Surveillance Security Policy

Person Responsible:	Mrs A Dalglish	**Frequency of Review:**	1 Year
Authorisation By:	Headteacher	**Notice Date:**	08/11/2022
Authorisation Date:	08/12/2021	**Review Due By:**	08/12/2022

1 Introduction

As part of Upper Wharfedale School's programme to comply with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 (DPA), it has a suite of Information Governance policies.

The Surveillance policy concerns the use and governance with regards to the systems; and the processing of personal data which has been collected by using surveillance technology. The policy is written in accordance with various data protection legislation, and the Information Commissioner's Office's (ICO) Surveillance Code of Practice.

2 Scope

This policy applies to all school employees (both those employed directly by the school and those employed on behalf of the school by a local authority (or other such body), any authorised agents working on behalf of the School, including temporary or agency staff, governors, volunteers, and third party contractors.

This Policy will refer to all individuals within scope of the policy as 'employees'. Employees who are found to knowingly or recklessly infringe this policy may face disciplinary action.

Surveillance is the monitoring of behaviour, activities, or other changing information for the purpose of influencing, managing, directing, or protecting people. The school only uses surveillance in the context of CCTV, e-monitoring software and call recording software.

The school does not operate covert surveillance technologies and therefore this policy does not cover the use of such technology.

3 CCTV

3.1 Introduction

The system comprises a number of dome cameras located around the school site. All cameras are monitored from a Central IT Support Office and are only available to designated staff – members of the ICT Support and Site Teams and members of the Senior Leadership and Management Team.

The CCTV system is owned by Upper Wharfedale School. The Head Teacher is responsible for compliance with the policy.

3.2 Planning CCTV Systems

Any new implementation of CCTV systems will employ the concept of 'privacy by design' which will ensure that privacy implications to data subjects will be considered before any new system is procured. The prescribed method for this is through the completion of a Data Protection Impact Assessment (DPIA).

The school has various statutory responsibilities to protect the privacy rights of data subjects. Therefore during this planning phase, the school will consider:

I. The purpose of the system and any risks to the privacy of data subjects,

II. That there are statutory requirements placed on the location and position of cameras. This means that cameras must be positioned to meet the requirement(s) of the intended purpose(s) and not exceed the intended purpose(s).

III. The obligation to ensure that the CCTV system can meet its intended purpose(s) also means that the system specification must be such that it can pick up any details required for these aims. For example the system must record with sufficient resolution to perform its task.

IV. The system must also have a set retention period (the typical retention period is one month) and, where appropriate, the school must also have the ability to delete this information prior to the set retention period in order to comply with the rights of data subjects.

V. That the school will need a level of access to the system and there will need to be the option to provide other agencies (such as law enforcement agencies) with specific footage if requested. If a data subject is captured and recorded by the system, then that individual also has the right to request a copy of that footage under subject access provisions.

The school will ensure that a contract will be agreed between the school (as Data Controller) and the CCTV system provider. Consideration should also be given as to whether there are any joint data controller arrangements where the system is shared with another organisation. Data Processing clauses must be included within the written contract if the provider will be processing (e.g. monitoring, storing, accessing) the data on behalf of the school.

3.3 CCTV Privacy Notices

The processing of personal data requires that the individuals that the data relates to (in this case any individuals captured by the CCTV) are made aware of the processing. Therefore the use of CCTV systems must be visibly signed.

The signage will include the purpose for the system (e.g. the prevention or detection of crime), the details of the organisation operating the system and who to contact about the system (including basic contact details). The signage must be clear enough that anyone entering the recorded area will be aware that they are being recorded.

A more detailed Privacy Notice for the use of CCTV must be maintained with the intention of informing data subjects of their rights in relation to surveillance data.

3.4 Access to CCTV Recordings

CCTV footage will only be accessed to comply with the specified purpose. For example, if the purpose of maintaining a CCTV system is to prevent and detect crime then the footage must only be examined where there is evidence to suggest criminal activity having taken place.

