CCTV Policy

Document Control Information

CCTV Policy, Issue 2 – August 2017

Review Period	**Review Committee**
Every 2 years	Trustees

Revision History

Author	Summary of changes	Issue	Date Authorised
R Righini	New policy extracted section from data protection policy	1	31st August 2017

Authorisation

Approved By:	**This policy was approved by the Trustees**
Date Approved:	**31st August 2017**
Date of Next review:	**31st August 2019**
Document Owner & Reviewer:	The senior manager responsible for this policy is the Operations Director

Equality Impact

Statement	**We welcome feedback on this document and the way it operates. We are interested to know of any possible or actual adverse impact that may affect any groups in respect of any of the Equality Act 2010 protected characteristics.** **The person responsible for equality impact assessment for this document is the Director of Equality and Diversity.**
Screening	**This document has been screened by the Equality Team and the impact has been assessed as:** ☐ **Not applicable** ☐ **Low** ☐ **Medium** ☐ **High**

1. Purpose

1.1. The purpose of this policy is to regulate the management, operation and use of the Closed Circuit Television (CCTV) system across the New Bridge Multi Academy Trust (MAT). Due regard is paid to the CCTV Code of Practice, Data Protection Act 1998, the Human Rights Act 1998 and the Regulation of Investigatory Powers Act 2000.

2. Scope of Policy

2.1. This policy applies to all staff, particularly those who are involved in CCTV recording.

3. Reason for Review

3.1. This policy was reviewed as part of a MAT policy audit. The review also acknowledges the significant changes that will take place in May 2018 for all schools.

4. Aim(s)

4.1. The aims of the CCTV scheme are:

4.1.1. to increase the personal safety of staff, pupils and visitors.

4.1.2. to protect the MAT buildings and their assets.

4.1.3. to assist in identifying, apprehending and prosecuting offenders.

4.1.4. to protect members of the public and private property.

4.1.5. to assist in managing the MAT.

5. Procedures and practice

5.1. The CCTV System

5.1.1. Within the MAT:

5.1.1.1. **New Bridge School** has one CCTV system with 5 live monitoring stations set up for viewing only and a central control unit, located in the reception office. Footage or images can be downloaded by authorised staff who have network access to CCTV from their desktops. The CCTV system operates 24 hours each day, every day of the year. The system has a 30 day cycle. Cameras are used to monitor areas within the school building and the outside area around the front of the building.

5.1.1.2. **Hollinwood Academy:** has no CCTV.

5.1.1.3. **Spring Brook Academy**: has no CCTV.

5.2. Legal Obligations

5.2.1. Our CCTV systems are registered with the Information Commissioner under the terms of the Data Protection Act 1998 and as a MAT we will comply with the requirements both of the Data Protection Act and the Commissioner's Code of Practice.

5.2.2. The MAT will treat CCTV systems and all information, documents and recordings obtained and used as data which is protected by the Data Protection Act.

5.2.3. Notification of CCTV Recording, as required by the CCTV Code of Practice, is placed at all access routes to the school grounds and at each entrance to the building where CCTV is in operation. This ensures people entering areas across the MAT are aware that CCTV surveillance is in place.

5.3. **Operation of the system**

5.3.1. The scheme is overseen, administered and managed by the MAT Controller.

5.3.2. The day-to-day management of CCTV systems will be the responsibility of the ICT Team with support from the Data Protection Manager and the CEO.

5.3.3. All operating equipment will be checked daily to ensure it is working correctly, i.e. date /time stamp is correct.

5.3.4. Requests for any recordings must be made via the Data Protection Manager, Rita Righini. These recordings will be made available only with authorisation from named staff with key responsibility for CCTV.

5.3.5. Recordings will be made available, on request, to law enforcement agencies involved in the prevention and detection of crime and no other third parties.

5.3.6. Any recordings and/or images copied from CCTV footage will be password protected.

5.4. **Staff with Key Responsibility**

5.4.1. Access to recorded footage or images is limited to named staff and will only be disclosed to others with their authorisation. Named staff are:

Graham Quinn, CEO
Rita Righini, Data Protection Manager

5.4.2. The above staff have responsibility for following set procedures when recording, storing, viewing, retrieving and deleting images from the CCTV system. They will ensure:

5.4.2.1. the MAT maintains adequate and comprehensive records relating to the management of the system and incidents.
5.4.2.2. monitors are correctly sited taking into account the images that are displayed.
5.4.2.3. the monitor viewing areas are appropriate and secure.
5.4.2.4. viewing of live images on monitors is restricted to operators.
5.4.2.5. recorded images are viewed in the ICT Technicians' room, a locked room only accessible to authorised staff.
5.4.2.6. the monitoring or viewing of images from areas where an individual would have an expectation of privacy is restricted to authorised persons.
5.4.2.7. recordings are used appropriately, in accordance with Data Protection Rules and the CCTV Code of Practice.

5.4.2.8. footage/images taken from CCTV will only be used for clearly defined and specific purposes

5.4.2.9. footage or images taken from CCTV are securely stored in the ICT Technicians' Office in a limited access folder, only accessible to authorised staff.

5.4.2.10. footage is deleted off the network once it has been used for the specific purpose the recording was taken for.

5.4.2.11. any footage or images copied onto CD or other storage media are securely stored in the ICT Technicians' office.

5.4.2.12. the Image Retention Guidelines are followed. Images are kept for no longer than strictly necessary, they are only retained to meet the purposes for recording them e.g. serious incidents, images will be retained until the situation is fully resolved. Images may be passed to the police in some cases. Images required for evidence will be recorded witnessed and packaged before copies are released to the police.

5.4.2.13. where copies of images are disclosed, they are safely delivered to the intended recipient by an authorised, named member of staff. Records of disclosures are recorded; the disclosure records are stored securely in the ICT Technicians' room.

5.4.2.14. measures are in place to ensure the permanent deletion of images through secure methods at the end of the retention period by incineration.

5.4.2.15. staff are fully aware of the security procedures relating to the use of CCTV.

5.4.2.16. staff are aware that they could be committing a criminal offence if they misuse CCTV images.

5.5. **Staff Training**

5.5.1. Staff using the CCTV system receive appropriate training to ensure they are able to comply with the CCTV Code of Practice (revised edition 2008) published by the Information Commissioner and are fully aware of the Data Protection Rules.

5.6. **Breaches of the Policy (including breaches of security)**

5.6.1. Any breach of the policy by staff will be initially investigated by the CEO to determine disciplinary action, if necessary, and to make recommendations on how to remedy the breach.

5.7. **Assessment of the CCTV System**

5.7.1. An annual assessment will be undertaken by the CEO to evaluate the effectiveness of the CCTV system. The outcome of the assessment will be reported to a meeting of the Trustees who will determine if the system is achieving the objectives of the scheme, or if the system requires modification.

5.8. **Complaints**

5.8.1. Any complaints about the MAT's CCTV system should firstly be made, in writing, to the CEO. All complaints will be fully investigated.

5.9. **Access by the Data Subject**

5.9.1. The Data Protection Act provides Data Subjects (individuals to whom 'personal data' relates) with a right to data held about themselves, including those obtained by CCTV.

5.9.2. If the individual is not the focus of the footage i.e. they have not been singled out or had their movements tracked then the images are not classed as 'personal data' and the individual is not entitled to the image under the provisions of Subject Access.

6. Sources and references

6.1. Data Protection Act 1998
6.2. Equality Act 20107
6.3. Human Rights Act 1998
6.4. Regulation of Investigatory Powers Act 2000
6.5. Data Protection: CCTV Code of Practice. Revised edition 2008

7. Other useful documents

7.1. Subject Access Request Policy
7.2. Freedom of Information Policy
7.3. Equality Impact Scheme
7.4. Publication Scheme
7.5. Complaints Policy

8. Monitoring

8.1. This policy will be monitored through the MAT's accountability framework.