CCTV Policy

Introduction and intent

This policy sets out appropriate actions and procedures, which the Trust; which includes Winterhill School (WHS), Oakwood High School (OHS), Sitwell Junior School (SJS), and Thomas Rotherham College (TRC); must follow to comply with the Data Protection Act 2018, 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, TRC and WHS 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
- ICO Code of Practice
- 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 safety and 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 Learning Trust (22/03/16). **Registration number: ZA174607.**

Responsible persons: The Senior Leader responsible is David Naisbitt, CEO of Inspire Learning Trust. The systems are supported by the Site and Facilities teams (at TRC, OHS) and Trust IT Services (at TRC, OHS, WHS) with regard to networking and servers. The Facilities team will work with suitable suppliers to provide maintenance and servicing where required.

CCTV Systems in operation

The Trust (TRC, WHS and OHS) have purpose built internal and external CCTV recording systems. 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, where applicable or required, with recording and archive units supporting them. The external contractor (where used) 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 the Trust cannot guarantee to cover or detect every single incident taking place in areas of coverage. Cameras should not be positioned in any manner to view, or record footage, from intentionally focusing on private, residential dwellings, gardens and other private property. As some Trust sites border close to residential properties there may be instances where it is not possible to have cameras fully diverted away from these dwellings and maintain suitable coverage of the Trust site. In these cases, masking software will be used to ensure that all sight of properties is removed at all times for monitoring and saving of footage.

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 at Oakwood and TRC. Due to previous incidents, Winterhill have cameras in the handwashing areas of toilet rooms, but for privacy these are not aimed in the direction of any cubicles or urinals.

Access to images is restricted to a number of authorised staff, as the equipment is kept in locked rooms 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), attendance office (OHS) and Student Reception (WHS) for basic monitoring of those entrances/exits. ANPR (Automated Number Plate Recognition) quality cameras are used at the two traffic entrances at TRC to monitor traffic and any incidents which take place on site. All sites have intercoms with integrated cameras, with no recording facility.

Consideration will be given to staff and pupils/students regarding potential invasions of privacy and confidentiality. Monitoring and viewing of footage will be conducted in a professional, ethical and legal manner. The use of CCTV for purposes outside of the scope of the policy is prohibited; including monitoring of political or religious activities. All other policies must be adhered to: relating to Discrimination, Bullying, Harassment etc. The ICO Code of Practice prohibits monitoring based on characteristics and classifications outlined in the Equality Act, including, but not limited to, race, gender, sexual orientation, nationality, disabilities etc.

Images recorded and/or downloaded

Pupils/students and staff are notified of the use of the CCTV via the privacy statements issued or made available 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 - an example of which is shown below. While the Trust site teams do not have access at Winterhill, the same email can be used with enquiries to be forwarded to WHS, rather than using a specific named account.

- Systems are operational 7 days a week, 24 hours a day.
- The Site Team will routinely check that the system is operational at OHS and TRC, IT Services will check the system at WHS. Any faults will be reported and rectified as soon as practically possible.
- All information, documentation and recordings will be treated as data protected under the Data Protection Act 2018. Data Subjects have a right to access data held about themselves, including those obtained by CCTV. Requests for Data Subject Access should be made to the Headteacher of the school, Principal of the college or the CEO.
- Recorded images can only be accessed by those who are authorised to do. Access to images is in secure locations, either through locked doors and/or password protected terminals. A record of when CCTV is accessed, by whom and for what purpose, should be kept.
- CCTV terminals are locked when not in use and rooms locked when vacated.
- Google Drive (or similar) should be prioritised, portable storage should be avoided unless absolutely essential and secured with a unique password 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 delete. 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 to 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 and Facilities Team
- The Principal, SLT Members, Safeguarding Leads
- For specific issues the CEO may delegate other senior staff to view

Winterhill School:

- The Headteacher, SLT Members, Safeguarding Leads
- Staff with L3 DSL training
- Other staff as directed by SLT
- IT Services

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. Pupils or students can only view CCTV in exceptional circumstances where doing so will assist in investigating incidents or through disciplinary procedures to have a positive influence on student behaviour and learners should not be sent to view footage without being accompanied by an appropriate member of staff.

Parents or carers must not be allowed to see footage where pupils/students are present, other than their own, unless specifically agreed in writing or email from the Headteacher, Principal or CEO and other identities must be kept confidential.

Members of the public should not be allowed on site to view footage under any circumstances. Where crime has been committed and footage is available relating to off-site activities, footage may be shared to the Police upon the clear instructions of the Headteacher/Principal or CEO.

Access by the Police

Requests by the police and other external agencies to view CCTV must be for the prevention and/or 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.

Access by external parties

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

CCTV is not monitored or accessible by external third parties other than appointed and authorised contractors for the purposes of system maintenance only. Materials or knowledge secured through CCTV will not be used for any commercial purpose.

Complaints and breaches

Any complaints in relation to the CCTV system should be addressed via the Trust Complaints Policy to the CEO. Any breach of this policy or the ICO Code of Practice by Trust staff will be investigated through appropriate disciplinary channels. A breach of the ICO Code of Practice will be thoroughly investigated utilising independent third parties to establish recommendations on remedying the breach.

Policy Review

Current review:	March 2024
Next review due:	March 2025 (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 UK-GDPR will be dealt with in accordance with that legislation. All authorised employees viewing CCTV images must be aware of their liability under this act.