

Surveillance and CCTV Policy

School Name: The White Horse Federation

Version No:

Ratified date: March 2024

Author: Lyn Rouse

Interim Review Date: N/A

Owner: Helen Peace

Next Review Date: December 2024

Approved by: Board of Trustees

Executive Summary

The Surveillance and CCTV Policy aims to ensure the safety and security of students, staff, contractors, visitors and school premises while maintaining privacy and complying with the legal and ethical standards.

It establishes guidelines for the use, installation and management of surveillance cameras and CCTV systems within the school premises. It aims to deter, prevent and identify unlawful activities, ensuring a safe environment and protection of the school property.

Personal data, as defined by Data Protection laws, refers to any information that relates to an identified or identifiable individual. CCTV captures images and potentially other personal information of individuals within its range. Therefore, to ensure compliance with data protection regulations, the data processor must adhere to the CCTV policy.

By implementing this comprehensive Surveillance and CCTV policy, TWHF aims to create a secure environment that fosters learning while respecting the privacy of all individuals within its premises.

Statement of Intent

We take our responsibility towards the safety of staff, visitors and pupils very seriously. To that end, we use surveillance cameras to monitor any instances of aggression or physical damage to our school and its members.

The purpose of this policy is to manage and regulate the use of the surveillance and CCTV systems at the school and ensure that:

- We comply with the UK GDPR.
- The images that are captured are useable for the purposes we require them for.
- We reassure those persons whose images are being captured, that the images are being handled in accordance with data protection legislation.

This policy covers the use of surveillance and CCTV systems which capture moving and still images of people who could be identified, as well as information relating to individuals for any of the following purposes:

- Observing what an individual is doing.
- Taking action to prevent a crime.

The surveillance system will be used to:

- Maintain a safe environment.
- Ensure the welfare of pupils, staff and visitors.
- Deter criminal acts against persons and property.
- To ensure a person's conduct meets with the White Horse Federation code of conduct.
- Assist the police in identifying persons who have committed an offence

Contents

1. Aims
2. Legal Framework
3. Definitions
4. The data controller
5. Roles and responsibilities
6. Purpose and Justification
7. Protocols
8. Security and Storage
9. Code of Practice
10. Access including SAR
11. Monitoring and Review
12. CCTV information

Appendix 1: Personal data breach procedure

Appendix 2: CCTV Details

1. Aims

This policy aims to address TWHF's obligations under the General Data Protection Regulations (GDPR) and the Code of Practice provided by the Information Commissioners Office.

2. Legal Framework

This policy has due regard to all relevant legislation and statutory guidance including, but not limited to, the following:

- Regulation of Investigatory Powers Act 2000
- Protection of Freedoms Act 2012
- The UK General Data Protection Regulation (GDPR)
- Data Protection Act 2018
- UK GDPR 2021
- Human Rights Act 1996
- Freedom of information Act 2000
- The Education (Pupil information) (England) Regulations 2005 (as amended in 2016)
- The Freedom of Information and Data Protection (Appropriate Limit and Fees) Regulations 2004
- School Standards and Framework Act 1998
- Children Act 1989
- Children Act 2004
- Equality Act 2010

This policy operates in conjunction with the following statutory and non-statutory guidance:

- Home Office (2021) 'The Surveillance Camera Code of Practice'
- ICO (2021) 'Guide to the UK General Data Protection Regulation (UK GDPR)'
- ICO (2017) 'In the picture: A data protection code of practice for surveillance cameras and personal information'
- ICO (2022) 'Video Surveillance'
- DfE (2022) 'Protection of biometric data of children in schools and colleges'

This policy operates in conjunction with the following school policies:

- Online Safety Policy
- Data Protection Policy

3. Definitions

Terminology	Definition
Surveillance	Monitoring the movements and behaviour of individuals; this can include video, audio or live footage e.g. real-time recordings and live streams. For the purpose of this policy only video footage will be applicable.
Overt Surveillance	Surveillance which is clearly visible and signposted around the school and does not fall under the Regulation of Investigatory Powers Act 2000
DPO	Data Protection Officer, the individual designated in overseeing data protection strategy.

The White Horse Federation does not condone the use of covert surveillance when monitoring the school's staff, pupils and/or volunteers. Covert surveillance will only be operable in extreme circumstances.

Data Controller	A data controller is a person or organisation that determines the purpose and means of processing personal data.
Data Processors	A person that processes data on behalf of the data controller.

4. The Data Controller

The White Horse Federation processes personal data relating to parents, pupils, staff, governors, visitors and others, and therefore is a **Data Controller**.

The White Horse Federation is registered as a data controller with the ICO and will renew this registration annually or as otherwise legally required.

