CCTV Policy

Introduction

This policy sets out appropriate actions and procedures, which the Trust, including Oakwood High School (OHS), Sitwell Junior School (SJS), and Thomas Rotherham College (TRC), must follow to comply with the General Data Protection Regulation (GDPR) guidelines (May 2018) and the Information Commissioner's Code of Practice in respect of the use of CCTV (closed circuit television) surveillance systems managed by OHS and TRC currently and any future installation at SJS.

This document should be read in conjunction with the following related policies and procedures:

- Trust Data Protection Policy.
- Other policies and procedures relating to GDPR.

The CCTV system includes internal and external remotely operated cameras and is used for the purpose of:

- Safeguarding of pupils/students, staff and visitors.
- Security of the Trust's premises and assets.
- Without prejudice, to protect the personal property of pupils/students, staff and visitors.
- To support the police in preventing and detecting crime.
- In a limited and restricted number of cases, to support insurance companies with possible claims.

The CCTV system is registered with the Information Commissioner's Office: Inspire Trust (14/09/20). **Registration number: ZA073427**

Responsible persons: The Senior Leader responsible is David Naisbitt, CEO of Inspire Trust. The systems are supported by the Site and Facilities teams and Trust IT Services with regard to networking and servers only. The Facilities team will work with a suitable supplier to provide maintenance and servicing.

CCTV SYSTEMS IN OPERATION

The Trust (OHS and TRC) have a purpose built internal and external CCTV system. The internal network, with associated recording and archive equipment, is under constant review to improve, upgrade and expand the system to meet the Trust's requirements. The CCTV system and cameras are serviced and maintained by an external contractor with recording and archive units supporting them. The external contractor and IT support teams will have access to the images captured only to troubleshoot the system and do not retrieve or store any images.

The design of the system ensures that the system gives the maximum effectiveness and efficiency possible but cannot guarantee to cover or detect every single incident taking place in areas of coverage.

Cameras are located in areas where pupils/students and staff have public access. Cameras are not located in areas where privacy is expected; such as toilets and changing rooms. Access to images is restricted to a small number of authorised staff, as the equipment is kept in a locked room with PC password protection and limited access. Minimal real time access to CCTV of exits and entrances is located in the site team office (TRC only) for basic monitoring of those entrances/exits. ANPR (Automated Number Plate Recognition) is used at the two traffic entrances at TRC to monitor traffic and any incidents which take place on site.

Images recorded and/or downloaded

Pupils/students and staff are notified of the use of the CCTV via the privacy statements issued to all parties and this details our legal basis for processing this data.

GDPR-appropriate signage will be displayed in reception areas and entrance areas (of any outer buildings) to notify all users that CCTV is in operation, highlighting the Trust as operator and conveying the purpose of the system, as shown below.

- The system is operational 7 days a week, 24 hours a day.
- The Site Team will routinely check that the system is operational. Any faults will be reported and rectified as soon as possible.
- All information, documentation and recordings will be treated as data protected under the Data Protection Act 2018.
- Recorded images can only be accessed by those who are authorised to do. Access to images is in a secure location. A record of when CCTV is accessed, by whom and for what purpose, is kept.
- The CCTV terminals are locked when not in use and rooms locked when vacated.
- Google Drive should be prioritised, portable storage should be avoided unless absolutely essential and authorised by the CEO and Trust IT Services.

- Images are stored for a minimum of 7 days and maximum 30 days, at which point the system will automatically be deleted. After that time all images are erased from the system apart from any which are saved pending the results of investigations.
- Downloading images is strictly controlled and is only done on the instructions of the Headteacher / Principal, Designated Safeguarding Lead or the CEO.

Access to CCTV Footage

Restrictions are in place and are as follows:

Oakwood High School:

- The Headteacher, SLT Members, Heads of House, Site Team and leading ARC staff.
- Heads of House have a real time view of the CCTV cameras only.
- The attendance team have a real time view of the entrance to school only.
- For specific issues the CEO may delegate other senior staff to view.

Thomas Rotherham College:

- Site Team
- The Principal, SLT Members, Safeguarding Leads
- For specific issues the CEO may delegate other senior staff to view.

Access by individuals

The Trust (including our schools and college) recognises the rights of staff, pupils/students and visitors to make a Data Subject Access Request (DSAR) for details of personal data held, in line with the Data Protection Act. Applications should be made in writing to the Headteacher / Principal / CEO. No public access is permitted at any time to CCTV rooms, PCs or data.

Access by the Police

Requests by the police and other external agencies to view CCTV must be for the prevention and detection of crime. Any requests must be reported to the CEO / Headteacher / Principal. The request must be accompanied by the appropriate paperwork, specifying date, time and location (as far as possible) of the image required.

If the decision is taken not to release the images, then the image in question will be held and not destroyed until all legal avenues have been exhausted.

Images will not be released to the media under any circumstances.

Access by external parties

CCTV is not monitored or accessible by external third parties other than appointed and authorised contractors for the purposes of system maintenance only.

Complaints

Any complaints in relation to the CCTV system should be addressed via the Trust Complaints Policy to the CEO.

Policy Review

Current review:	March 2022
Next review due:	March 2023 (subject to any changes in legislation)

Appendix One

CCTV – Use and Disclosure of Images Protocol

Legitimate public concerns exist over the use of CCTV and many of the specific guidelines are designed to satisfy the community that the use of cameras is subject to adequate supervision and scrutiny. It is of fundamental importance that public confidence is maintained by fully respecting individual privacy.

All employees that are authorised to view the CCTV images must read this protocol alongside the CCTV Policy and confirm that they understand and agree to abide by the policy and protocol.

CCTV images may only be viewed by authorised individuals. All authorised employees viewing the CCTV images will act with utmost probity at all times.

All images viewed by authorised employees must be treated as confidential. All authorised employees are to ensure that whilst viewing CCTV images, unauthorised employees or visitors cannot view the images.

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.

Every viewing of the images will accord with the purposes and key objectives of the CCTV system and shall comply with the CCTV Policy.

A logged entry will be kept on record for every authorised viewing.

All named individuals viewing CCTV images are responsible for their every viewing of the images, which must be justifiable.

Any breach of the CCTV Policy or CCTV Protocol (or resulting data breach) will be dealt with in accordance with existing disciplinary policy and procedures. Individuals must recognise that any such breach may amount to gross misconduct, which could lead to dismissal.

Any breach of the General Data Protection Regulations (2018) will be dealt with in accordance with that legislation. All authorised employees viewing CCTV images must be aware of their liability under this act.