ALDRIDGE EDUCATION

CCTV POLICY

Document Control Table	
Version no:	**2.0**
Date of last revision:	August 2024
Approval Required By: (Adoption and full 5 Year Review)	**FOC**
Date last approved:	**12th November 2024**
Policy owner:	Director of IT
Frequency of revision:	2 years
Next review date:	November 2026
Revision approval required by:	**FOC**
Policy family:	IT
Policy status:	**Approved**

Applies to (Mark as appropriate)			
Staff	Pupils / Students / Adult Learners	Parents / Carers / Guardians	Contractors
✓			✓
Volunteers	Students on placement	Trustees / LGC / Members	Visitors
✓			
Agency Staff	Other	a	a
✓			

Published Locations					
Trust Website	Academy Website	Aldridge Intranet	Pre-admission documentation	Student/Parent planners	On-request
✓		✓			✓

Consultation (Complete as appropriate in line with master policy document)			
With	Reason for Consultation	Final Consultation Date	Version No

Version History (please note below if a policy has been replaced)					
Version	Reviewer	Revision Date	Nature of Change	Adopted/ Approved by	Approval Date
1		June 2022	Approval		
2	JB	August 2024	Review		
			Sign Off	COO	10/9/24
			Approval	FOC	12/11/24

Contents

1. Purpose of Policy

- 1.1 Our responsibility

  At Aldridge Education, we take our responsibility towards the safety of staff, visitors, and pupils very seriously. The Trust recognises that CCTV systems can be privacy intrusive. For this reason, the Trust has carried out a data protection impact assessment with a view to evaluating whether the CCTV system in place is a necessary and proportionate means of achieving the legitimate objectives set out below. The result of the data protection impact assessment has informed the school's use of CCTV and the contents of this policy. To that end, we use CCTV cameras to monitor any instances of aggression or physical damage to our academies and its members.

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

  - We comply with UK GDPR and all current UK regulations.
  - 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 all UK data protection legislation.

  As a Trust, we have a responsibility to keep students, staff, and others safe.

- 1.2 The CCTV system is used for:
  - Monitoring any criminal activity, assisting with the identification and prosecution of any offences.
  - Monitoring any unwanted visitors as they move through the school grounds.
  - To deter any crime and anti-social behaviour.
  - To identify behavioural and safeguarding issues around the school, helping maintain a safe environment that support the safety and welfare of students, staff, and all other people in our premises.
  - Reduce bullying and improving the school learning environment.
  - Create a safer environment for all students and staff.
  - To protect buildings and assets.

- 1.3 The CCTV system will <u>not</u> be used for:
  - Monitoring any private areas, offices, or classrooms.
  - Monitoring any employee activity like attendance or performance, except to prevent crime and for staff and student safety.
  - Monitoring any private homes, gardens, or any other areas of private properly.
  - Sharing recordings with any external organisation or individual. The only exception will be under the written request and authority from the police, government authority or in the case of a subject access request.
  - The Trust CCTV systems do not include any form of AI-driven monitoring or analysis, such as facial recognition, behavioural analysis, or automated decision-making tools.