5. Roles and Responsibilities

This policy applies to everyone, all staff employed by our Federation, those who volunteer in any capacity including but not limited to Trustees, Local governors, Parent helpers and to external organisations or individuals working on our behalf.

Staff who do not comply with this policy may face disciplinary action. This policy does not form part of any employee's contract of employment and may be amended at any time.

5.1 Trustees & Governing board

The Board of Trustees have overall responsibility for ensuring that The White Horse Federation complies with all relevant data protection legislations.

The school governing bodies are overall responsible for ensuring their school complies with all relevant data protection legislation including this policy, Surveillance and CCTV.

5.2 Data Protection Officer

The role of the DPO includes:

- Reporting to the highest management level of the TWHF e.g. Board of Trustees, CEO and COO.
- Confer with the Principal to confirm who has access to CCTV.
- Ensuring that all data processors at the school handle and process surveillance and CCTV footage in accordance with data protection legislation.
- Ensuring that surveillance and CCTV footage is obtained in line with legal requirements.
- Ensuring consent is clear, positive and unambiguous. Pre-ticked boxes and answers inferred from silence are non-compliant with the UK GDPR.
- Ensuring that surveillance and CCTV footage is destroyed in line with legal requirements when it falls outside of its retention period.
- Keeping comprehensive and accurate records of all data processing activities, including surveillance and CCTV footage, detailing the purpose of the activity and making these records public upon request.
- Informing data subjects of how their data captured in surveillance and CCTV footage will be used by the school, their rights for the data to be destroyed and the measures implemented by the school to protect individuals' personal information.
- Preparing reports and management information on the school's level of risk related to data protection and processing performance.
- Abiding by confidentiality requirements in relation to the duties undertaken while in the role.
- Dealing with freedom of information requests and subject access requests (SARs) in line with legislation, including the Freedom of information Act 2000.

The DPO is Lyn Rouse and is contactable via email at DPO@twhf.org.uk

5.3 The Role of the Principal includes:

- Conferring with the DPO to discuss CCTV release to third parties.
- Reviewing the Surveillance and CCTV Policy to ensure it meets the local needs of the school.
- Always stay informed about the policy to prevent function creep.
- Communicating any changes with all members of staff.
- Working with the DPO to complete the CCTV DPIA.
- To be aware at all times of who has access to CCTV.
- Ensure that any new installation of CCTV systems is compliant with guidance from the DPO.
- Ensure that only those with authorised access have access to view CCTV.
- Access to CCTV remains strictly limited.

5.4 The Role of the Site Team

- The Site Manager will ensure that the equipment is working correctly, including camera operation, clarity and view and effective recording.
- Ensure CCTV equipment is serviced annually by a competent contractor and records of the service should be retained on site.
- Performance monitoring, including random operating checks, to be carried out, under the direction of the principal.

5.5 The Role of a CCTV Operator

- The system will be operated by a nominated person, as agreed by the principal.
- Understand where the cameras are and what they capture.
- Understand that we do not enable audio.
- Understand that the retention period is 30 days.
- Understand that access to CCTV should be logged and submitted to the DPO.
- Understand that the release of images is strictly forbidden unless agreed by DPO.

5.6 The Role of the IT Network Manager includes:

Each secondary school within the White Horse Federation has assigned an IT Network Manager as an information Asset Owner. The IT Network Manager will aid the Senior Head of IT and Head of GDPR by ensuring:

- That information flows smoothly between the Senior Head of IT, DPO and school
- Challenge security of CCTV systems and employees working practice
- Identify risks for data protection and report these immediately to the DPO.
- To recognise when to contact the DPO and to recognise when a DPIA is required.
- To contact the DPO if this policy is not being followed.

5.6 All staff

Staff are responsible for:

It is imperative that everyone is aware that CCTV is classified as 'Personal Data' and that access is strictly limited to authorised operators.

Staff should also be aware of:

- Who the DPO for the organisation is
- How to report a breach of data protection
- How to handle requests for CCTV data
- Be aware of and adhere to this policy which governs the collection, storage and use of personal data obtained through CCTV.
- To contact the DPO if this policy is not being followed.

Any breach of this policy by employees may be subject to disciplinary action and any instance will be referred to the DPO.

All breaches will be immediately investigated by the Principal and an independent investigation may be carried out by the DPO to mitigate any repeats.

6 Purpose and Justification

Surveillance will be used as a deterrent for violent behaviour, misconduct and damage to the school.

We use CCTV if we suspect pupil, staff and any third party conduct does not meet the White Horse Federation standards. Therefore, from time to time, it may be necessary to view the CCTV for expulsion, disciplinary or safeguarding purposes. However, CCTV will not be viewed solely for the purpose of monitoring movement.

