CATHEDRAL SCHOOLS TRUST

Security policy

It is the responsibility of all Cathedral Schools Trust employees, governors and volunteers to familiarise themselves with the contents of all Trust policies and any amendments hereafter.

Cathedral Schools Trust

March 2025

Contents

1. Introduction

1.1. Cathedral Schools Trust is dedicated to ensuring the safety and wellbeing of all people within the school and trust community through implementing effective security measures. The trust recognises that security risks do not only take a physical form; therefore, e-safety and electronic control measures will also be used to protect members of the school. The aim of this policy is to inform staff, students, parents, carers and visitors of the security arrangements and controls in place, and encourage them to help ensure that these are implemented effectively.

1.2. The trustees and governors of all CST schools recognise and accept their corporate responsibility to provide a safe and secure environment for students, employees and visitors. Each school's security procedures will operate within the framework described in this policy.

1.3. Where appropriate schools will seek any necessary expert advice to determine the security risks and precautions to deal with them. This policy and its associated procedures apply to all individuals entering the school premises.

2. Roles and responsibilities

2.1. The following groups and/or individuals have responsibilities for ensuring the security of CST schools and sites.

2.2. **The Governors** will:

- Ensure that each school implements security measures in line with this policy and that these are regularly monitored and reviewed.
- Monitor the performance of the school security measures. This will be achieved by:
    - The Health and Safety nominated Governor monitoring performance on their visits.

- The Headteacher's reports to Governors.
- The Governors will observe implementation during their visits but will delegate the day-to-day implementation of the policy to the Headteacher.

2.3. **The Headteacher** will:

- Have delegated responsibility for the day to day security of the school.
- Set up arrangements in school that comply with the Security Policy and monitor and review these arrangements.
- Ensure that all relevant staff receive information, instruction and training in the policy, its procedures, and their own responsibilities.
- Monitor the implementation of the policy and security arrangements.
- Consider particular risk situations and consult with local professionals as appropriate.
- Provide appropriate information to pupils, parents and visitors.

2.4. **The Senior Leadership Team** will:

- Promote a collaborative and co-ordinated response to risk management within their school.
- Identify improvements in security culture.
- Implement on-going improvements in the effectiveness of security measures and controls.
- Monitor and review security measures.
- Ensure that staff are consulted and informed about security and receive appropriate training where required whether new or existing.
- Advise contractors, visitors, volunteers, parents and students of the security policy and encourage them to help to ensure that it is effective.
- Report any crimes to the police and maintain a log of crime reference numbers. Advice will be sought from the police where necessary.

2.5. **The School Business Manager and Estates/Facilities Team** will ensure that:

- The security systems and equipment, including entrances/exits, door locks and catches and fencing are maintained and checked regularly.
- Regular routine security checks are carried out.
- Security lapses are recorded and bring these promptly to the attention of the Headteacher.
- Security procedures are reviewed as and when required.
- Awareness of security issues is highlighted with all staff.
- Classrooms, windows and site entrances/exits are secure.

2.6. **All staff**

- All staff will comply with this policy and the arrangements made by the Headteacher to ensure the safety of students, employees and visitors on the school site.
- ID passes and keys must be looked after and any loss reported.

- Items of value must be kept secure.
- Site staff will secure the site at the end of the school day. All staff should support this process by ensuring that doors / windows are locked wherever possible and equipment is turned off, if appropriate.
- Staff should be vigilant at all times to the risk of intruders on the school site and report any such incidents immediately to the Estates/Facilities Team and to SLT.
- Buildings must be kept clear of all materials that can be used for arson or vandalism.
- Any security issues must be reported to the Estates/Facilities Team so that any immediate actions that need to be taken can be undertaken.

2.7. **Students, parents and visitors**

- Should not approach any stranger. They must report all strangers immediately to the nearest member of staff.
- Students are encouraged to exercise personal responsibility for their own security and the security of others.
- Students will cooperate with the arrangements made for the security of the school and will report ideas and problems to the staff.

3. Arrangements

3.1. Visitors

- Visitors must follow security procedures and be appropriately monitored whilst in school.
- Visitors must follow signing in and signing out procedures (via the InVentry System where required) and wear the relevant badge and coloured lanyard.
- All will be expected to comply with the school's security arrangements as a condition of access to the buildings and the use of them.
- Each school will identify legitimate visitors and monitor:
    - Their arrival and reason for their visit by requiring them to sign in.
    - Their departure time.
- It is preferred that all visitors have photographic ID before they enter the premises but this will not always be the case. Steps should be taken to identify visitors if there is any doubt or concern over a person's identity.

