Health & Safety Policy
HSP 25
Closed Circuit Television (CCTV)

Key Document details:			
Author:	**David Maine**	Approver:	**Chief Operating Officer**
Reviewer:	**Rachael Lawton & Mark Weller**	Version No.:	**1.5**
Date:	**September 2022**	Next review date:	**September 2024**
Ratified:	**October 2022**		

Record of changes			
Date	**Issue**	**Section**	**Changes**
September 2020	1.4		No changes
September 2022	1.5	2 9	Changes to remote access to CCTV by Site Managers Access to images

Title:	HSP 25 CCTV
Author(s):	David Maine
Date:	September 2022
Review date:	September 2024
Application:	This policy applies equally to all The White Horse Federation (TWHF) employees including agency or casual staff, and to all premises where TWHF is either the 'employer' or is in control of the premises.

Definitions	For the purpose of this policy, the following definitions apply;	
	CCTV	Closed Circuit Television
	DVR	Digital Video Recorders
	ESD	Encrypted Storage Device used to pass on recorded images to a third part. EG Police
Policy Aims	This policy aims to address TWHF's obligations under the General Data Protection Regulations (GDPR) and the Code of Practise provided by the Information Commissioners Office.	
Policy	TWHF is committed to ensuring, so far as is reasonably practicable, the health, safety and welfare of all its employees, and any other class of person who may work on, visit, or use its premises, or who may be affected by its activities or services. To achieve this TWHF uses CCTV in its premises for the purposes of safeguarding and security.	
Risk	Injury or damage to property, assets or persons.	
Responsibility	This responsibility is discharged primarily at the line management/operational level.	

	<u>Roles & Responsibilities</u>
1.	Roles and responsibilities are defined in HSP 2 Organisation. Any specific actions are detailed in the arrangements section below.
	Arrangements
1.	St**atement Of Intent** The CCTV Scheme will be registered with the Information Commissioner under the terms of GDPR and will seek to comply with the requirements both of GDPR and the Commissioner's Code of Practice.

	TWHF will treat the system and all information, documents and recordings obtained and used as data which are protected by GDPR. Cameras will be used to monitor activities within TWHF premises, car parks and other public areas to identify criminal activity actually 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. Unless an immediate response to events is required, staff must not direct cameras at an individual, their property or a specific group of individuals. Materials or knowledge secured as a result of CCTV will not be used for any commercial purpose. Recorded images will never be released to the media for purposes of entertainment. The planning and design has endeavoured to ensure that the scheme 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. Warning signs, as required by the Code of Practice issued by the Information Commissioner will be displayed at all access routes to areas covered by the school's CCTV. Only in extreme circumstance should cameras be situated in toilet or changing areas. Such cameras must not invade personal privacy but rather, capture the entrance/exit, cubicle doors and also wash basin areas. Additional signage must be displayed in these areas to inform users that images are being viewed or recorded.
2.	**Operation of the System** The system will be administered and managed by the Principal or his nominee, in accordance with the principles and objectives expressed in this policy. 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 persons authorised by the Principal. The Principal will keep a record of the authorised persons. Any Covert Surveillance or use of a Covert Human Intelligence Source being considered or planned as part of an operation must comply with TWHF policies and procedures and be authorised by the Principal. A site plan of all the CCTV camera's will be maintained by the Site Manager or WHFIT Support Team member. The Site Manager may access the CCTV during evenings and weekends for security purposes only. The Site manager must access the CCTV through their work mobile phones using an app provided by IT, the use of personal mobile phones is prohibited.

3.	**Equipment** The Site Manager or WHFIT Support Team staff (who will be confirmed locally) will ensure the equipment is working correctly daily including camera operation, clarity of view and effective recording. Responsibility for this maintenance will be confirmed locally. Access to CCTV system monitors should be controlled and must not be viewed by unauthorised staff or visitors. CCTV equipment should be serviced annually by a competent contractor and records of the service should be retained on site.
4.	**Liaison** Ad-hoc meetings may be held with all bodies involved in the support of the system, which may include suppliers, Principals, WHF senior officers and the Police.
5.	**Image Storage Procedures** Recorded images are stored on the DVR. If images are required for evidential purposes, the following procedures for their use and retention must be strictly adhered to: • The images need to be transferred to an Encrypted Storage Device (ESD) which must be sealed witnessed, signed by the Principal or his nominated officer. The ESD will be dated and secured until collected. • Each ESD will be identified by a unique reference number. • The ESD must be new or cleaned of any previous recording. • If the ESD is archived at a later date, the reference number must be noted. • If the Police or a Court requires a copy of the ESD then the Principal or nominated officer will maintain detailed records concerning the data to be released. Recorded images may be viewed by the Police or relevant local authority officers for the prevention and detection of crime, or to prevent anti-social behaviour, with the permission of the Principal or his nominated officer. A record will be maintained of the release of the ESD to the police or other authorised applicants. A register will be available for this purpose. Viewing of ESD's by the Police must be recorded in writing and in the log book. Requests by the Police will be processed under Article 6(1)(e) gives you a lawful basis for processing where: "processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller" Should an ESD be required by the Police as evidence, a copy may be released to the Police under the procedures described above. ESD's will only be released to the police on the clear understanding that the ESD remains the property of the TWHF, and both the ESD and information contained on it are to be treated in accordance with this code. TWHF also retains the right to refuse permission for the Police to pass to any other person the ESD or any part of the information contained thereon. On occasions when a Court requires the release of an original ESD this will be produced from the secure evidence ESD store and placed in a sealed envelope awaiting collection.

	The Police may require TWHF to retain the stored ESD's for possible use as evidence in the future. Such ESD's will be properly indexed and properly and securely stored until they are needed by the Police. Applications received from outside bodies (e.g. solicitors) to view or release ESD's will be referred to the school Principal. In these circumstances ESD's 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. A fee can be charged in such circumstances: £10 for subject access requests; a sum not exceeding the cost of materials in other cases. Subject access requests must be responded to within 30 calendar days. Images will be stored for no more than 30 days and automatically overwritten unless saved for a specific reason under the terms of this policy.
6.	**Breaches of the Code (including breaches of security)** Any breach of the Code of Practice by school staff may be subject to disciplinary action and any instance will be referred to the Principal. Any serious breach of the Code of Practice will be immediately investigated by the Principal and an independent investigation will be carried out to make recommendations on how to remedy the breach.
7.	**Assessment of the Scheme and Code of Practice** Performance monitoring, including random operating checks, may be carried out by the under the direction of the Principal.
8.	**Complaints** Any complaints about the school's CCTV system should be addressed to the Principal. Complaints will be investigated in accordance with Section 6 of this policy.
9.	**Access by the Data Subject** GDPR 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 should be made to the Principal or will be forwarded to the Principal for resolution. CCTV images will only be provided if all parties who are within the CCTV images agree to its release, if redaction/ blurring of the footage isn't possible then stills of the CCTV will be provided to protect individuals rights and freedoms.
10.	**Public Information** Copies of this policy will be available to the public via the website or school office when requested.

11.	**Information Commissioners Office** Further details relating to data protection and CCTV can be found in the Information Commissioners Office Code of Practice for Surveillance Cameras and Personal Information.
12.	**Limitations of this Policy** The policy cannot anticipate all eventualities; therefore professional judgement should be used to identify the appropriate course of action needed to protect those who are vulnerable and/or at risk. This judgement should derive from multi-disciplinary team discussion rather than any one individual where possible.
13.	**Appendices** **None**