If upon review a disciplinary action is observed, CCTV can be used for the purpose of a disciplinary investigation. CCTV will not be viewed solely for the purpose of monitoring behavior but will be subject to review if standards are thought to be breached.

Third parties and contractors may also have images of CCTV shared with their organisation following an incident or concern raised by the school.

If, during a DPIA the camera is found to have fulfilled their purpose and is no longer required, the DPO will take measures to deactivate them.

For the safety and well-being of individuals there are some **areas** that are continually monitored, these **areas** have additional signage.

We will adhere to the ICO's guidance for the use of CCTV.

We do not need to ask individuals' permission to use CCTV, but we make it clear where individuals are being recorded. Security cameras are clearly visible and accompanied by prominent signs explaining that CCTV is in use.

7 Protocols

The surveillance system will be registered with the ICO in line with data protection legislation.

The surveillance system is a closed digital system.

Signs have been placed throughout the premises where the surveillance system is active, as mandated by the ICO's Code of Practice. Signs will be more prominent in areas where surveillance is less expected to be in operation, and when using systems that can capture a large amount of personal data at one time.

The surveillance system has been designed for maximum effectiveness and efficiency; however, the school cannot guarantee that every incident will be detected or covered and 'blind spots' may exist.

Requests by the Police will be processed under Article 6(1) (e). Cameras will be used to monitor activities within TWHF premises, car parks and other public areas to identify criminal activity occurring, anticipated, or perceived, and for the purpose of securing the safety and wellbeing of the school, together with its visitors.

Static cameras will not focus on private homes, gardens and other areas of private property. Staff must not direct cameras at an individual, their property or a specific group of individuals.

Materials or knowledge secured because of CCTV will not be used for any commercial purposes.

Recorded images will never be released to the media for purposes of entertainment.

Only in extreme circumstances should cameras be situated in the toilet or changing areas. Such cameras must not invade personal privacy but rather, capture the entrance/exit, cubicle doors and also was basin areas. Additional signage must be displayed in these areas to inform users that images are being viewed or recorded.

The system will operate 24hrs per day 365 days per year, except for when maintenance down time is required. This will be out of school hours where possible.

Recorded images must only be viewed by people with authorised access.

A site plan of all CCTV cameras must be maintained.

The use of personal mobile phones is strictly prohibited, access must be through work mobile phones using an app provided by IT.

Any complaints about the use of CCTV system should be addressed to the DPO on DPO@twhf.org.uk

8 Security

Access to the surveillance system, software and data will be strictly limited to authorised operators and will be password protected.

- Viewing is restricted and each operator will have their own login.
- The school's authorised CCTV system operators are listed on the DPIA.
- The main control facility is kept secure and locked when not in use.
- The ability to produce copies of CCTV information will be limited to the appropriate staff and only actioned with DPO approval.
- Each camera has an overwrite system that automatically deletes footage after a period of 30 days. Recordings will only be retained if there is a specific purpose for which they are required to be retained for longer.
- Each system will have a visual system that can be run independently of one another.
- The school will not record audio as this is too intrusive into individual rights.
- Where possible CCTV monitors will be located in restricted access areas.
- The Site Manager will check daily to ensure that it works.
- The Site Manager will check the positions of the cameras have not moved.

Requests to view CCTV recordings by individuals will be considered as a **subject access request (see section 10)** and the footage will be viewed by an individual who has access and will view and send to the DPO for consideration on whether it can be shared.

9 Code of Practice

The TWHF understands that recording images of identifiable individuals constitutes processing personal information, and as such, is in line with data protection principals.

- The school notifies all pupils, staff and visitors of the purpose for collecting surveillance data via appropriate signage and privacy notices.
- CCTV cameras are only placed where they do not intrude on anyone's privacy and are necessary to fulfil their purpose.
- All surveillance footage will be kept for 30 days for security purposes.
- The school has a surveillance system for the purpose of the prevention and detection of crime and the promotion of the health, safety and welfare of staff, pupils and visitors.
- The surveillance and CCTV system is owned by the school and images from the system are strictly controlled and monitored by authorised personnel only.
- The school will ensure that the surveillance and CCTV system is used to create a safer environment for staff, pupils and visitors to the school, and to ensure that its operation is consistent with the obligations outlined in data protection legislation. The policy is available from the school's website.

The surveillance and CCTV system will:

- Be designed to take into account its effect on individuals and their privacy and personal data.
- Be transparent and include a contact point which enables people to request information and submit enquiries via the DPO.
- Have clear responsibility and accountability procedures for images and information collected, held and used.
- Have defined policies and procedures in place which are communicated throughout the school.
- Only keep images and information for as long as required.
- Restrict access to retained images and information with clear rules on who can gain access.
- Consider all operational, technical and competency standards, relevant to the surveillance and CCTV system and its purpose, and work to meet and maintain those standards in accordance with the law.
- Be subject to stringent security measures to safeguard against unauthorised access.
- Be regularly reviewed and audited to ensure that policies and standards are maintained.
- Only be used for the purposes for which it is intended.
- The school will ensure that information is included in its privacy notices.

10. Subject Access Requests and Other Rights of Individuals ACCESS

Under the UK GDPR, individuals have the right to obtain confirmation that their personal information is being processed.

Requests by third parties should be submitted to the DPO via DPO@twhf.org.uk who will give close regard to data protection and freedom of information legislation. The rights and freedoms of others will be protected, by asking for their consent or removing specific footage where appropriate.

It is important that access to, and disclosure of, the images recorded by surveillance and CCTV footage is restricted and carefully controlled, not only to ensure that the rights of individuals are preserved, but also to ensure that the chain of evidence remains intact, should the images be required for evidential purposes.

The DPO may release CCTV to the following third parties:

- The police – where the images recorded would assist in a specific criminal inquiry.
- Prosecution agencies – such as the Crown Prosecution Service (CPS).
- Relevant legal representatives – such as lawyers and barristers.
- Persons who have been recorded and whose images have been retained where disclosure is required by virtue of data protection legislation and the Freedom of information Act 2000.

11 Monitoring and Review

This policy will be monitored and reviewed on an annual basis by the DPO.

The DPO will be responsible for monitoring any changes to legislation that may affect this policy and make the appropriate changes accordingly.

The Principal will communicate changes to this policy to all members of staff.

Please see Appendix 2 for further CCTV information

Any enquiries about the CCTV system should be directed to Lyn Rouse DPO@twhf.org.uk

Appendix 1

Personal Data Breach Procedure

The WHF is committed to the protection of all **personal data** and **special category personal data** for which we are the **data controller**.

The law imposes significant fines for failing to lawfully **process** and safeguard **personal data** and failure to comply with this policy may result in those fines being applied.

All members of our **workforce** must comply with this policy when **processing personal data** on our behalf. Any breach of this policy may result in disciplinary or other action.

Reporting Procedure

If you suspect or become aware of CCTV not being used as per this policy, this must be reported to the DPO.

The breach must be reported **on the day of discovery** to the DPO Lyn Rouse by emailing DPO@twhf.org.uk or calling 07719 314166

Further information on SAR's and Reporting a data breach can be found in the Data Protection Policy.

Actions to minimise the impact of data breaches

We will take the actions set out below to mitigate CCTV data breaches.

- Staff must login to CCTV with WHF devices only.
- Permission is sought before sharing CCTV footage with a third party (which is anyone without authorisation).
- All staff keep CCTV access passwords confidential.
- All staff to complete GDPR / Data Protection training.
- All staff to recognise when a breach has occurred and report accordingly.
- All staff to recognise a SAR request and report accordingly.
- Staff with CCTV access must log and report when viewing footage.

The DPO will review the effectiveness of these actions and amend them as necessary after any data breach.

Appendix 2 Further CCTV Information

The CCTV system will operate continuously 24 hours each day of the year. The CCTV is sited at the following educational settings:

Educational Setting	Camera Description	Number of Cameras	Capture sound? Yes or No	Move or Fixed
Devizes	X Vision	70	Some	Fixed
Drove	Hik Vision	33	No	Fixed
Forest & Sandridge		10	No	Fixed
Gaglebrook	Hik Vision	14	No	Fixed
Gorse Hill	Cobra	16	No	Fixed
Grange Infants	Pyrotechnic	4		Fixed
Grange Junior	Hik Vision	9	No	Fixed
Haydon Wick	CSA	9	No	Fixed
JMA	UNVR Avigilon	53	21	Fixed
Moak	Samsung SND-460V	87	No	Fixed and Move
Mountford Manor	Hik Vision	16	No	Fixed
Nyland	IVMS-4200	52	No	Fixed
Ridgeway School	Hik Vision	154	No	Fixed
Rodbourne Cheney	Cobra	14	No	Fixed
Southbroom infants	Kalax	4	No	Fixed
Southwold Primary	Cobra	7	No	Fixed
St Luke's Academy	Honeywell	68	Some	Fixed
St Mary's & All Saints	Geovision	16	No	Fixed
The Croft	Hik Vision	16	No	Fixed
The Manor	Concept Pro Edge	9	No	Fixed
Tregoze	Hi Look	15	No	Fixed
West Kidlington	Hik Vision	6	No	Fixed
Whitelands	Hik Vision	68	No	Fixed
Zouch		6	No	Fixed