

High Tunstall College of Science



Inspire | Support | Achieve

CCTV Surveillance Policy

Revised	- May 2026
Stakeholder Consulted	- Resources Committee
Review Date	- May 2028
Responsibility for Review	- Senior Teacher – Achievement and Standards/Headteacher/Site Manager

V0.0

Contents:

[Statement of intent](#)

1. **[Updated]** [Legal framework](#)
2. [Definitions](#)
3. **[Updated]** [Roles and responsibilities](#)
4. **[Updated]** [Purpose, justification and transparency](#)
5. **[Updated]** [The data protection principles](#)
6. [Objectives](#)
7. [Protocols](#)
8. **[Updated]** [Security](#)
9. [Data Protection by design and default](#)
10. [Code of practice](#)
11. **[Updated]** [Access](#)
12. **[Updated]** [Monitoring and review](#)
13. [Scenarios for example situations](#)

Statement of intent

At High Tunstall College of Science, we take our responsibility towards the safety of staff, visitors and students very seriously. To that end, we use surveillance cameras to monitor any instances of aggression or physical damage to our college and its members.

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

- We comply with 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 the CCTV surveillance system 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
- Using images of individuals that could affect their privacy.

The surveillance system will be used to:

- Maintain a safe environment
- Ensure the welfare of students, staff and visitors
- Deter criminal acts against persons and property
- Assist the police in identifying persons who have committed an offence.

1. **[Updated]** Legal framework

1.1. This policy has due regard to legislation 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
- Freedom of Information Act 2000
- 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
- **[New]** Human Rights Act 1998
- Children Act 1989
- Children Act 2004
- Equality Act 2010.

1.2. This policy has been created with regard to 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'
- **[New]** DfE (2023) Data protection in schools (Updated 2026)
- **[New]** Biometrics and Surveillance Camera Commissioner 'Surveillance Camera Code of Practice.'

1.3. This policy operates in conjunction with the following college policies:

- Photography and Video Policy
- Freedom of Information Policy
- Data Protection Policy
- Information Security Policy
- Protection of Biometric Information Policy.

For information regarding protection of biometric information please see the college Protection of Biometric Information Policy.

For information regarding protection of right to erasure, rectification or redaction of data please see the college Data Protection Policy.

2. Definitions

- 2.1. For the purpose of this policy a set of definitions will be outlined, in accordance with the surveillance code of conduct:
- **Surveillance** – monitoring the movements and behaviour of individuals; this can include video, audio or live footage
 - For the purpose of this policy only video and audio footage will be applicable
 - **Overt surveillance** – any use of surveillance for which authority does not fall under the Regulation of Investigatory Powers Act 2000
 - **Covert surveillance** – any use of surveillance which is intentionally not shared with the subjects it is recording. Subjects will not be informed of such surveillance.
- 2.2. High Tunstall College of Science does not condone the use of covert surveillance when monitoring the college's staff, students and/or volunteers. Covert surveillance will only be operable in extreme circumstances.
- 2.3. Any overt surveillance footage will be clearly signposted around the college.
- 2.4. **NOTE:** The college does not use any surveillance system that utilises facial recognition, biometric or automated biometric recognition systems.

3. [Updated] Roles and responsibilities

- 3.1. [Updated] The role of the Senior Information Risk Owner (SIRO) supported by the Single Point of Contact (SPOC) includes:
- [New] Considering the appropriate lawful basis to legitimise CCTV use
 - Ensuring that all data controllers at the college handle and process CCTV surveillance system footage in accordance with data protection legislation
 - Ensuring that CCTV surveillance system 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 CCTV surveillance system 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 CCTV surveillance system footage, detailing the purpose of the activity and making these records public upon request

- Informing data subjects of how their data captured in CCTV surveillance system footage will be used by the college, their rights for the data to be destroyed and the measures implemented by the college to protect individuals' personal information
- Preparing reports and management information on the college's level of risk related to data protection and processing performance
- Reporting to the highest management level of the college, e.g. the Governing Body
- Abiding by confidentiality requirements in relation to the duties undertaken while in the role
- Monitoring the performance of the college's data protection impact assessment (DPIA) and providing advice where requested
- Presenting reports regarding data processing at the college to senior leaders and the Governing Body
- **[New]** Meeting with the Site Manager & Senior Duty Site Officer to decide where CCTV is needed, to justify its means and is considered appropriate and proportionate for the college's circumstances
- Conferring with the Site Manager regarding the lawful processing of the CCTV surveillance system footage
- Reviewing the CCTV surveillance system Policy to ensure it is compliant with current legislation
- Monitoring legislation to ensure the college is using surveillance fairly and lawfully
- Communicating any changes to legislation with all members of staff.

3.2. High Tunstall College of Science, as the corporate body, is the data controller. The Governing Body of High Tunstall College of Science therefore has overall responsibility for ensuring that records are maintained, including security and access arrangements in accordance with regulations.

3.3. The Site Manager deals with the day-to-day matters relating to CCTV surveillance system data and thus, for the benefit of this policy will act as the data controller.

3.4. The role of the Data Controller includes:

- Processing CCTV surveillance system footage legally and fairly
- Collecting CCTV surveillance system footage for legitimate reasons and ensuring that it is used accordingly
- Collecting CCTV surveillance system footage that is relevant, adequate and not excessive in relation to the reason for its collection

- Ensuring that any CCTV surveillance system footage identifying an individual is not kept for longer than is necessary
- Protecting footage containing personal data against accidental, unlawful destruction, alteration and disclosure – especially when processing over networks.

3.5. The role of the Compliance Officer (SPOC) includes:

- Dealing with freedom of information requests (FOI), subject access requests (SAR) or a third-party information request (TPIR) in line with legislation, including the Freedom of Information Act 2000.

4. **[Updated]** Purpose, justification and transparency

4.1. **[Updated]** The college will only use surveillance cameras for the safety and security of the college and its staff, students and visitors, and this may include but not be limited to:

- Assisting in emergency situations
- Managing lockdowns
- Supporting the application of internal policies
- Supporting the safeguarding of students & adults
- Providing a sense of security for students and staff.

4.2. **[New]** The college will consider which lawful basis is most appropriate to use. This will be either public task or legitimate interests.

4.3. **[New]** When using legitimate interests as its lawful basis, the college will complete a legitimate interest's assessment.

4.4. Surveillance will be used as a deterrent for violent behaviour and damage to the college.

4.5. The college will only conduct surveillance as a deterrent and under no circumstances will the CCTV surveillance system cameras be present in college classrooms or any changing facility.

4.6. **[New]** If the CCTV surveillance system fulfil the purpose and if it is no longer required, the college will deactivate them and consider less intrusive alternatives.

4.7. **[New]** In its use of CCTV surveillance system, the college will be open and honest towards the college community including the SLT. The college have previously consulted with neighbours, parents and staff, and have explained where the cameras will be, and what the footage will be used for.

5. **[Updated]** The data protection principles

5.1. Data collected from CCTV surveillance system will be:

- **[Updated]** Processed lawfully, fairly and in a transparent manner in relation to individuals as documented by the college in its DPIA that:
 - Describes the nature, scope, context, and purposes of the processing.
 - Assess necessity, proportionality, and compliance measures.
 - Identify and assess risks to individuals.
 - Identify any additional measures to mitigate those risks
- **[New]** If the DPIA reveals any potential security risks or other data protection issues, the college will ensure it has provisions in place to overcome these issues
- Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes;
 - Further processing for archiving purposes in the public interest,
 - Scientific or historical research purposes
 - Statistical purposes shall not be considered to be incompatible with the initial purposes.
- Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed
- Accurate and, where necessary, kept up to date; every reasonable step will be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay
- **[Updated]** Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed as started in section 9 below
- **[Updated]** Processed in a manner that ensures appropriate security of the personal data, as per section 9 below.

6. Objectives

6.1. The CCTV surveillance system will be used to:

- Maintain a safe environment
- Ensure the welfare of students, staff and visitors
- Deter criminal acts against persons and property
- Assist the police in identifying persons who have committed an offence.

7. Protocols

- 7.1. The CCTV surveillance system is registered with the ICO in line with data protection legislation Certificate No. Z6791477.
- 7.2. The CCTV surveillance system is a closed digital system which does not record audio.
- 7.3. Warning signs have been placed throughout the premises where the CCTV surveillance system is active, as mandated by the ICO's Code of Practice.
- 7.4. The CCTV surveillance system has been designed for maximum effectiveness and efficiency; however, the college cannot guarantee that every incident will be detected or covered and 'blind spots' in coverage may exist.
- 7.5. The CCTV surveillance system will not be trained on individuals unless an immediate response to an incident is required.
- 7.6. The CCTV surveillance system will not be trained on private vehicles or property outside the perimeter of the college.

8. **[Updated]** Security

- 8.1. Access to the CCTV surveillance system, software and data will be strictly limited to authorised operators and the system is kept within a lockable room.
- 8.2. **[Updated]** Only employees authorised by the Headteacher may have access to the CCTV surveillance system. The college's authorised CCTV surveillance system operators or those with permission to access are:
 - Operations Manager, Site Manager and Site Officers:
 - Sarah Prestedge
 - Dean Lester
 - Gary Sawyer
 - Stewart Longstaff
 - Allan Robinson.
 - Senior Leadership Team:
 - Mark Tilling
 - Peter Hayward
 - David Pickford
 - **[New]** Nichola Benson
 - John Leary
 - Gareth James
 - Louise Watson
 - Stuart Waites
 - **[New]** Tracey Dodds
 - Andrew Small
 - Emma Watson (SIRO)

- Lindsay Carling.
- Year Leaders:
 - Rachel Harbron
 - Amanda Dunlop
 - Lucy Ewart
 - Jonathan Turner
 - Dan Cook.
- Compliance Officer:
 - Peter Ireland (SPOC).
- Student Support Officers:
 - Kieron Johnson
 - Maxine McQuilling
 - Marie Tate
 - Leanne Harrison
 - **[New]** Stacey Lester
- ICT Staff:
 - Stephen Tingle
 - Mark Rattigan.

- 8.3. A minimum of two (2) members of the above staff must be in attendance when CCTV surveillance system footage is being viewed. Ideally, this should include a member of the Site Team but in exceptional circumstances, when one is unavailable, this can be another authorised individual. It is expected that at least one (1) member of staff using the system should have been trained to do so (except in exceptional circumstances).
- 8.4. Unauthorised staff and students will only have access to view footage in exceptional circumstances that require this to happen, e.g. to identify students or property that might not be identifiable without their help. No images will be allowed to be removed or taken by individuals. In these circumstances, members of the authorised team must be in attendance to supervise the security of this.
- 8.5. In circumstances when no authorised personnel are available, such as on a weekend, the named staff who can be contacted to follow up on any urgent access to the system or for guidance, e.g. due to requests from the Police, are:
- Sarah Prestedge
 - Peter Hayward.
- 8.6. The main control facility is kept secure and locked when not in use.
- 8.7. If, in exceptional circumstances, covert surveillance is planned, or has taken place, copies of the Home Office's [authorisation forms](#) will be completed and retained.
- 8.8. CCTV surveillance system will be tested monthly to ensure they are being properly maintained at all times.

- 8.9. CCTV surveillance system will not be intrusive.
- 8.10. **[Updated]** The Site Manager, Senior Duty Site Officer and Headteacher will decide when to record footage, within the college grounds to deter intruders.
- 8.11. Any unnecessary footage captured will be securely deleted from the college system.
- 8.12. Any cameras that present faults will be repaired immediately as to avoid any risk of a data breach.
- 8.13. Visual display monitors are located in the site office.
- 8.14. **[Updated]** Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

9. **[Updated] Data protection by design and default**

- 9.1. The use of CCTV surveillance system cameras has been critically analysed using a DPIA, in consultation with the DPO.
- 9.2. A review of the Data Protection Impact Assessment (DPIA) has been carried out prior to the installation of any new CCTV surveillance system.
- 9.3. If the DPIA reveals any potential security risks or other data protection issues, the college will ensure they have provisions in place to overcome these issues.
- 9.4. Where the college identifies a high risk to an individual's interests, and it cannot be overcome, the college will consult the DPO before they use CCTV, and the college will act on the DPO's advice.
- 9.5. The college will ensure that the installation of the CCTV surveillance system will always justify its means.
- 9.6. If the use of a CCTV surveillance system is too privacy intrusive, the college will seek alternative provision.
- 9.7. **[New]** The college CCTV system is visual video only no sound is recorded.
- 9.8. **[New]** The college will not use CCTV with live-facial recognition technology.

10. Code of practice

- 10.1. The college understands that recording images of identifiable individuals constitutes as processing personal information, so it is done in line with data protection principles.

- 10.2. The college notifies all students, staff and visitors of the purpose for collecting surveillance data via the privacy notice on the college website.
- 10.3. CCTV cameras are only placed where they do not intrude on anyone's privacy and are necessary to fulfil their purpose.
- 10.4. **[Updated]** The college retains CCTV surveillance footage for fourteen (14) days for security purposes and then overwritten. the Headteacher and the data controller are responsible for keeping the records secure and allowing access. Footage may be held for longer in exceptional circumstances, e.g. if it is required to assist a criminal investigation or safeguarding issue.
- 10.5. The college has a CCTV surveillance system for the purpose of the prevention and detection of crime and the promotion of the health, safety and welfare of staff, students and visitors.
- 10.6. The CCTV surveillance system is owned by the college and images from the system are strictly controlled and monitored by authorised personnel only.
- 10.7. The college will ensure that the CCTV surveillance system is used to create a safer environment for staff, students and visitors to the college, and to ensure that its operation is consistent with the obligations outlined in data protection legislation.
- 10.8. The CCTV surveillance 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, through which people can access information and submit complaints
 - 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 college
 - 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 CCTV surveillance 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, including supporting public safety, the protection of students, staff and volunteers, and law enforcement.

10.9. Be accurate and well maintained to ensure information is up to date.

11. **[Updated]** Access

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

11.2. All disks containing images belong to, and remain the property of, the college.

11.3. **[Updated]** Individuals have the right to submit an SAR to gain access to their personal data in order to verify the lawfulness of the processing. SARs will be handled in accordance with the Subject Access Request (SAR) Policy.

11.4. The college will verify the identity of the person making the request before any information is supplied.

11.5. A copy of the information will be supplied to the individual free of charge; however, the college may impose a 'reasonable fee' to comply with requests for further copies of the same information.

11.6. **[Updated]** Requests by persons outside the college for viewing or copying disks, or obtaining digital recordings, will be assessed by the Headteacher, SIRO, SPOC and DSL who will consult the DPO, on a case-by-case basis with close regard to data protection and freedom of information legislation.

11.7. **[New]** Individuals maintain the right to have personal data erased or restricted under certain conditions, of which the legitimacy test will be applied prior to any action.

11.8. **[Updated]** Where a request is manifestly unfounded, excessive or repetitive, a reasonable fee will be charged or refused and the requestor referred to the ICO.

11.9. All fees will be based on the administrative cost of providing the information.

11.10. All requests will be responded to without delay and at the latest, within one (1) month of receipt.

11.11. In the event of numerous or complex requests, Veritau Ltd (DPO) will be consulted as the period of compliance may be extended by a further two (2) months. The individual will be informed of the outcome and will receive an explanation of why the extension is necessary, within one (1) month of the receipt of the request.

11.12. Where a request is manifestly unfounded or excessive, the college holds the right to refuse to respond to the request. The individual will be informed of this decision and the reasoning behind it, as well as their right to complain to the ICO and to a judicial remedy, within one (1) month of the refusal.

- 11.13. In the event that a large quantity of information is being processed about an individual or it is not clear as to the information being requested, the college will ask the individual to specify the information the request is in relation to.
- 11.14. It is important that access to, and disclosure of, the images recorded by CCTV surveillance system 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.
- 11.15. Releasing the recorded images to third parties will be permitted only in the following limited and prescribed circumstances, and to the extent required or permitted by law:
- 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.
- 11.16. Requests for access or disclosure via a third-party information request (TPIR) will be recorded by the SPOC and the Headteacher will make the final decision as to whether recorded images may be released to persons other than the police.

12. [Updated] Monitoring and review

- 12.1. **[Updated]** This policy will be monitored and reviewed on a biennial basis by the Senior Teacher – Achievement and Standards, Headteacher, Site Manager and the Senior Duty Site Officer.
- 12.2. The Headteacher will be responsible for monitoring any changes to legislation that may affect this policy and make the appropriate changes accordingly.
- 12.3. The Headteacher will communicate changes to this policy to all members of staff.
- 12.4. **[Updated]** The scheduled review date for this policy is May 2028.

13. Scenarios for example situations

- 13.1. The below is designed to give some helpful example situations to guide staff actions and it should be understood that this is not an exhaustive list.
- 13.2. Remember, only authorised members of staff may access the CCTV system. A minimum of two (2) authorised members of staff must be in attendance when CCTV footage is being viewed. Ideally, this should include a member of the

authorised Site Team but in exceptional circumstances, when one is unavailable, this can be another authorised individual.

Example 1: Student says bike has gone missing from the bike shed (or similar situations involving missing property)

- In the first instance this should be referred to the students relevant SSO to follow up (if on a weekend or after college, request that the student/individual contact the relevant SSO, or other staff member appropriate, during college open hours)
- If it is possible to identify the bike (property) without the student observing the CCTV footage, then this would always be the preferable way to follow this up. In situations where the student is needed to help identify the bike (or other lost item), they may do so in the presence of an authorised member of staff (see 8.2) to aid in the investigation
- At no point should any individual be allowed to take an image/photo of what they see on the screen
- If a follow up is needed with a parent, they can be informed that we have an image of any individual involved in an incident but to ask them to refer the matter to the Police who can contact the College to follow up
- For any situation that needs further urgent follow up or questions, staff should contact the identified members of staff to discuss (see 8.5).

Example 2: Designated staff looking at CCTV footage need help identifying individuals from images

- In circumstances where authorised individuals cannot identify individuals from images, the assistance of asking other non-designated staff can be requested to help but this should happen in the presence of authorised staff
- At no point should any individual be allowed to take an image/photo of what they see on the screen.

Example 3: On a weekend or evening, an unauthorised member of staff feels that CCTV footage needs accessing due to a specific situation

- The unauthorised individual should not access the CCTV system
- Where possible, this should be followed up on by authorised staff at an appropriate time (e.g. the following day/after the weekend)
- For any situation that needs further urgent follow up or questions, staff should contact the identified members of staff to discuss (see 8.5).