MALTBYLEARNINGTRUST
Exceptional Experiences. Successful Lives.

Document Title	**MLT Surveillance and CCTV Policy**
Author/Owner (Name and Title)	Leader of ICT and Data Protection
Version Number	V2
Date Approved	15th May 2023
Approved By	Chief Executive Officer

Policy Category (Please Indicate)	**1**	**Trust/Academies to use without amendment**
	2	Academy specific appendices
	3	Academy personalisation required (in highlighted fields)

Summary of Changes from Previous Version

Version	Date	Author	Note/Summary of Revisions
V2	09.05.2023	EPR	Updates to the following areas: - Legal Framework - Definitions - Security

TABLE OF CONTENTS

STATEMENT OF INTENT

Maltby Learning Trust takes 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 Academies and its members.

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

- We comply with the UK GDPR.
- The images that are captured are useable for the purposes we require them for.
- We can 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.
- 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.

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
- 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 (2022) 'Video Surveillance'.

This policy operates in conjunction with the following Trust policies:

- Safe Use of ICT Policy
- Freedom of Information Policy
- Data Protection Policy.

DEFINITIONS

For the purpose of this policy the following definitions are given for the below terms:

- **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 and audio footage will be applicable.
- **Overt surveillance** – Surveillance which is clearly visible and signposted around the Trusts buildings and 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 are not informed of such surveillance.

Maltby Learning Trust does not condone the use of covert surveillance when monitoring the Trust's staff, students and/or volunteers. Covert surveillance will not be used.

- **Biometric data** – Data which is related to the physiological characteristics of a person, which confirm the unique identification of that person, such as fingerprint recognition, facial recognition (FRT), or iris recognition.
- **Automated biometric recognition system** – A system which uses technology to measure an individual's physical or behavioural characteristics by using equipment that operates 'automatically'.
- **Facial recognition** – The process by which a person can be identified or otherwise recognised from a digital facial image. Cameras are used to capture these images and facial recognition technology software produces a biometric template.

ROLES AND RESPONSIBILITIES

The role of the Data Protection Officer and Trust Data Leads include:

- Dealing with Freedom of Information requests (FOIs) and Subject Access Requests (SARs) in line with legislation, including the Freedom of Information Act 2000.
- Ensuring that all Data Controllers within the Trust 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 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 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., the Trust Board.
- Abiding by confidentiality requirements in relation to the duties undertaken while in the role.
- Monitoring the performance of the Trust's Data Protection Impact Assessment (DPIA) and providing advice where requested.
- Presenting reports regarding data processing at the Trust/Academy to Senior Leaders and the Governing Board.

Maltby Learning Trust, as the corporate body, is the Data Controller. The Trust Board therefore has overall responsibility for ensuring that records are maintained, including security and access arrangements in accordance with regulations.

The role of the Data Controller includes:

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

The role of the Trust includes:

- Meeting with the Data Protection Officer to decide where CCTV is needed to justify its means.
- Conferring with the Data Protection Officer with regard to the lawful processing of the surveillance and CCTV footage.
- Reviewing the Surveillance and CCTV Policy to ensure it is compliant with current legislation.
- Monitoring legislation to ensure the Trust is using surveillance fairly and lawfully.
- Communicating any changes to legislation with all members of staff.

PURPOSE AND JUSTIFICATION

The Trust will use the surveillance system for the purpose of the prevention and detection of crime and to provide a safe and secure environment for the safety and welfare of staff, students and visitors.

Surveillance will be used as a deterrent to anti-social behaviour and damage to the Trust buildings and assets. Cameras will not be located in general classrooms for monitoring of students or staff. In certain specialist classrooms such ICT suites cameras may be used for the security of equipment. In other specialist areas, cameras may be used for the safety of students and staff.

If the surveillance and CCTV systems are no longer effective or useful, the Trust will deactivate and remove them.

DATA PROTECTION

Data collected from surveillance and CCTV will be:

- Processed lawfully, lawful processing will be determined by a Legitimate Interests Assessment (LIA).
- Processed fairly, in a manner that people would reasonably expect, and taking into account advancements in technology that may not be anticipated by some people.
- Processed in a transparent manner, meaning that people are informed when their data is being captured.
- Collected for specified and legitimate purposes – data will not be processed further in a manner that is incompatible with the following purposes:

    - Further processing for archiving data in the public interest
    - Scientific or historical research
    - Statistical 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 is inaccurate, having regard to the purposes for which they are processed, is 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 is processed.
- 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.

PROTOCOLS

CCTV signs have been placed throughout the Trusts facilities where the surveillance system is active, as mandated by the ICO's guidance. Warning 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 Trust cannot guarantee that every incident will be detected or covered and 'blind spots' may exist.

The surveillance system will not be used to focus on a particular group or individual unless an immediate response to an incident is required. Cameras will not be located in general classrooms for monitoring of students or staff. In certain specialist classrooms such ICT suites cameras may be used for the security of equipment. In other specialist areas cameras may be used for the safety of students and staff.

The surveillance system will not be trained on private vehicles or property outside the perimeter of the Trusts buildings.

Audio recording will not be used. Where audio capability is a feature included in the cameras this will be disabled.

The Trusts current systems do not feature any automated biometric recognition. They do not have facial recognition capability. No biometric data is recorded by the systems. If and when replacement systems or updates do feature capabilities such as this, it will be disabled and not utilised by the Trust.

SECURITY

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

In exceptional cases where large amounts of information needs to be collected and retained, the Trust will consider using cloud storage. This will be secure and only accessible to authorised individuals.

The Trust's authorised CCTV system operators are:

- Executive Directors of Primary and Secondary Education
- Principal
- Senior Leadership Team
- Trust Facilities and Premises Team
- ICT Support
- PFI Authorised Users.

The main control facility is kept secure and locked when not in use.

Staff will be trained in security procedures, and sanctions will be put in place for those who misuse security system information. Staff will be made aware that they could be committing a criminal offence if they do this.

The ability to produce copies of information will be limited to the appropriate staff.
The system will be tested regularly. Any system or camera faults will be repaired quickly.

CODE OF PRACTICE

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

The Trust notifies all students, staff and visitors of the purpose for collecting surveillance data via privacy notices and signage.

CCTV cameras are only placed where they do not overly intrude on anyone's right to privacy and are necessary to fulfil their purpose.

All surveillance footage will be kept for approximately one month depending on the system. The Trusts authorised CCTV system operators are responsible for keeping the records secure and allowing access.

The Trust has surveillance systems for the purpose of the prevention and detection of crime and the promotion of the health, safety and welfare of staff, students and visitors.

The surveillance and CCTV systems are owned by the Trust and images from the system are strictly controlled and monitored by authorised personnel only. On some Trust sites there may be separate systems owned and operated by the PFI partner.

The Trust will ensure that the surveillance and CCTV systems are used to create a safer environment for staff, students and visitors to the Trust/Academy, and to ensure that their operation is consistent with the obligations outlined in data protection legislation.

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 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 across 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 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, including supporting public safety, the protection of pupils, staff and volunteers, and law enforcement.
- Be accurate and well maintained to ensure information is up-to-date.

ACCESS

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

All disks and hard drives containing images belong to and remain the property of the Trust. Individuals have the right to submit a SAR to gain access to their personal data in order to verify the lawfulness of the processing.

The Trust will verify the identity of the person making the request before any information is supplied. If it is possible to fulfil the request, a copy of the information will be supplied to the individual free of charge; however, the Trust may impose a 'reasonable fee' to comply with requests for further copies of the same information. The individual will either be provided with a permanent copy of the information or allowed to view the information.

Requests by persons outside the Trust for viewing or copying disks, or obtaining digital recordings, will be assessed by the Chief Executive Officer/Principal, who will consult the Data Protection Officer, on a case-by-case basis with close regard to data protection and freedom of information legislation.

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

All requests will be responded to without delay and where possible, within one month of receipt. In the event of numerous or complex requests, the period of compliance may be extended by up to an additional 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.

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.

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.

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.

Where data requests contain the personal data of a separate individual/s, the rights and freedoms of others will be protected by asking for their consent or removing specific footage where appropriate. Where this is not possible or practical the request may be refused.

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.

Requests for access or disclosure will be recorded and the Data Protection Officer/Principal will make the final decision as to whether recorded images may be released to persons other than the police.

MONITORING AND REVIEW

This policy will be monitored and reviewed on a biennial basis by the Data Protection Officer and the Trust Data Lead.

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

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