy notice?	✓	N/A
Q2. If new data is being collected do the data collection forms clearly explain what the data will be used for and who it will be shared with?	✓	
Q3. If a data processor is being used does the contract comply with the GDPR Article 28 requirements? (see annex E)	✓	Dunottar School will maintain sole access as the data controller. If another party was to request access, this would be reviewed on a case by case basis in line with the schools CCTV policy.

3 (b) purpose limitation

Question	Response	Further action if required
Q1. Has a clear purpose for the processing been identified and documented?	✓	
Q2. Are you using the data for the purpose for which it was collected? Please list this here.	✓	Protection and Prevention
Q3. Do United Learning's notifications to the ICO cover the processing? (See annex F)	✓	

Question	Response	Further action if required
Q4. How will you ensure use of the personal data is limited to these purposes?		Only the schools Network Manager has access to the CCTV network and this is to be reviewed annually.

3 (c) data minimisation

Question	Response	Further action if required
Q1. Is each category of data that will be used necessary and relevant for the project? Is there any data you could not use and still achieve the same goals?	✗	
Q2. Is the data being used adequate for the purposes of the project? *For example if you are making decisions about people are you collecting enough information?*	✓	
Q3. Can the data be pseudonymised / anonymised for the project?	✗	

3 (d) accurate and up to date

Question	Response	Further action if required
Q1. What steps will be taken to ensure the data used is accurate?		The CCTV fixed network will only record in real time.

Question	Response	Further action if required
Q2. How will the accuracy of the data be maintained? Can records be easily amended?		
Q4. Will multiple copies of records be created? How will you keep track of these and ensure they are all	✓	Copies of the recorded surveillance will only be downloaded for legal requirements ie if a crime has been committed.

3 (e) Data retention and destruction

Question	Response	Further action if required
Q1. Is the data used for the project covered by the school's record retention policy?	✓	Data/recordings will be deleted in-line with the schools data retention policy.
Q2. How long will the data used be retained?		3 months
Q3. How will you ensure the destruction of the data when it is no longer needed?		All data will be permanently destroyed after 3 months in line with the data retention policy.
Q4. Will multiple copies of the data be created? If so how will you keep track of the copies and ensure they are destroyed?		No

3 (f) Rights of the data subject

Question	Response	Further action if required
Q1. Can the data be searched in the event of a SAR and an individual's information extracted?	✓	Yes, CCTV recording posters have been added around the site and on the external boundary of the school for the purpose of crime prevention, public safety, named controller and displaying how to contact the school in case of a SAR.
Q2. Can one individual's data be deleted in the event of a successful request to have data erased?	x	
Q3. Is any processing under the project likely to cause damage or distress to individuals?	x	
Q4. Does the project involve any direct marketing?	x	
Q5. Does the project involve any automated decision making?	x	

3 (g) Data security, integrity and confidentiality

Question	Response	Further action if required
Q1. Who will have access to the data?		The schools network manager is the only person will access.

Question	Response	Further action if required
Q2. How will access to the data be granted?		Through a request of a SAR.
Q3. If using a secure system can you / will you prevent the data from being downloaded from the system / printed?		Only the schools network manager has access to the software.
Q4. If storing in office 365 how will you control access to the data and prevent proliferation of copies?		N/A
Q5. If storing the personal data in paper form how will you ensure it is kept secure?		N/A
Q6. How will data be shared by people working on the project?		N/A

3 (h) If there are any data processors involved in the project please answer the following questions for each data processor (i.e. you may be using a software developer and a data aggregator)		
Question	**Response**	**Further action if required**
Q1. How will the data processor access the data?		N/A
Q2. What security guarantees do you have?		Unique email, username and password – plus the possibility of biometrics

Question	Response	Further action if required
Q3. Is the contract compliant with Article 28 GDPR? (see annex E for requirements)		
Q4. How will the actions of the data processor be monitored and enforced?		
Q5. Will the data processor keep the personal data within the EU?	✓	

3 (i) If your project involves use of a website

Question	Response	Further action if required
Q1. Do you use cookies or similar technologies to store or gain access to information about users of your website?	x	
Q2. If yes, how do you provide information about the cookies to the user and obtain their consent?		

3 (j) Human Rights Act 1998

Question	Response	Further action if required
Q1. Does the project involve any intrusion in to the private and family life of individuals? *I.e. monitoring, surveillance or recording activities*	✓	There is surveillance and recording of activities. CCTV recordings will be permanently deleted after a specific time (in line with the data retention policy) if no criminal act has been recorded.

Question	Response	Further action if required
Q2. Can any such intrusion be justified? *Legal requirement, public safety, protection of the rights and freedoms of others.*		Public safety and the legal requirement to provide a safe space for students, staff and stakeholders.

Signed: AK

Date: 25/05/2018

reviewed 14/12/2023

Name: Anthony Kerr

Position: Data Manager

You should now pass this form to your school Data Protection Lead for review.

Step 4: 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 being until this is completed.

Immediate actions required

Examples might include revisions to one or more privacy notices (either to improve the transparency of the statement or to include new data processing not referred to previously) and/or revisions to data sharing/data processing agreements.

Any actions here MUST be reviewed and checked for implementation within one month of the date below.

Recommendations for business process enhancements

Examples might include: changes to school processes, review of document storage, training or awareness-raising.

Any recommendations here MUST be considered and responded to within two months of the date below.

Signed (School DPL): RAS **Date:**

Name: **Rhona Stringer**

Step 5: Receipt & Review by the Group Data Protection Officer's team

Comments

Signed: **Date:**

Name: