



The
Rise
Partnership
Trust

Love • Learn • Laugh

CCTV Policy

May 2024

1 Policy Statement

- 1.1 The Trust uses Closed Circuit Television (“CCTV”) within the premises of the trust. The purpose of this policy is to set out the position of the trust as to the management, operation and use of the CCTV at the trust.
- 1.2 This policy applies to all members of our Workforce, visitors to the trust premises and all other persons whose images may be captured by the CCTV system.
- 1.3 This policy takes account of all applicable legislation and guidance, including:
 - 1.3.1 General Data Protection Regulation (“GDPR”)
 - 1.3.2 CCTV Code of Practice produced by the Information Commissioner
 - 1.3.3 Human Rights Act 1998
- 1.4 This policy sets out the position of the trust in relation to its use of CCTV.

2 Purpose of CCTV

- 2.1 The trust uses CCTV for the following purposes:
 - 2.1.1 To provide a safe and secure environment for pupils, staff and visitors
 - 2.1.2 To prevent the loss of or damage to the trust buildings and/or assets
 - 2.1.3 To assist in the prevention of crime and assist law enforcement agencies in apprehending offenders

3 Description of system

- 3.1 All of our cameras are positioned to ensure coverage of high risk areas. The vast majority of cameras are external, with those few internal cameras being used to monitor high risk and/or high traffic (footfall) shared areas, such as reception/foyer. All cameras are fixed with no sound capability or external (over internet) access.

4 Siting of Cameras

- 4.1 All CCTV cameras will be sited in such a way as to meet the purpose for which the CCTV is operated. Cameras will be sited in prominent positions where they are clearly visible to staff, pupils and visitors.
- 4.2 Cameras will not be sited, so far as possible, in such a way as to record areas that are not intended to be the subject of surveillance. The trust will make all reasonable efforts to ensure that areas outside of the trust premises are not recorded.
- 4.3 Signs will be erected to inform individuals that they are in an area within which CCTV is in operation.
- 4.4 Cameras will not be sited in areas where individuals have a heightened expectation of privacy, such as changing rooms or toilets.

5 Privacy Impact Assessment

- 5.1 Prior to the installation of any CCTV camera, or system, a privacy impact assessment will be conducted by the trust to ensure that the proposed installation is compliant with legislation and ICO guidance.
- 5.2 The trust will adopt a privacy by design approach when installing new cameras and systems, taking into account the purpose of each camera so as to avoid recording and storing excessive amounts of personal data.

6 Management and Access

- 6.1 The CCTV system will be managed by the Site Manager, with technical support provided by the trust's IT team.
- 6.2 On a day to day basis the CCTV system operates in background mode (no one person sits and monitors it)
- 6.3 The viewing of live CCTV images will be restricted to the Site Manager, Headteacher, Designated Safeguarding Leads, and Lead Data Controller, for purposes relating to Subject Access Requests.
- 6.4 Recorded images which are stored by the CCTV system will be restricted to access by a password, known only by the Lead Data Controller, SLT, and Site Manager.
- 6.5 No other individual will have the right to view or access any CCTV images unless in accordance with the terms of this policy as to disclosure of images.
- 6.6 The CCTV system is checked periodically by the Site Manager, to ensure that it is operating effectively

7 Storage and Retention of Images

- 7.1 Any images recorded by the CCTV system will be retained only for as long as necessary for the purpose for which they were originally recorded.
- 7.2 Recorded images are stored only for a period of 28 days unless there is a specific purpose for which they are retained for a longer period.
- 7.3 The trust will ensure that appropriate security measures are in place to prevent the unlawful or inadvertent disclosure of any recorded images. The measures in place include:
 - 7.3.1 CCTV recording systems being located in restricted access areas;
 - 7.3.2 The CCTV system being encrypted/password protected;
 - 7.3.3 Restriction of the ability to make copies to specified members of staff
- 7.4 A log of any access to the CCTV images, including time and dates of access, and a record of the individual accessing the images, will be maintained by the trust.

8 Disclosure of Images to Data Subjects

- 8.1 Any individual recorded in any CCTV image is a data subject for the purposes of the Data Protection Legislation, and has a right to request access to those images.

- 8.2 Any individual who requests access to images of themselves will be considered to have made a subject access request pursuant to the Data Protection Legislation. Such a request should be considered in the context of the trust's Subject Access Request Policy.
- 8.3 When such a request is made the Lead Data Controller will review the CCTV footage, in respect of relevant time periods where appropriate, in accordance with the request.
- 8.4 If the footage contains only the individual making the request then the individual may be permitted to view the footage. This must be strictly limited to that footage which contains only images of the individual making the request. The Lead Data Controller must take appropriate measures to ensure that the footage is restricted in this way.
- 8.5 If the footage contains images of other individuals then the trust must consider whether:
- 8.5.1 The request requires the disclosure of the images of individuals other than the requester, for example whether the images can be distorted so as not to identify other individuals;
 - 8.5.2 The other individuals in the footage have consented to the disclosure of the images, or their consent could be obtained; or
 - 8.5.3 If not, then whether it is otherwise reasonable in the circumstances to disclose those images to the individual making the request.
- 8.6 A record must be kept, and held securely, of all disclosures which sets out:
- 8.6.1 When the request was made;
 - 8.6.2 The process followed by Dean Newby, Lead Data Controller, in determining whether the images contained third parties;
 - 8.6.3 The considerations as to whether to allow access to those images;
 - 8.6.4 The individuals that were permitted to view the images and when; and
 - 8.6.5 Whether a copy of the images was provided, and if so to whom, when and in what format.