3.2. Physical security measures for the site include intruder alarms, key holding arrangements, sign-posted entry to ensure all visitors report to reception. All visitors are required to sign in and out at Reception.

4. Trespass

4.1. Trespass may give rise to a criminal offence under section 547 of the Education Act 1996 and section 206 of the Education Act 2002. In the first instance, members of the SLT should consider the level of risk. If pupils are outside, it may be necessary for them to return to the school. However, in any case, where such measures fail to resolve the situation, recourse to the law will be considered. This extends to unlawful presence on site, individuals creating a nuisance or disturbance, verbal abuse of pupils or staff, as well as violence to an individual. Any such situation will be contained as appropriate at the time, but as this is a criminal offence, the school will always refer to the police.

4.2. Any person who is not included in the following categories, and enters without permission, is considered to be a trespasser and may be asked to leave:

- Members of staff - unless suspended for health or disciplinary reasons.
- Registered students - unless excluded for disciplinary reasons.
- Parents or carers responsible for a student at the academy - unless prevented for legal reasons.
- Others - Governors, suppliers, contractors and authorised users of the premises for 'out of hours' activities.
- Professionals such as school advisers, trainers and coaches.

4.3. Staff Badges are to be deactivated following cease of employment with the school and destroyed accordingly.

4.4. Security tags / fobs are to be returned to the Business / Facilities / Site manager following cease of employment with the school

4.5. Lost / misplaced security tags / fobs are to be reported urgently to the Business / Facilities / Site manager and appropriate arrangements made to ensure site security (deactivation / wiping of fobs).

4.6. A register of keys is to be maintained, and managed by the School Business manager / Site Manager, with a full audit undertaken annually.

4.7. Staff are to return all keys following cease of employment with the school and the Key register updated.

4.8. Lost / misplaced keys are to be reported to the Business / Facilities / site manager as a matter of urgency, and a cost £100 is to be paid by the original key holder for replacement

4.9. Security Alarm Codes are to be changed regularly / upon a change of employment for staff who have knowledge of the codes

5. Offensive Weapons

5.1. It is an offence to be in possession of firearms, knives or other weapons on School/ Trust premises in line with the Behaviour Policy. The Headteacher

has discretion to determine what an offensive weapon is or what may cause harm if worn or brought to school, and to ban it. Any appeal against the Headteacher's decision will be considered by the Governing Body. The school/Trust may impose a requirement that pupils undergo screening/searches for the detection of weapons. This will be carried out in line with the Behaviour Policy.

6. Personal Property

6.1. Students are discouraged from bringing valuable items to school and in the event that they do so, the School/Trust accepts no liability including for the loss or damage to mobile phones.

6.2. If this is unavoidable on some occasion, then special arrangements should be made in advance regarding temporary safe keeping. Staff are responsible for their personal property and the School/Trust accepts no liability for it.

7. CCTV

7.1. Cathedral Schools Trust (the Trust) uses Close Circuit Television ('CCTV') within its premises. The following sections set out the position of the Trust as to the management, operation and use of the CCTV within its schools. This should be read in conjunction with the CCTV configuration and code of practice document for each school which lists the software users and checks required.

7.2. This applies to all members of our workforce, students, contractors, visitors to Trust premises and all other persons whose images may be captured by the CCTV system. It takes account of all applicable legislation and guidance, including:

- The General Data Protection Regulation (UK GDPR).
- Data Protection Act 2018.
- The Freedom of Information Act 2000
- The Protection of Freedoms Act 2012
- The Regulation of Investigatory Powers Act 2000
- Surveillance Camera Code of Practice produced by the Information Commissioner.
- Human Rights Act 1998.
- Information Commissioner's Office (ICO) (2014) 'CCTV Code of Practice'
- The Equality Act 2010

Purpose of CCTV

7.3. The Trust uses CCTV for the following purposes:

- To provide a safe and secure environment for learners, staff and visitors including safeguarding and behaviour management of students

- To prevent the loss of or damage to Trust buildings and/or assets
- To assist in the prevention of crime and assist law enforcement agencies in apprehending offenders
- To deter trespassing, criminal activity or material damage / vandalism to trust facilities.