The CCTV system will have a nominated Information Asset Owner who will be responsible for the governance and security of the system. The Information Asset Owner will authorise officers to access CCTV footage either routinely or on an ad-hoc basis.

3.5 CCTV Footage Disclosures

A request by individuals for CCTV recordings that include footage of them should be regarded as a subject access request (SAR). For more information on the right of access for individuals captured on CCTV, refer to the School's Information Policy.

If the school receives a request from another agency (for example a law enforcement agency) for CCTV recordings, then it will confirm the following details with that agency:

- the purpose of the request,
- that agency's lawful basis for processing the footage,

- confirmation that not receiving the information will prejudice their investigation,
- whether the school can inform the data subject of the disclosure, and if not, the reasons for not doing so.

The school will liaise with its appointed Data Protection Officer should it have any concerns about such requests.

3.6 Review of CCTV

CCTV systems must be reviewed annually to ensure that systems still comply with data protection legislation and national standards. The Information Asset Owner should use the checklist included in Appendix 1 of this policy to complete this review. It is the responsibility of the Information Asser Owner to ensure reviews are completed and evidence of those reviews taking place are maintained.

3.7 Camera Locations

There are 5 cameras located in school which are all visual only, no audio is recorded.

- Sports Block Reception
- Reception
- Main classroom corridor
- Sports Hall / Swimming Pool corridor
- Hall (does not record only used for live feed backstage during School Performances)

4 E-Safety Monitoring

4.1 Introduction

The school operates 'e-safety' monitoring software systems in order to ensure the safety of our staff and students when accessing online resources. This is considered to be a form of non-convert surveillance processing. The school uses Smoothwall web filtering device.

4.2 Planning Monitoring System

Any new implementation of systems will employ the concept of 'privacy by design' which will ensure that privacy implications to data subjects will be considered before any new system is procured. The prescribed method for this is through the completion of a Data Protection Impact Assessment (DPIA).

The school has various statutory responsibilities to protect the privacy rights of data subjects. Therefore during this planning phase, the school will consider:

- The purpose of the system and any risks to the privacy of data subjects,
- The system must be installed in a way which meets the requirement(s) of the intended purpose(s) and not exceed the intended purpose(s).
- The obligation to ensure that the system can meet its intended purpose(s) also means that the system specification must be such that it can pick up any details required for these aims. For example the system must record with sufficient detail to perform its task.
- The system must also have a set retention period and, where appropriate, the school must also have the ability to delete this information prior to the set retention period in order to comply with the rights of data subjects.
- That the school will need a level of access to the system and there will need to be the option to provide other agencies (such as law enforcement agencies) with specific system data if requested. If a data subject's activity is captured and recorded by the system, then that individual also has the right to request a copy of that data under subject access provisions.

The school will ensure that a contract will be agreed between the school (as Data Controller) and the system provider. Consideration should also be given as to whether there are any joint data controller arrangements where the system is shared with another organisation. Data Processing clauses must be included within the written contract if the provider will be processing (e.g. monitoring, storing, accessing) the data on behalf of the school.

4.3 System Privacy Notices

The processing of personal data requires that the individuals that the data relates to (in this case any individuals whose activity is recorded by the system) are made aware of the processing. Therefore, the use of monitoring systems must be visibly signed – for example on the log in screen of computers where the system is installed.

A more detailed Privacy Notice for the use of the system must be maintained with the intention of informing data subjects of their rights in relation to surveillance data. This privacy notice should link to the privacy notice of any system provider.

4.4 Access to Systems Data

System data will only be accessed to comply with the specified purpose. For example, if the purpose of maintaining the monitoring system is to safeguard children, then the data must only be examined where there is evidence a child is at risk.

The system will have a nominated Information Asset Owner who will be responsible for the governance and security of the system. The Information Asset Owner will authorise officers to access the system data either routinely or on an ad-hoc basis.

4.5 Monitoring Data Disclosures

A request by individuals for system data that includes their activity should be regarded as a subject access request (SAR). For more information on the right of access for individuals refer to the School's Information Policy.