9 Disclosure of Images to Third Parties

- 9.1 The trust will only disclose recorded CCTV images to third parties where it is permitted to do so in accordance with the Data Protection Legislation.
- 9.2 CCTV images will only be disclosed to law enforcement agencies in line with the purposes for which the CCTV system is in place.
- 9.3 If a request is received from a law enforcement agency for disclosure of CCTV images then the Site Manager, must follow the same process as above in relation to subject access requests. Detail should be obtained from the law enforcement agency as to exactly what they want the CCTV images for, and any particular individuals of concern. This will then enable proper consideration to be given to what should be disclosed, and the potential disclosure of any third party images.

- 9.4 The information above must be recorded in relation to any disclosure.
- 9.5 If an order is granted by a Court for disclosure of CCTV images then this should be complied with. However very careful consideration must be given to exactly what the Court order requires. If there are any concerns as to disclosure then the Data Protection Officer should be contacted in the first instance and appropriate legal advice may be required.

10 Review of policy and CCTV System

- 10.1 This policy will be reviewed annually.
- 10.2 The CCTV system and the privacy impact assessment relating to it will be reviewed biannually.

11 Misuse of CCTV systems

- 11.1 The misuse of CCTV system could constitute a criminal offence.
- 11.2 Any member of staff who breaches this policy may be subject to disciplinary action.

12 Complaints relating to this policy

- 12.1 Any complaints relating to this policy or to the CCTV system operated by the trust should be made in accordance with the trust Complaints Policy.

CCTV PRIVACY IMPACT ASSESSMENT

1 Who will be captured on CCTV?

Pupils, staff, parents/carers, volunteers, Governors, Trustees, contractors, and other visitors, including members of the public etc.

2 What personal data will be processed?

Facial Images and behaviour

3 What are the purposes for operating the CCTV system? Set out the problem that the trust is seeking to address and why the CCTV is the best solution and the matter cannot be addressed by way of less intrusive means.

- To provide a safe and secure environment for pupils, staff and visitors
- To prevent the loss of or damage to the trust buildings and/or assets
- To assist in the prevention of crime and assist law enforcement agencies in apprehending offenders

4 What is the lawful basis for operating the CCTV system?

Legal obligation, legitimate interests of the organisation to maintain safeguarding, health and safety, and to prevent and investigate crime

5 Who is/are the named person(s) responsible for the operation of the system?

School Site Manager

6 Describe the CCTV system, including:

a. how this has been chosen to ensure that clear images are produced so that the images can be used for the purpose for which they are obtained;

Advice from the supplier.

b. siting of the cameras and why such locations were chosen;

the cameras were sited to assist with the purposes stated in section 2 of the CCTV policy.

- c. how cameras have been sited to avoid capturing images which are not necessary for the purposes of the CCTV system;

Cameras have been sited so that they only capture images relevant for the purposes for which they were installed and care taken to ensure privacy expectations are not violated

- d. where signs notifying individuals that CCTV is in operation are located and why those locations were chosen; and

Signs are located at main entrances, and can be easily seen.

- e. whether the system enables third party data to be redacted, for example via blurring of details of third party individuals.

No, the system doesn't have this feature, but this could be done professionally – with the correct data protection checks and 3rd party processing agreements in place.

7 Set out the details of any sharing with third parties, including processors

The police will be granted viewing access, which will be strictly limited to footage which contains only images of the incident/individual being investigated. Should they wish to store/save images to take away with them, then a record of whom, when and in what format, will be completed and signed (as receipt) by them. As per section 9 of the CCTV Policy.

Subject Access Requests: if the footage requested contains only the individual making the request then the individual may be permitted to view the footage. This will be strictly limited to that footage which contains only images of the individual making the request. Should they wish to store/save images to take away with them, then a record of whom, when and in what format, will be completed and signed (as receipt) by them. As per section 8 of the CCTV Policy.

8 Set out the retention period of any recordings, including why those periods have been chosen

28 days (as per the CCTV policy), as this allows enough time for any issues for which CCTV footage may be needed to be reported.

- 9 Set out the security measures in place to ensure that recordings are captured and stored securely

The system is not remotely accessible and is password protected.

- 10 What are the risks to the rights and freedoms of individuals who may be captured on the CCTV recordings?

There is minimal risk, because:

- Recording takes place to safeguard all individuals, not just pupils
- Data processing is minimised due to the small number of cameras we have, the fact that they do not record audio, and the locations in which cameras are sited
- The system is not remotely accessible and is password protected, so a data breach is highly unlikely
- Risks during transfer/disclosure of recordings are minimal as this will only occur with those named in sections 6, 8, and 9 of the CCTV Policy

- 11 What measures are in place to address the risks identified?

Measures are as stated in sections 7, 8, and 9 of this impact assessment.

- 12 Have parents and pupils where appropriate been consulted as to the use of the CCTV system? If so, what views were expressed and how have these been accounted for?

No, consultation has not taken place as CCTV is essential for safeguarding staff and pupil wellbeing.

- 13 When will this privacy impact assessment be reviewed?

Annually or when the CCTV equipment/system is changed.