Description of System

7.4. The Trust sites use fixed and pan, tilt and zoom cameras on sites. Cameras are not equipped for sound recording as standard.

Siting of Cameras

7.5. 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, learners and visitors. 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. Signs will be erected to inform individuals that they are in an area within which CCTV is in operation. Signage will outline 'who the school is', the purpose of capturing footage and contact details of the school. The signs should be displayed where they can be seen, such as in reception areas or external facing windows. Cameras will not be sited in areas where individuals have a heightened expectation of privacy, such as changing rooms or toilet cubicles.

Data protection impact Assessment

7.6. Prior to the installation of any CCTV camera, or system, a data protection impact assessment (available here) will be conducted by each school utilising CCTV to ensure that the proposed installation is compliant with legislation and ICO guidance.

7.7. 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.

Management, Access, Staff Conduct and Licences

7.8. CCTV policy and procedures will be managed at Trust level by the Central Estates Team. Within each school there will be a named person with responsibility for the operation of the CCTV system (Business Managers for primary schools and Facilities/ Site Managers for secondary schools). On a day to day basis the CCTV system will be operated by authorised staff in schools with delegated authority as per the table below:

Viewing Function:		**Downloading Function:**
1	Headteachers and senior leadership teams	*Yes*

2	Trust Directors / IT Director	*Yes*
3	Business Managers	*Yes*
4	Facilities / Site Managers	*Only with the written expression of 1,2 or 3*
5	ICT Technicians	*Only with the written expression of 1,2 or 3*
6	Designated behaviour lead plus one nominated pastoral member of staff (two per school)	*Only with the written expression of 1,2 or 3*
Viewing Function Only:		
6	Designated Safeguarding Lead	*Yes*
7	Deputy Designated Safeguarding Lead	*Yes*
8	Other Staff Members (*For Positive identification of individuals)*	*Only with the Written expression of 1,2,3*
9	Office and reception staff for entrance security viewing	*Yes*

7.9. The viewing of live and recorded CCTV images will be restricted to authorised members of staff in schools and the Trust offices as per the table above with explicit powers to view images, for the reasons set out above.

7.10. 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.

7.11. The CCTV system is checked annually by the Facility/Site Manager or ICT Lead technician in schools to ensure that it is operating effectively.

7.12. The CCTV system is only to be accessed during working hours or by exception out of hours with permission from the named person with responsibility for CCTV in each school.

7.13. The CCTV system is only to be accessed utilising Trust technology, within Trust premises where practical.

7.14. The CCTV system and associated software is only to be installed on Trust devices, ideally desktop computers, and have appropriate login security - No applications on mobile devices are to be used for access of any CCTV images.

7.15. CCTV systems will be installed with all due consideration to public privacy, however, some premises will by way of arrangements, have cameras that capture public areas.

7.16. A log will be maintained of when CCTV footage is accessed and reviewed (name of reviewer, date, time and reason).

Storage and Retention of Images

7.17. 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.

7.18. Recorded images are stored only for a period of 28 days during term time with the option of extension for holiday periods and unless there is a specific purpose for which they are retained for a longer period.

7.19. The Trust will ensure that appropriate security measures are in place to prevent the unlawful or inadvertent disclosure of any recorded images.

7.20. The measures in place include:

- New DVRs / NVRs installations are to be locked in secure areas
- Any existing unsecure locations should be identified by the school and a data protection impact assessment carried out (see template on Trust website)
- The CCTV system being encrypted/password protected;
- Restriction of the ability to make copies to specified members of staff;

Disclosure of Images to Data Subjects

7.21. 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.

7.22. 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 Data Protection Policy and with regard to the age of consent of a learner.

7.23. When such a request is made the named person with responsibility for CCTV in each school should review the CCTV footage, in respect of relevant time periods where appropriate, in accordance with the request.

7.24. 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 and with regard to the age of consent with a learner. The named person with responsibility for CCTV in each school must take appropriate measures to ensure that the footage is restricted in this way.

7.25. If the footage contains images of other individuals, then the school must consider whether: 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; the other individuals in the footage have consented to the disclosure of the images, or their consent could be obtained; or if not, then whether it is otherwise reasonable in the circumstances to disclose those images to the individual making the request.

7.26. A record must be kept, and held securely, of all disclosures which sets out: when the request was made; the process followed by the school Estates/Facilities Manager in determining whether the images contained third parties; the considerations as to whether to allow access to those images; the individuals that were permitted to view the images and when; and whether a copy of the images was provided, and if so to whom, when and in what format.