- 1.4 We ensure at all times that:
    - We have a clearly defined purpose for installing all CCTV cameras.
    - We have a legal basis for installing CCTV under Article 6 of the UK GDPR.
    - Our use of CCTV is proportionate, so that it will no cause an unlawful and unreasonable intrusion on privacy.
    - All CCTV recordings are kept securely and in line with all current security standards.
    - All CCTV recordings are not kept for any longer than is strictly necessary.
    - All CCTV recordings and use is transparent and in compliance with this policy, our Data Protection and Data retention policies.
    - Review and update the CCTV policy on a regular basis.
    - Clearly communicate the locations of CCTV cameras. We have CCTV signs to inform individuals that the areas are being recorded.
    - Warning signs, as required by the Code of Practice of the Information Commissioner will be clearly visible on the site and make clear who is responsible for the equipment.
    - Not capture footage for one purpose and then use that for another. Only using the CCTV to investigate within the lawful basis on UK GDPR.
    - We conduct or update the data protection impact assessment before deploying CCTV cameras.
- Any CCTV changes go through our Change Request process, so data protection concerns are addressed at the earliest stage of the project adhering to the principle of DP by design and by default.
    - The school will treat the system, all information, documents, and recordings (both those obtained and those subsequently used) as data protected under the Act.
- Materials or knowledge secured as a result of CCTV will not be used for any commercial purpose.
    - Images will only be released to the media for use in the investigation of a specific crime with the written authority of the police. Images will never be released to the media for purposes of entertainment.
    - Where wireless communication takes place between cameras and a receiver, signals shall be encrypted to prevent interception.
- CCTV images are not retained for longer than necessary, taking into account the purposes for which they are processed. Data storage is automatically overwritten by the system after the period set in our data retention policy (can be up to 60 days and will be dependent upon each individual sites CCTV system and storage capacity).
- Recorded images will only be retained long enough for any incident to come to light (e.g., for a theft to be noticed) and the incident to be investigated. However, where there is an ongoing investigation or legal action CCTV images may be saved and kept for the period necessary in discharging a statutory function and in line with the GDPR and the Data Protection Act.

2. Legal Framework

- 2.1 This policy has due regard to legislation including, but not limited to, the following:
    - The Regulation of Investigatory Powers Act 2000
    - The Protection of Freedoms Act 2012
    - The UK General Data Protection Regulation (UK GDPR)
    - The Data Protection Act 2018
    - The 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
    - The School Standards and Framework Act 1998
    - The Children Act 1989
    - The Children Act 2004

- The Equality Act 2010

- 2.2 This policy has been created with regard to the following statutory and non- statutory guidance:
  - Home Office (2021) 'The CCTV Camera Code of Practice'
  - UK GDPR.
  - ICO (2017) 'Preparing for the General Data Protection Regulation (GDPR) 12 steps to take now'
  - ICO (2017) 'In the picture: A data protection code of practice for CCTV cameras and personal information'

- 2.3 This policy operates in conjunction with the following Trust policies including but not limited to:
  - E-safety Policy
  - Freedom of Information Policy
  - Data Protection Policy / GDPR
  - Disciplinarily Policy
  - Safeguarding Policy

3. Roles and Responsibilities

- 3.1 The role of the data protection officer (DPO) includes:
  - Dealing with freedom of information requests and subject access requests (SAR) in line with
  - current UK legislation, including UK GDPR and the Freedom of Information Act 2000.
  - Ensuring that all data controllers handle and process CCTV footage in accordance with data protection legislation.
  - Ensuring that CCTV footage is obtained in line with legal requirements.
  - Ensuring that 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 CCTV footage, detailing the purpose of the activity, and making these records public upon request and in line with all legislation as appropriate.
  - Informing data subjects of how their data captured in CCTV footage will be used by the Trust, their rights for the data to be destroyed and the measures implemented by the Trust to protect individuals' personal information.
  - Preparing reports and management information on the Trust's level of risk related to data protection and processing performance.
  - Reporting to the highest management level of the Trust, e.g., Trust Board.
  - Abiding by confidentiality requirements in relation to the duties undertaken while in the role.
  - Monitoring the performance of the CCTV systems against the Trust's data protection impact assessment (DPIA) and providing advice where requested.
  - Presenting reports regarding data processing to senior leaders and Trust Committees.
  - Ensure that a record of all their processing activities is maintained at all times; The data controllers have an obligation to demonstrate that they have adopted and implemented the technical and organisational measures, enabling them to meet their responsibilities under the UK GDPR.

- 3.2 Aldridge Education as the corporate body, is the data controller.

  - The Trust Board of Aldridge Education therefore has overall responsibility for ensuring that records are maintained, including security and access arrangements in accordance with regulations.

- 3.3 The data controller.
    - The DPO deals with the day-to-day matters relating to data protection 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 footage legally and fairly.
    - Collecting CCTV footage for legitimate reasons and ensuring that it is used accordingly.
    - Collecting CCTV footage that is relevant, adequate, and not excessive in relation to the reason for its collection.
    - Ensuring that any CCTV 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 Director of IT and Lead IT Manager includes:
    - Meeting with the Estates Managers and COO/Principal to decide where CCTV is needed to justify its means.
    - Conferring with the DPO with regard to the lawful processing of the CCTV footage.
    - Reviewing the CCTV Policy to ensure it is compliant with current legislation.
    - Monitoring legislation to ensure the Trust is using CCTV fairly and lawfully.
    - Communicating any changes to legislation with all members of staff.
    - Make sure that the Change Request process has been followed for new cameras and changes to existing systems or configuration.
    - Manage CCTV access, permissions, CCTV operator agreement (Appendix B), security and GDPR documentation has been processed appropriately and it is up to date.
    - Leading and ultimately responsible for the requirement of taking appropriate technical and organisational measures to implement data protection principles and that these are integrated at the planning stage of any data processing operations and managed through the entire CCTV data lifecycle. This is in line with the principle of privacy and security by design and default.

- 3.6 The role of the Director of Estates or Lead Estates Manager includes:
    - Liaise with the IT team, COO/Principal to decide where CCTV is needed to justify its means.
    - Processing the Change Request as necessary for the CCTV system changes and new projects.
    - Work with the IT team on the design, implementation, security, and compliance with safeguarding, GDPR, Information Security, CCTV policy, and other legislation for all CCTV systems.
    - Administration and BAU (Business As Usual) day-to-day operational responsibilities of CCTV systems.
    - Liaising and assisting the IT team (and operationally responsible) for the requirement of taking appropriate technical and organisational measures to implement data protection principles and that these are integrated at the planning stage of any data processing operations and managed through the entire data lifecycle. This is in line with the principle of privacy and security by design and default.

4.Purpose and Justification

- 4.1 The CCTV system is used for:
    - Monitoring any criminal activity, assisting with the identification and prosecution of any offences.
    - Monitoring any unwanted visitors as they move through the school grounds.

- To deter any crime and anti-social behaviour.
- To identify behavioural and safeguarding issues around the school, helping maintain a safe environment that support the safety and welfare of students, staff, and all other people in our premises.
- Reduce bullying and improving the school learning environment.
- Create a safer environment for all students, staff, and visitors.
- To protect buildings and assets.

- 4.2 We manage our purpose and justification through a Data Protection Impact Assessment, included in our ROPA (Recording of Processing Activities). In line with best practices, UK regulations and ICO guidance, we assess the CCTV system and carry out a DPIA when:
  - cameras are added or removed from systems
  - cameras are moved or change position
  - whole or parts of systems are upgraded
  - new systems are installed
  - where systems that include biometrics capabilities such as automatic facial recognition are in use
  - When new CCTV systems have integrated AI technologies by design/default. It is our policy not to integrate AI technologies, such as automatic facial recognition or other biometric capabilities, into our CCTV systems. If any consideration is given to the inclusion of AI in the future, it will be subject to a rigorous consultation, DPIA and a comprehensive review in line with ICO guidance. See ICO guidance: https://www.gov.uk/government/publications/data-protection-impact-assessments-for-surveillance-cameras

- 4.3 We use UK GDPR article 6 for our legal basis for processing to ensure that personal data is processed lawfully, fairly, and transparently. The six legal bases are:
  - Consent
  - Performance of a Contract
  - Legitimate interest
  - Vital Interest
  - Legal Requirement
  - Public interest

5.The Data Protection Principles

- 5.1 Data collected from CCTV will be:
  - Processed lawfully, fairly and in a transparent manner in relation to individuals.
  - Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those 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.
  - 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; personal data may be stored for longer periods, insofar as the personal data will be processed solely for archiving purposes in the public interest. Subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals.
  - 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 and organisational measures.

6.Objectives

- 6.1 The purpose of the CCTV system is to assist the Trust in reaching these objectives:
    - To protect pupils, staff, and visitors against harm to their person and/or property.
    - To identify behavioural and safeguarding issues around the school, helping maintain a safe environment that support the safety and welfare of students, staff, and all other people in our premises.
    - To increase a sense of personal safety and reduce the fear of crime.
    - To protect the school buildings and assets.
    - To support the police in preventing and detecting crime.
    - To deter any crime and anti-social behaviour.
    - To assist in identifying, apprehending, and prosecuting offenders.
    - To assist in establishing cause of accidents and other adverse incidents and prevent reoccurrence
    - Monitoring any unwanted visitors as they move through the school grounds.
    - Reduce bullying and improving the school learning environment.
    - Create a safer environment for all students and staff.

7.Protocols

- 7.1 The CCTV system will be registered with the Information Commissioner (ICO) in line with data protection legislation.

- 7.2 The CCTV system is a closed digital system which does not record audio.

- 7.3 Warning signs have been placed throughout the premises where the CCTV system is active, as mandated by the ICO's Code of Practice and UK GDPR.

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

- 7.5 The CCTV system will not be trained on individuals unless an immediate response to an incident is required.

- 7.6 The CCTV system will not be trained on private vehicles or property outside the perimeter of the academies.

- 7.7 The CCTV system does not incorporate AI technology or automated decision-making processes. The Trust is committed to ensuring that the system does not utilise AI for facial recognition, behavioural analysis, or any other form of automated surveillance.

- 7.8 The CCTV system will follow a Change Management process where we can appropriately manage full compliance against this policy and UK GDPR regulations.

8. Security

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

- 8.2 The Trust's authorised CCTV system operators due to their roles and responsibilities are:
    - Central Trust staff – Exec Team members, Director of IT, DPO, Safeguarding Leads

- Aldridge Schools – SLT, Estates staff, IT staff, DPLs, Safeguarding staff and Pastoral leads.

- 8.3 Footage may be accessed by other users as follows:
    - In discussion with the Academy Principals, Premises/Estates Leads may request access for health and safety purposes
    - With the authorisation of the CEO/COO/CPO/CAO/DPO for specific purposes such as disciplinary investigations, complaint investigations and criminal matters, where there is a lawful reason and in line with UK GDPR

- 8.4. CCTV systems will not be intrusive in exceeding the normal boundaries of school operations.

- 8.5. Any cameras that present faults will be repaired as soon as possible through the agreed maintenance contracts in place.

- 8.6 Downloading Captured Data on to Other Media:
    - In order to maintain and preserve the integrity of the data (and to ensure their admissibility in any legal proceedings) any downloaded media used to record events from the hard drive must be prepared in accordance with the following procedures:
        - Each downloaded media must be identified by a unique mark.
        - Before use, each downloaded media must be cleaned of any previous recording.
        - The CCTV operator will register the date and time of downloaded media insertion, including its reference.
        - Downloaded media required for evidential purposes must be sealed, witnessed, and signed by the CCTV operator, then dated and stored in a separate secure evidence store.
        - If a downloaded media is not copied for the police before it is sealed, a copy may be made at a later date providing that it is then resealed, witnessed, and signed by the CCTV operator, then dated and returned to the evidence store.
        - If downloaded media is archived the reference must be noted.
        - If downloaded media is put onto a device, the device will be encrypted, and password protected.
    - Images may be viewed by the police for the prevention and detection of crime and by Academy / Trust authorised CCTV operators, including but not limited to the principal and other authorised senior leaders. However, where one of these people may be later called as a witness to an offence and where the data content may be used as evidence, it shall be preferable, if possible, for that person to withhold viewing of the data until asked to do so by the police.
    - A record will be maintained of the viewing or release of any downloaded media to the police or other authorised applicants.
    - Should images be required as evidence, a copy may be released to the police under the procedures described in this policy. Images will only be released to the police on the clear understanding that the downloaded media (and any images contained thereon) remains the property of the school and downloaded media (and any images contained thereon) are to be treated in accordance with Data Protection legislation. The school also retains the right to refuse permission for the police to pass the downloaded media (and any images contained thereon) to any other person. On occasions when a Court requires the release of a downloaded media this will be produced from the secure evidence store, complete in its sealed bag.
    - The police may require the school to retain the downloaded media for possible use as evidence in the future. Such downloaded media will be properly indexed and securely stored until they are needed by the police.
    - Applications received from outside bodies (e.g., solicitors or parents) to view or release images will be referred to the Trust's Data Protection Officer and a decision made by a senior leader of the school in consultation with the school's Data Protection Officer. Where CCTV images are authorised to be viewed by outside bodies (excluding the police),