If the school receives a request from another agency (for example a law enforcement agency) for system data, then it will confirm the following details with that agency:

- the purpose of the request,
- that agency's lawful basis for processing the data,
- confirmation that not receiving the data will prejudice their investigation,
- whether the school can inform the data subject of the disclosure, and if not, the reasons for not doing so.

The School will liaise with its appointed Data Protection Officer should it have any concerns about such requests.

4.6 Review of Systems

Systems must be reviewed annually to ensure that systems still comply with data protection legislation and national standards. The Information Asset Owner should use the checklist included in Appendix 1 of this policy to complete this review. It is the responsibility of the Information Asser Owner to ensure reviews are completed and evidence of those reviews taking place are maintained.

5 Call Recording Software

5.1 Introduction

There is a call recording feature on the telephone system which allows members of staff to record a call by pressing a button on their handset, to ensure the health and wellbeing of staff and students. Calls are only recorded if this feature is activated by the user.

5.2 Operation

The following extensions have call recording enabled, and are operated using the button identified in the list:

- Extension 201 – button 11
- Extension 204 – button 8
- Extension 205 – button 8
- Extension 213 – button 8

The call is then stored on the handset as a voicemail. A light will show in the top right-hand corner of the handset when the call has been ended. To access the recording, the user must dial into their voicemail using a password to access the messages. The call is stored until it is deleted by the user.

6 Complaints

Complaints by individuals about the use of surveillance systems, or the way surveillance data is processed, should be treated as a data protection concern and the school's data protection officer should be made aware.

The School's Data Protection Officer is:

Schools Data Protection Officer
Veritau Ltd
County Hall
Racecourse Lane
Northallerton
DL7 8AL

schoolsDPO@veritau.co.uk
01904 554025

Please ensure you include the name of your school in all correspondence

7 Records of Processing

The school has a duty under Article 30 of the UK GDPR to ensure that all instances of data processing activity is recorded for regulatory inspection where required. The school maintains an information asset register in order to fulfil this requirement.

The school will ensure that the use of surveillance systems is recorded on their information asset register. This should detail each separate surveillance system in use.

8 Related Documents

Employees who are responsible for planning, maintaining, or reviewing the implementation of a surveillance system are encouraged to read the following related documents prior to implementation:

- ICO Surveillance Code of Practice (External Link)
- The school's Data Protection Impact Assessment (DPIA) template (available through Veritau)

9 Appendix 1 – Surveillance System Checklist

School Name:

Name and Description of Surveillance System:		
The purpose and requirements of the system are addressed by the system (i.e. the cameras record the required information)	**YES**	**NO**
	Notes:	
The system is still fit for purpose and produces clear images of adequate resolution.	**YES**	**NO**
	Notes:	
Cameras are sited in effective positions to fulfil their task.	**YES**	**NO**
	Notes:	
Cameras are positioned so that they avoid capturing the images of persons not visiting the premises and/or neighbouring properties.	**YES**	**NO**
	Notes:	
There are visible signs showing that CCTV is in operation. These signs include: ▪ Who operates the CCTV, ▪ Their contact details, ▪ What the purpose of the CCTV is.	**YES**	**NO**
	Notes:	
CCTV recordings are securely stored and access limited.	**YES**	**NO**
	Notes:	
	YES	**NO**

The system has the capability to transfer recordings to law enforcement or to fulfil a request for an individual's own personal information.	**Notes:**	
The system has a set retention period. This retention period should only be long enough to fulfil the CCTV's purpose and not longer. Outside of this retention period information should be deleted	**YES**	**NO**
	Notes:	
The system users should be able to selectively delete information still inside the retention period to fulfil the right to erasure.	**YES**	**NO**
	Notes:	
All operators have been authorised by the Information Asset Owner and have sat their mandatory data protection training.	**YES**	**NO**
	Notes:	
The system has been added to the school/MAT's central record of surveillance systems. (This is particularly relevant if there are multiple systems or they are spread across multiple sites).	**YES**	**NO**
	Notes:	

Checklist Completed By: Name: Job Title: Date:	**Checklist Reviewed and Signed By (Information Asset Owner):** Name: Job Title: Date: