MLT CCTV Policy

Date Last Reviewed:	September 2016
Reviewed by:	ICT Team Leader
Approved by:	CEO
Next Review Due:	September 2018

Maltby Learning Trust

Assurance Statement

This policy aims to ensure that the use of CCTV adheres to the principles of the Data Protection Act 1998, Human Rights Act 1998, Regulation of Investigatory Powers Act 2000 and other relevant legislation.

1. INTRODUCTION

Maltby Learning Trust places the health, safety and welfare of its students, staff and visitors high amongst its priorities and will ensure it maintains a safe and secure environment throughout the Trust. Close Circuit TV is now used within the Trust with the express intention of providing a safe environment. CCTV can only be operated and used safely within a stringent framework encompassing legal and regulatory requirements.

2. PURPOSE

The purpose of this policy is to ensure:

1. That the use of CCTV adheres to the principles of the Data Protection Act 1998, the Human Rights act 1998, the Regulation of Investigatory Powers Act 2000 and other relevant legislation.
2. That any CCTV system is not abused or misused.
3. That CCTV is correctly and efficiently installed and operated.

3. SCOPE

The policy is binding on all employees of the Trust and applies to all other persons who may, from time to time, be present on Trust premises.

4. LEGAL FRAMEWORK AND REQUIREMENTS

Article 8 of the Human Rights Act 1998 protects the right to respect for private and family life. No public Authority may interfere with this right except when in accordance with the law and when necessary. Any interference must be proportional to the threat or risk to community safety, comply with all relevant legal requirements, be necessary for safety and the prevention and detection of crime and cause the minimum of interference to the individual. The use of CCTV must therefore be open to scrutiny and be fully documented.

The Trust must be able to demonstrate that it complies with the Data Protection principles which state that data must be:

1. Fairly and lawfully processed

2. Processed for limited purposes and not in any manner incompatible with those purposes

3. Adequate, relevant and not excessive

4. Accurate

5. Not kept for longer than is necessary

6. Processed in accordance with individual's rights

7. Secure

8. Not transferred to countries without adequate protection

The Information Commissioner has the power to issue Enforcement Notices where he/she considers there has been a breach of one or more of the Data Protection principles.

The Information Commissioner has issued a CCTV Code of Practice and the Trust is required to comply with the guidelines within that document.

5. PURPOSE OF THE CAMERAS

The positioning of cameras has been based upon a security assessment of the site and buildings to identify likely areas of concern. The survey identified the following areas of concern:

- Approaches to Trust buildings;
- Gate and door entry systems;
- Corridors and circulation areas;
- Breakout and dining spaces;
- Approaches to toilets;
- A number of fire exit doors

6. OWNERSHIP AND OPERATION OF CCTV

All CCTV systems in buildings solely occupied by the Trust are owned and operated by the Trust. All cameras monitors and data collection and retention processes are maintained operationally by named individual staff for each site. Maintenance is also provided by third party organisations under separate maintenance contracts in accordance with this policy.

The following staff at the Trust have responsibility for governing and having access to the CCTV System. They are required to sign the CCTV Use and Disclosure of Images Protocol at Appendix 1:

- Executive Principal MLT;
- Principal;
- Assistant Principal;
- Director Business & Finance;
- Office Manager;
- ICT Team Leader;
- ICT Technician;
- Premises/Facilities Manager;

- Site Manager.

7. PRINCIPLES

All schemes will be monitored and managed using the following procedures and must be formally approved (as above) prior to any installation.

The Trust will assess the appropriateness of and reasons for, using CCTV or similar surveillance equipment.

- The person(s) or organisation(s) who are responsible for ensuring the day-to-day compliance with the operational requirements of such schemes and this policy will be documented.
- The CCTV system will have an accountable 'Scheme Manager' who is responsible on a day-to-day basis for the appropriateness of its use.
- All maintenance or servicing of CCTV equipment must be recorded.
- All CCTV images if recorded must be retained for a minimum of 31 days and then erased permanently.
- The Code of Practice requires that signs are placed across the site so that everyone is aware that CCTV is in operation. The signs need to contain the following information:
    - Identity of the organisation responsible for the scheme
    - The purposes of the scheme
    - Details of who to contact regarding the scheme
    - The equipment should be sited in such a way that it only monitors the spaces which are intended to be covered by the equipment.
    - It is important that the images produced by the equipment are as clear as possible in order that they are effective for the purposes for which they are intended.

8. COVERT CCTV SURVEILLANCE

Under the Regulation of Investigatory Powers Act 2000, covert or directed surveillance can only be carried out with the permission of the Executive Principal or under instruction from the police. Covert surveillance should be strictly targeted at obtaining evidence where there are grounds for suspecting criminal activity and that notifying the individual about the monitoring would prejudice its prevention or detection. Covert surveillance must not continue when an investigation is complete. Cameras should not be placed in areas which would reasonably be expected to be private (e.g. toilets).

9. VIEWING IMAGES

Access to images is restricted to staff that need to have access in order to achieve the purpose of using the equipment.

All access to records must be documented on a Viewing of CCTV Images form (Appendix 2)

Under Data Protection legislation, the data subject can request access to recorded images. However, the Information Commissioner has issued guidance that says there is no need "to give individual's access to those images that are just general scenes neither focusing on a particular individual nor being used to learn information about individuals"

The police may request access to images if they are investigating an incident which may result in a request for a permanent copy of the images. If a permanent copy of the images is released to the police or the data subject it must be recorded on the form Image Provision to a Third Party (Appendix 3)

Appendix 2 and 3 forms should be securely stored for a minimum of 3 complete years if it is a subject access request, or 5 years if it will result in litigation.

9. COMPLAINTS

Grievances and complaints regarding the operation of the Academy's CCTV system should be processed through the Trust's complaints procedure.

APPENDIX 1 – USE AND DISCLOSURE OF IMAGES PROTOCOL

There are legitimate public concerns that exist around the use of CCTV. There are numerous guidelines that are designed to satisfy the community that the use of cameras is subject to adequate supervision and scrutiny. It is therefore important that public confidence is maintained by fully respecting and individual's privacy.

All employees that are authorised to view the CCTV images within the Trust must read this policy and confirm that they accept and agree to the terms below:

1. CCTV images may only be viewed by authorised employees or the Police;
2. All authorised employees viewing the CCTV images will act with the utmost probity at all times;
3. All images viewed by authorised employees must be treated as confidential;
4. All authorised employees are to ensure that whilst viewing CCTV images, unauthorised employees or visitors cannot view the images;
5. All authorised employees are responsible to ensure that CCTV images are not left on any screen without an authorised employee being left in charge. An authorised employee should log out of the programme when leaving the screen unattended;
6. Every viewing of the images will accord with the purposes and key objectives of the CCTV system and comply with the CCTV Policy;
7. All authorised employees viewing CCTV images should be aware of exercising prejudices, which may lead to complaints of the system being used for purposes other than those for which it is intended. The viewers may be required to justify their interest in any particular individual, group of individuals or property at any time;
8. All authorised employees viewing CCTV images are responsible for their every viewing of the images, which must be justifiable;
9. Any breach of the CCTV Policy or CCTV Protocol will be dealt with in accordance with existing discipline regulations. Individuals must recognise that any such breach may amount to gross misconduct, which could lead to a dismissal;
10. Any breach of the Data Protection Act 1988 will be dealt with in accordance with the legislation. All authorised employees viewing CCTV images must be aware of their liability under this act.

I understand and agree to abide by the CCTV Policy and the CCTV Protocol

Name……

Signature……

Date……

APPENDIX 2 - VIEWING OF CCTV IMAGES

Date of Viewing	Time	CD identifier	Operator

Reason for viewing
Outcome if any

Name(s) of person viewing	Organisation details

Date of Incident		Description	Outcome
Time of Incident			
Camera identifier			
Operator			

APPENDIX 3 - IMAGE PROVISION TO A THIRD PARTY

Original to be provided, copy to be retained Yes/No		**Copy to be provided, original to be retained Yes/No**	
Reason for Provision		**Legal Proceedings / Subject Access / Other**	
Date of Creation	**Time of Creation**	**Operator**	**Tape/CD Identifier**
Crime / Incident no / Reason for Access			
Police Officer / Third Party name			
Police Station / Third Party Address			
Telephone number		**Date of Handover**	
Signature			
Date of destruction / return	**Method of Destruction**	**Operator**	