



inspiring the journey for
independence together

CCTV Policy

Non-Statutory

Reviewed Two Yearly

Signed:  (Chair of the Trust)

Date: October 2023

Review Date: October 2025

1. Introduction

The purpose of this policy is to regulate the use of the CCTV system and its associated technology in the monitoring of both the internal and external environments of all schools across the Rivermead Inclusive Trust (hereafter referred to as the RIT). CCTVs are installed internally and externally in the premises for the purpose of enhancing security of the building and its associated equipment as well as creating a mindfulness among the occupants, as well as keeping all staff and learners safe. At any one time a surveillance security system is in operation within and/or in the external environments of the premises during both the daylight and night hours each day. This policy applies to all personnel, and relates directly to the location and use of CCTV, the monitoring, recording and subsequent use of recorded materials. The system comprises a variety of cameras located around the school sites. All cameras are monitored from a Central Control Room and are only available to selected staff (e.g. SLT, Network Manager, Facilities Manager). This Code follows Data Protection Act guidelines. The Code of Practice will be subject to review bi-annually to include consultation as appropriate with interested parties. The CCTV system is owned by each individual school under the RIT.

2. Objectives of the CCTV scheme

There MUST be clear, visible and readable signs across the site, confirming that CCTV is in operation across the site. This contains details of the purpose of the surveillance and who to contact about the scheme.

2.1 Purpose of CCTV

- To protect the school buildings and their assets.
- Increase personal safety and reduce the fear of crime.
- To support the Police in a bid to deter and detect crime.
- To assist in identifying, apprehending and prosecuting offenders.
- To protect members of the public and private property.
- To assist in managing the school.
- To keep all staff and learners across the site safe.
- To be part of any allegation when staff are involved and the police or an internal investigation requires to be undertaken.

2.2 Misuse of CCTV

The CCTV must only be used for appropriate reasons, any misuse of the CCTV system across the RIT may result in disciplinary action. The misuse of the CCTV system includes but may not be limited to:

- Checking the location of staff (unless in an emergency situation).
- Checking staff entering and exiting the school site.
- Using the CCTV system for personal use.
- Must NOT be used to violate privacy.

3. Statement of Intent

The CCTV Scheme will be registered with the Information Commissioner under the terms of the Data Protection Act 1998 and will seek to comply with the requirements both of the Data Protection Act and the Commissioner's Code of Practice. The RIT will treat the system and all information, documents and recordings obtained and used as data which are protected by the Act. Cameras will be used to monitor activities within the RIT and its car parks and other public areas to identify criminal activity actually occurring, anticipated, or perceived, and for the purpose of securing the safety and wellbeing of the school, Staff, Learners and together with its visitors. Staff have been instructed that cameras are not to focus on private homes, gardens and other areas of private property. Unless an immediate response to events is required, staff must not direct cameras at an individual, their property or a specific group of individuals, without an authorisation being obtained using the RIT'S forms for Directed Surveillance to take place, as set out in the Regulation of Investigatory Power Act 2000. Materials or knowledge secured as a result of CCTV will not be used for any commercial purpose. Data will only be released to the media for use in the investigation of a specific crime and with the written authority of the police. **Data will never be released to the media for purposes of entertainment.**

The planning and design has endeavoured to ensure that the Scheme will give maximum effectiveness and efficiency but it is not possible to guarantee that the system will cover or detect every single incident taking place in the areas of coverage. Warning signs, as required by the Code of Practice of the Information Commissioner have been placed at all access routes to areas covered by the RIT CCTV. Monitoring for security purposes will be conducted in a professional, ethical and legal manner and any diversion of the use of CCTV security technologies and personnel for other purposes is prohibited e.g. monitoring of political or religious activities, or employee and/or pupil evaluations that would undermine the acceptability of the resources for use regarding critical safety and security objectives. CCTV monitoring of public areas, for security purposes, will be conducted in a manner consistent with all existing policies adopted by the school including Discrimination, Bullying and Harassment, Sexual Harassment etc.

The code of practice for digital monitoring prohibits monitoring based on the characteristic and classification contained in Equality and other related legislation, for example race, gender, sexual orientation, national origin, disability etc. The system is in place to monitor

suspicious behaviour and not individual characteristics. Digital monitoring of public areas, for security purposes is limited to uses that do not violate the reasonable expectation of privacy as defined by Law. The Head of the school or special provision will approve the temporary cameras to be used during special events that have particular security requirements and ensure their withdrawal following such events. (Temporary cameras does not include mobile video equipment or hidden surveillance cameras used for criminal investigations) Consideration will be given to both staff and pupils regarding possible invasions of privacy and confidentiality due to the location of a particular CCTV camera or associated equipment. The Head teacher will ensure that all areas being monitored are not in breach of an enhanced expectation of the privacy of individuals within the school and be mindful that no such infringement is likely to take place. The camera control will be monitored to ensure it is not in breach of the intrusion on intimate behaviour by persons in public changing and toilet areas. When a zoom facility on a camera is being used, a second person will be present with the camera operator to guarantee that there is no unwarranted invasion of privacy

4. Operation of the System

The Scheme will be administered and managed by the Executive Head, Head teacher or head of specialist provision, in accordance with the principles and objectives expressed in the code. The day-to-day management will be the responsibility of both the Senior Management Team, Trust IT Lead and the Network Manager during the day and out of hours and at weekends. The Control Room if they have one will only be staffed by Trust IT Lead, Network Manager or Facilities Manager. The CCTV system will be operational 24 hours each day, every day of the year.

5. Control Room (Main school office)

Access to the CCTV Control Room will be strictly limited to the SLT, Trust IT Lead, Network Manager, Admin Staff and the Facilities Manager. Unless an immediate response to events is required, staff in the CCTV Control Room must not direct cameras at an individual or a specific group of individuals. Visitors and other contractors wishing to enter the Control Room will be subject to particular arrangement as outlined below. Control Room Operators must satisfy themselves over the identity of any other visitors to the Control Room and the purpose of the visit. Where any doubt exists access will be refused. Details of all visits and visitors will be endorsed in the visitor signing in book.

The system may generate a certain amount of interest. It is vital that operations are managed with the minimum of disruption. Casual visits will not be permitted. Visitors must first obtain permission from the Head teacher, or his/her deputy and must be accompanied

by them throughout the visit. Any visit may be immediately curtailed if prevailing operational requirements make this necessary. If out of hours' emergency maintenance arises, the Control Room Operators must be satisfied of the identity and purpose of contractors before allowing entry. A visitor's book will be maintained in the RIT. Full details of visitors including time/data of entry and exit will be recorded. There must always be at least one Control Room Operator present within the Control Room out of hours and weekends OR the Control Room must be locked. During the working day when not manned the room must be kept secured. Other administrative functions will include maintaining digital Data and hard disc space, filing and maintaining occurrence and system maintenance logs. Emergency procedures will be used in appropriate cases to call the Emergency Services.

6. Liaison

Liaison meetings may be held with all bodies involved in the support of the system.

7. Monitoring Procedures

Camera surveillance is maintained at all times. A monitor is installed in the Control Room or main office to which pictures will be continuously recorded.

8. Recording Procedures

In order to maintain and preserve the integrity of the Data used to record events from the hard drive and the facility to use them in any future proceedings, the following procedures for their use and retention must be strictly adhered to:

- Recordings MUST be kept for at least 30 days
- If recordings are recorded to a DVD they must be identified by a unique mark. - . -
The controller shall register the date and time of DVD insert, including DVD reference. A DVD required for evidential purposes must be sealed, witnessed, signed by the controller, dated and stored in a separate, secure location as in the school safe. If a DVD 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, signed by the controller, dated and returned to the evidence DVD store. If the DVD is archived the reference must be noted.

- Data may be viewed by the Police for the prevention and detection of crime. A record will be maintained of the release of Data to the Police or other authorised applicants. A register will be available for this purpose. Viewing of Data by the Police must be recorded in writing and in the log book. Requests by the Police can only be actioned under section 29 of the Data Protection Act 1998. Should a copy of the recording be required as evidence, a copy may be released to the Police under the procedures described previously in this Code. Data will only be released to the Police on the clear understanding that the DVD remains the property of the RIT, and both the DVD and information contained on it are to be treated in accordance with this code.

The Police may require the RIT to retain the stored Data for possible use as evidence in the future. Such data will be properly indexed and properly and securely stored until they are needed by the Police. Applications received from outside bodies (e.g. solicitors) to view or release data will be referred to the Head teacher. In these circumstances data will normally be released where satisfactory documentary evidence is produced showing that they are required for legal proceedings, a subject access request, or in response to a Court Order.

9. Breaches of the code (including breaches of security)

Any breach of the Code of Practice by RIT staff will be initially investigated by the Head teacher, in order for him/her to take the appropriate disciplinary action. Any serious breach of the Code of Practice will be immediately investigated and an independent investigation carried out to make recommendations on how to remedy the breach. Information obtained in violation of this policy may not be used in a disciplinary proceeding against an employee of the RIT, or a pupil

10. Assessment of the scheme and code of practice

Performance monitoring, including random operating checks, may be carried out by the Trust IT Lead and or Network Manager.

11. Complaints

Any complaints about the school's CCTV system should be addressed to the Executive Head / Head teacher or Head of School. Complaints will be investigated in accordance with Section 9 of this Code.

12. Access by the Data Subject

The Data Protection Act provides Data Subjects (individuals to whom "personal data" relate) with a right to data held about themselves, including those obtained by CCTV. Requests for Data Subject Access should be made on an application form available from the Head teacher.

13. Public information

Copies of this Code of Practice will be available to the public from the School Office and the Head teacher.

Summary of Key Points

- This Code of Practice will be reviewed every two years.
- The CCTV system is owned and operated by the school.
- The Control room will not be manned out of school hours.
- The Control Room is not open to visitors except by prior arrangement and good reason.
- Liaison meetings may be held with the Police and other bodies.
- Recording Data will be used properly indexed, stored and destroyed after appropriate use.
- Data may only be viewed by Authorised School Officers, Control Room staff and the Police.
- Data required as evidence will be properly recorded witnessed and packaged before copies are released to the police.
- Data will not be made available to the media for commercial or entertainment.
- Data will be disposed of securely by incineration.
- Any breaches of this code will be investigated by the Executive Head, Head teacher or Head of School. An independent investigation will be carried out for serious breaches.
- Breaches of the code and remedies will be reported to the Head teacher and the CEO of the Trust