HART SCHOOLS TRUST

CCTV POLICY

DOCUMENT PRODUCED BY:	KATE PRINCE
REVIEWED:	TRUST BOARD
LATEST REVIEW	NEW POLICY JANUARY 2023
NEXT REVIEW DATE:	JANUARY 2025

1. POLICY STATEMENT

1.1 This policy applies to all academies in the Hart Schools Trust ('HST Academies')

1.2 HST Academies use Close Circuit Television ("CCTV") within their sites. This policy applies to all members of our Workforce, visitors to the HST Academies' premises and all other persons whose images may be captured by the CCTV system.

1.3 The purpose of this policy is to set out the position of the Trust and leaders in the HST Academies as to the management, operation and use of the CCTV. This policy is an important part of the Trust's obligation as data controller, to define clear procedures to determine how CCTV systems are used and to set out what appropriate measures and records are in place to demonstrate compliance with GDPR.

1.4 This policy takes account of all applicable legislation and guidance, including:

- General Data Protection Regulation ("GDPR");
- CCTV Code of Practice produced by the Information Commissioner;
- Human Rights Act 1998.

1.5 The Harts Schools Trust will also work within a broader framework of legal, procedural and risk based obligations such as:

- obligations under the Freedom of Information Act 2000 (FOIA);
- the Human Rights Act 1998 (HRA); and
- the Surveillance Camera Code of Practice issued under the Protection of Freedoms Act 2012 (PoFA).

2. OPERATION AND ACCESS

2.1 The Hart Schools Trust uses CCTV for the following purposes:

- To provide a safe and secure environment for pupils, staff and visitors;
- To protect the school buildings and assets;
- To assist in reducing the fear of crime and for the protection of private property;
- To assist in the prevention of crime and assist law enforcement agencies in apprehending offenders.

2.2 The system comprises a number of internal and external day and night cameras and does not use any sound recording capability. The CCTV system is owned and operated by each academy and the deployment of it is determined by the Senior Leadership Team on each site. The Data Protection Officer ("DPO") or their representative has overall responsibility as delegated by the Data Controller (Board of Governors).

2.3 Access and viewing is restricted and all authorised operators with access to images will be aware of the procedures they are required to follow and their responsibilities under this policy. HST Academies will follow the '12 Guiding Principles' as listed in Appendix A. All employees will be aware of the restrictions in relation to

access to, and disclosure of, recorded images. The further introduction of, or changes to, CCTV monitoring will be subject to consultation with staff where appropriate

2.4 The ability to view live and historical CCTV data available via network software is only to be provided at designated locations and to authorised persons only. Direct access to recorded data is limited to members of the Site Team at each academy (Caretakers, Estates Manager), the Trust Business Manager, the Pastoral Administrator (Thomas Alleyne Academy only), and the Senior Leadership Team.

2.5 Specific live monitoring of the entrance gate is provided to Reception staff to allow monitoring of visitors to the site for safeguarding purposes.

3. COMPLIANCE

3.1 The Hart Schools Trust will:

- notify the Information Commissioners Office of its use of CCTV as part of the annual data protection registration;
- review this policy should the CCTV system be upgraded or significantly modified
- treat the system and all information processed on the CCTV system as data which is covered by the Data Protection Act/GDPR;
- use cameras to monitor activities within the school grounds to identify potential criminal activity for the purpose of securing the safety and well-being of the school, as well as for monitoring student behaviour;
- display CCTV warning signs which will be clearly and prominently placed at all external entrances of the school sites where CCTV is operational, including the school gates as coverage includes outdoor areas. The school will ensure that there are prominent signs placed at both the entrance of the CCTV zone and within the controlled area which will contain details of the purpose for using CCTV.
- not guarantee that a system will or can cover or detect every single incident taking place in the areas of coverage;
- not use materials or knowledge for any commercial purpose.
- Recorded materials will only be released for use in the investigation of a specific crime and with the written authority of the Police and in accordance with the Data Protection Act/GDPR.

4. SITING CAMERAS

4.1 Cameras will be sited so they only capture images relevant to the purposes for which they are installed (described above) and care will be taken to ensure that reasonable privacy expectations are not violated. For example, cameras will not be placed in areas which are reasonably expected to be private. The school will ensure that the location of equipment is carefully considered to ensure that images captured comply with the Data Protection Act/GDPR requirements.

4.2 Cameras will not be directed outside of the school sites at private property, an individual, their property or a specific group of individuals. The exception to this would be where

an authorisation was obtained for Directed Surveillance to take place, as set out in the Regulation of Investigatory Power Act 2000.

4.3 CCTV is not sited in classrooms and will not be used in such, except in exceptional circumstances.

4.4 Members of staff, on request can access details of CCTV camera location

5. STORAGE AND RETENTION OF CCTV IMAGES

5.1 The Data Protection Act/GDPR does not prescribe any specific minimum or maximum retention periods that apply to all systems or footage. Rather, retention should reflect the organisation's purposes for recording information, which should be informed by the purpose for which the information is collected, and how long it is needed to achieve this purpose. Storage availability is also a factor to be considered in the ability to retain recordings.

5.2 Recorded data will not be retained for longer than is necessary. While retained, the integrity of the recordings will be maintained to ensure their evidential value and to protect the rights of the people whose images have been recorded.

5.3 All retained data will be stored securely.

5.4 Recordings are kept for a minimum of 3 days and up to 31 days. Specific recordings which the school wishes to retain after this time will be logged (see Appendix B).

5.5 An electronic file is held on a secure central server where specific CCTV image/recordings are retained.

6. DISCLOSURE OF IMAGES TO DATA SUBJECTS (SUBJECT ACCESS REQUESTS)

6.1 Any Individual recorded in any CCTV image is a data subject for the purposes of the Data Protection Legislation, and has the right to request access to those images. .

6.2 Any individual who requests access to images of themselves will be considered to have made a subject access request pursuant to the Data Protection Legislation. Such a request should be considered in the context of the School's Subject Access Request Policy.

6.3 All requests should be made in writing to the Head Teacher or Data Protection Officer or their representative. Individuals submitting requests for access will be asked to provide sufficient information to enable the footage relating to them to be identified. For example, date, time and location.

6.4 When such a request is made, the Designated Safeguarding Leader or Trust Business Manager will review the CCTV footage, in accordance with the request. They will inform the Data Protection Officer of the request

6.5 If the footage contains only the individual making the request then the individual may be permitted to view the footage. This must be strictly limited to that footage which contains only images of the individual making the request. Staff who arrange the

viewing of the footage are responsible for taking appropriate measures to ensure that the footage is restricted in this way.

6.6 If the footage contains images of other individuals then staff must consider whether:

- The request requires the disclosure of the images of individuals other than the requester, for example whether the images can be distorted so as not to identify other individuals;
- The other individuals in the footage have consented to the disclosure of the images, or their consent could be obtained;
- or If not, then whether it is otherwise reasonable in the circumstances to disclose those images to the individual making the request.

6.7 Hart Schools Trust reserves the right to refuse access to CCTV footage where this would prejudice the legal rights of other individuals or jeopardise an ongoing investigation.

6.8 A record must be kept (see Appendix B), and held securely, of all disclosures which sets out:

- When the request was made;
- The process followed by HST Academy staff in determining whether the images contained third parties;
- The considerations as to whether to allow access to those images;
- The individuals that were permitted to view the images and when; and
- Whether a copy of the images was provided, and if so to whom, when and in what format.

7. DISCLOSURE OF IMAGES TO THIRD PARTIES

7.1 The School will only disclose recorded CCTV images to third parties where it is permitted to do so in accordance with the Data Protection Legislation.

7.2 Third parties acting behalf of a duty subject will be handled in accordance with the School's Subject Access Request Policy.

7.3 CCTV images will only be disclosed to law enforcement agencies in line with the purposes for which the CCTV system is in place.

7.4 If a request is received form a law enforcement agency for disclosure of CCTV images then HST Academies must follow the same process as above in relation to subject access requests. Detail should be obtained from the law enforcement agency as to exactly what they want the CCTV images for, and any particular individuals of concern. This will then enable proper consideration to be given to what should be disclosed, and the potential disclosure of any third-party images. The information above must be recorded in relation to any disclosure (see Appendix B).

7.5

7.6 If an order is granted by a Court for disclosure of CCTV images then this should be complied with. However, very careful consideration must be given to exactly what the Court order requires. If there are any concerns as to disclosure then the Data Protection Officer should be contacted in the first instance and appropriate legal advice may be required.

8. FURTHER INFORMATION

For further information on CCTV and its use please see below:

- Surveillance camera code of practice Update to Surveillance Camera Code of Practice - GOV.UK (www.gov.uk)
- Biometrics and Surveillance Camera Commissioner website Surveillance Camera Commissioner - GOV.UK (www.gov.uk)
- CCTV Code of Practice (ICO website) Video surveillance (including guidance for organisations using CCTV) | ICO

9. RELATED POLICIES

- HST Data Protection Policy
- Complaints Policy

APPENDIX A

The following 12 guiding principles are taken from the Surveillance camera code of practice Update to Surveillance Camera Code of Practice - GOV.UK (www.gov.uk):

1 Use of a surveillance camera system must always be for a specified purpose which is in pursuit of a legitimate aim and necessary to meet an identified pressing need.
2 The user of a surveillance camera system must take into account its effect on individuals and their privacy, with regular reviews to ensure its use remains justified.
3 There must be as much transparency in the use of a surveillance camera system as possible, including a published contact point for access to information and complaints.
4 There must be clear responsibility and accountability for all surveillance camera system activities including images and information collected, held and used.
5 Clear rules, policies and procedures must be in place before a surveillance camera system is used, and these must be communicated to all who need to comply with them.
6 No more images and information should be stored than that which is strictly required for the stated purpose of a surveillance camera system, and such images and information should be deleted once their purposes have been discharged.
7 Access to retained images and information should be restricted and there must be clearly defined rules on who can gain access and for what purpose such access is granted; the disclosure of images and information should only take place when it is necessary for such a purpose or for law enforcement purposes.
8 Surveillance camera system operators should consider any approved operational, technical and competency standards relevant to a system and its purpose and work to meet and maintain those standards.
9 Surveillance camera system images and information should be subject to appropriate security measures to safeguard against unauthorised access and use.
10 There should be effective review and audit mechanisms to ensure legal requirements, policies and standards are complied with in practice, and regular reports should be published.
11 When the use of a surveillance camera system is in pursuit of a legitimate aim, and there is a pressing need for its use, it should then be used in the most effective way to support public safety and law enforcement with the aim of processing images and information of evidential value.
12 Any information used to support a surveillance camera system which compares against a reference database for matching purposes should be accurate and kept up to date.

APPENDIX B

Hart Schools Trust - Record of CCTV Disclosure			
Senior staff should complete this form when they have received a request to view CCTV footage (subject access request), or when footage has been shared with a third party (e.g. police, court order).			
Details of request			
Academy Name			
Date of request/ disclosure			
Contact details of the person/ organisation requesting footage			
Briefly outline what has been requested - time, place and circumstances			
Member of staff who has reviewed the CCTV footage			
Does the footage contain third parties? Yes [ ] No [ ]			
If yes, please state if this footage can be shared with other parties and the reason for this judgement. Outline any mitigations in place (e.g. obscuring identities)			
Viewing CCTV Footage			
Was the footage viewed by anyone outside of Hart Schools Trust workforce? Yes [ ] No [ ]			
If yes, please include details below			
Name		Date viewed	
Was a copy of the footage provided? Yes [ ] No [ ]			
If yes, please state which format was used			
Form completed by	Name Signature	Date	
Has the DPO been informed?	Yes [ ] No [ ]	Date	