Disclosure of Images to Third Parties

7.27. The Trust will only disclose recorded CCTV images where it is permitted to do so in accordance with the Data Protection Legislation. Disclosure may take up to 30 school days or longer in exceptional circumstances if the Trust deems it necessary to refer to their Data Protection Officer or legal advisers as necessary.

7.28. CCTV images will only be disclosed where lawful under data protection laws.

7.29. If a request is received from a law enforcement agency for disclosure of CCTV images, the school Facilities/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.

7.30. The information above must be recorded in relation to any disclosure.

7.31. If an order is granted by a Court for disclosure of CCTV images, then this should be complied with unless the school/Trust wishes to appeal the order. 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.

Review and misuse of CCTV System

7.32. The CCTV system and the data protection impact assessment relating to it will be reviewed bi- annually.

7.33. The misuse of CCTV systems could constitute a criminal offence. Any member of staff who breaches this policy may be subject to disciplinary action.

8. Lone Working

8.1. Where possible staff should not work at school alone as there are risks involved, such as assault, accident, or sudden illness. Any member of staff wishing to work outside of normal working school hours should try to ensure that at least one other colleague is on site, ideally within 'hailing' distance, or with both parties having mobile phones programmed with each other's numbers. Should attendance be required outside of school hours this should be notified via school processes with appropriate measures put in place e.g. notification of arrival and departure from site.

8.2. However, if a member of staff is needed to work alone on site, they should take these precautions:

- Do not work at heights or on steps.
- Do not go into lofts or any other space in which you may become trapped.
- Do not do any tasks involving hazardous tools or materials.
- Lock the doors and close the windows to prevent intruders.
- Know the location of the nearest fire exit, and how to open it in an emergency.
- Know the location of the nearest first aid kit.
- Carry a mobile phone or take a school phone from the office.
- Cars should be parked close to the entrance.
- When you are leaving, limit the amount you are carrying to keep one hand free.
- Ensure someone knows where you are and when you intend to leave the school. Arrange to telephone them when you are leaving.
- If you arrive at school and find any sign of intruders, do not enter the building. Instead, call the police and notify a member of the SLT.
- If you become aware of intruders or vandals, do not challenge them. Instead, call the police, and notify a member of the SLT.
- Do not work alone if you know you have a medical condition that might cause you to become incapacitated or unconscious, unless an appropriate risk assessment has identified a way in which this can be managed.
- When working alone, do not attempt tasks which have been identified as medium or high risk, or which common sense tells you are potentially hazardous given your own level of expertise and the nature of the task.

9. Supervision of Contractors

9.1. The Facilities/ Site Manager and their team/ Business Manager have responsibility for the conduct of Contractors and external maintenance personnel. Not all will have been DBS checked; therefore, they should not have unsupervised access to children. Control measures will include:

- Agreed working times.
- Contractors will agree and sign the terms set out in the Contractor Approval Form / Guidance supplied by the School via the Senior Site Manager.
- Contractors will be signed in and issued ID badges at Reception. They are expected to wear them and sign out when leaving the site.
- Contractors will comply with all reasonable requests in connection with vehicle movements, parking and deliveries.
- Contractors must read, sign and understand the Asbestos Register contained within the main reception of the school, prior to undertaking any works.

10. Reporting and Recording Incidents

10.1. Theft, petty vandalism, criminal damage and arson are usually found in areas like recesses and doorways, which offer concealment or which are not under regular surveillance.

10.2. Incidents of this sort should be reported immediately to the Estates Team once they are discovered. Incidents should also be logged via iAMCompliant and reported to the police where required. Crime reference numbers should be collated and recorded to ensure an evidence audit trail.

10.3. Records will be kept of all incidents, which, while some may be quite minor in nature, could be significant if they recurred and became persistent.

10.4. To support school security a number of measures are in place across schools including:

- Access control systems
- CCTV
- Security lighting (where appropriate) maintained/monitored by the Estates Team.
- Intruder alarm systems
- Perimeter fencing

Each school will review all of the above on a periodic basis to see where further improvements may be necessary.

11. Complaints Relating to this Policy

11.1. 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.

Version control

Version	Date	Amended by	Recipients	Purpose
1	March 2025	Risk and Audit Committee	All schools	New policy
Date for next review	March 2026			