measures will be taken to protect third party data contained within the images, this could include CCTV redaction of the use of redacted CCTV still images.

9. Privacy by Design, Documentation and Maintenance

- 9.1 The use of CCTV cameras and CCTV will be critically analysed using a DPIA, in consultation with the DPO.
- 9.2 A DPIA will be carried out prior to the installation of any CCTV system.
- 9.3 Documentation detailing the location of CCTV cameras, and their coverage area should be kept at each school site by the Estates Lead and be up to date.
- 9.4 The overall technical maintenance of the CCTV system, including software updates, network integrity, and technical troubleshooting, will be the responsibility of the Director of IT and IT Leads. All CCTV systems should have a valid maintenance contract with an appropriate supplier and be appropriately recorded. Non-technical aspects, such as the physical upkeep of the cameras and related infrastructure, will be managed by the Estates team.
- 9.5 If the DPIA reveals any potential security risks or other data protection issues, the Trust will ensure they have provisions in place to overcome these issues.
- 9.6 Where the Trust identifies a high risk to an individual's interests, and it cannot be overcome, the Trust will consult the ICO before they use CCTV, and the Trust will act on the ICO's advice.
- 9.7 The Trust will ensure that the installation of the CCTV systems will always justify its means.
- 9.8 If the use of a CCTV system is too privacy intrusive, exceeding the boundaries of normal school operations, the Trust will seek alternative provision.

10.Code of Practice

- 10.1 The Trust 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 Trust notifies all pupils, staff, and visitors of the purpose for using CCTV data via notice boards, letters, and emails.
- 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 All CCTV footage will be kept for security purposes and in line with our data retention policies; the DPO and the IT department are responsible for keeping the records secure and allowing access as necessary.
- 10.5 The Trust has a CCTV system for the purpose of the prevention and detection of crime, inappropriate behaviour and the promotion of the health, safety and welfare of staff, pupils, and visitors.

- 10.6 The CCTV system is owned by the Trust and images from the system are strictly controlled and monitored by authorised personnel (CCTV operators) only.

- 10.7 The Trust will ensure that the CCTV system is used to create a safer environment for staff, pupils, and visitors to Trust academies, and to ensure that its operation is consistent with the obligations outlined in all data protection legislation. The policy is available from the Trust's website.

- 10.8 The 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, the DPO, 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 Trust.
    - 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 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 pupils, staff and volunteers, and law enforcement.

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

11. Access

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

- 11.2 All storage devices containing images belong to, and remain the property of, the Trust.

- 11.3 Individuals have the right to submit an SAR to gain access to their personal data in order to verify the lawfulness of the processing.

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

- 11.5 Access to the information will be supplied to the individual free of charge; however, the Trust may impose a 'reasonable fee' for the administrative costs of complying with a request if it is manifestly unfounded or excessive, of if further access of their data is requested.

- 11.6 Requests by persons outside the Trust for viewing or copying disks, or obtaining digital recordings, will be assessed by the DPO, on a case-by-case basis with close regard to data protection and freedom of information legislation.

- 11.7 When disclosing CCTV images of individuals, particularly during a subject access request, we need to consider whether the images contain identifying information of any other individuals. In this case we will pixelate, blank out or de-identify, where necessary the images of other individuals.

- 11.8 All requests will be responded to without delay and at the latest, within one month of receipt.

- 11.9 In the event of numerous or complex requests, the period of compliance will be extended by a further two months. The individual will be informed of this extension and will receive an explanation of why the extension is necessary, within one month of the receipt of the request. GDPR Article 12(3)

- 11.10 Where a request is manifestly unfounded or excessive, the Trust 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 month of the refusal.

- 11.11 In the event that a large quantity of information is being processed about an individual, the Trust will ask the individual to specify the information the request is in relation to.

- 11.12 It is important that access to, and disclosure of, the images recorded by 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.

- 11.13 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

- 11.14 Requests for access or disclosure will be recorded and the DPO will make the final decision as to whether recorded images may be released to persons other than the police.

12. Monitoring and Review

- 12.1 This policy will be monitored and reviewed at least every two years by the COO, DPO and Director of IT.

- 12.2 The Director of IT, in conjunction with the DPO, will be responsible for monitoring any changes to legislation that may affect this policy, and make the appropriate changes accordingly.

- 12.3 The IT Leads at each school site will ensure changes to this policy are communicated to all members of staff.

13. Breaches and Complaints

- 13.1 Any breach of the CCTV policy by Trust staff will be investigated in order to take appropriate action. When made aware staff are required to report any breaches.

- 13.2 Any serious breach of the CCTV policy will be immediately investigated, and an independent investigation carried out to make recommendations on how to remedy the breach (by the Trust).

- 13.3 Breaches of the CCTV policy could result in disciplinary action and may, in some cases, be a criminal offence.

- 13.4 Any complaints about the Trust CCTV policy or system should be addressed through the Trust's complaints policy and procedure.

APPENDIX A
TEMPLATE CCTV ACCESS LOG

(CCTV footage must only be accessed / viewed by authorised staff. An accurate log must be kept of all occasions when access was required, this form is for illustration purposes only and operators must use the online form provided for each site for ease of use and access)

Date	Time	Outline reason for access	Footage recorded (Y/N)	Name	Signature

APPENDIX B
CCTV Operator agreement.

As a CCTV operator, I agree to comply with this policy and the following conditions:

- The CCTV operators must be diligent, maintain accuracy and integrity, ensure that confidentiality of all information obtained is within compliance of this policy and in line with all UK data protection and current legislation.
- Operators must only operate the CCTV system within its reasons for deployment and operation, in line with their purpose, and within the remit and all legal basis stated in this policy.
- Operators must manage who can have access to the views and recordings, and what purpose (always in line with this policy and following the correct process). All operators must understand the data protection, information security, privacy rights, and regulations around CCTV access and its management.
- Operators cannot give control to the CCTV software to anyone who is not a CCTV Operator.
- I agree that I am solely responsible for the client software and access to the CCTV assigned to me.
- I agree to ensure that the chain of evidence remains intact, as the footage might be required for evidential purposes.
- I agree to report any security, privacy, safeguarding and GDPR concerns to the IT team or Principal as appropriate.
- I will log all access to the CCTV views, access, and recordings into the CCTV Logs in accordance with this policy. I agree that while using this system I will comply with all the Trust's policies and procedures.

Staff Full Name			
Job Title			
Department			
Agreement Start Date:			
Agreement End Date:			
I take full responsibility for the role. I have read and understood the agreement and this policy and agree to be bound by it, I also agree to notify the Trust in the event that circumstances change.			
SIGNED		DATE	
AUTHORISED BY (Aldridge Education)		DATE	