

# SECURITY POLICY

**Presented to:**

**Trustee Resource Committee  
6 December 2018**

Date approved: <sup>1</sup>	9 May 2017 (AMVC Property Committee)
Date adopted:	6 July 2017 (Four Cs MAT Trustees)
Date reviewed: <sup>2</sup>	6 December 2018 (Four Cs MAT Trustees)
Date of next review: <sup>3</sup>	Autumn 2021

---

<sup>1</sup> This is the date the policy was approved by the meeting

<sup>2</sup> This is the date the policy was reviewed prior to its approval above

<sup>3</sup> This is the date as set by the policy review clause or the date approved plus two years

- Headteacher also means Head of College and Principal
- School also means College, Academy or Academies
- References to School are taken to mean any school within the Four Cs Multi-Academy Trust

# Security Policy

**1.0** The aim of this policy is to advise all users within Trust schools of the measures in place in respect of the security of the school sites, associated activities undertaken and individual responsibilities.

1.1 This policy should be read in conjunction with the following policies:

- Students' Anti bullying
- Behaviour and Discipline
- General Data Protection Regulation (GDPR) and the Data Protection Act 2018
- Disciplinary, Capability and Misconduct
- Fire and Evacuation
- Health and Safety
- Information and Communication Technology (ICT) including three sub policies
- Lettings
- Safeguarding
- Trips and Visits
- Voluntary Helpers

1.3 **Users include:** Staff, Pupils / Students, Parents / Carers, Trustees / Governors, Visitors, Voluntary Helpers, Contractors, Community Users and Members of Public but do not include any of above if suspended/excluded for any reason.

1.4 **School sites includes:** all land, buildings, equipment and property.

## **2.0 Responsibilities**

The Trustees are responsible for the overall management of school security and will monitor and review this policy three yearly. Day to day management will be delegated to CEO who in turn will delegate to respective Headteachers who will be accountable for the overall implementation of this policy and, together with the Senior Management Team (SMT), will delegate responsibility for security to the relevant users in accordance with this policy.

2.1 All staff will familiarise themselves with this policy upon induction and will promote a positive attitude in respect of security.

2.2 All pupils / students should have an understanding of the need for the Security Policy and must follow all appropriate instructions from members of staff.

2.3 It is the responsibility of all users to bring to the immediate attention of the SMT any concerns in respect of security.

2.4 The decision to report any incident to the Police rests with the Senior Management Team.

## **3.0 Offences against the person**

3.1 For any offence of personal violence, Section 3 Criminal Law Act 1967 states that:  
*A person may use such force as is reasonable in the circumstances in the prevention of crime, or in effecting or assisting in the lawful arrest of offenders or suspected offenders or of persons unlawfully at large.*

3.2 To that extent, any member of staff may restrain any offender to protect any victim.

## **4.0 School Sites, Property and Equipment**

All users have an individual responsibility to reduce the potential of any damage being carried out to schools by adopting a common sense approach to the security of the site, property and equipment.

4.1 At the end of the school day, the Site team are responsible for securing all windows and doors and the setting of the alarm system. In the event of an alarm activation, the Alarm Centre Key-holder will attend in the first instance.

4.2 The following members of staff are usually designated Key-holders:

- Site Manager
- Members of Site team
- Headteacher
- Deputy Headteacher

## **5.0 Property and Equipment**

The Head of Department will be notified immediately of the loss of any property or equipment.

5.1 The property inventory will be checked annually during the Summer term and any discrepancy reported to the Head of Department.

### **5.2 Property marking**

All ICT equipment will be marked with a unique DNA code and microdots that are only visible under UV light together with an anti-tamper sticker. All other equipment identified by individual Heads of Department will also be marked in the same way to make it clearly identifiable as property of the school. This system will be registered with the suppliers, Police and Insurance approved secure asset register.

### **5.3 Vehicles**

All users parking their vehicles on school sites do so at their own risk. The Trust accepts no responsibility for any vehicle or contents brought onto the school site. Appropriate signage will be displayed in the parking areas.

### **5.4 Personal property**

The Trust accepts no responsibility for any personal property brought onto school sites. All users should be discouraged from bringing valuable items into school. If this is unavoidable, special arrangements should be made in advance for temporary safe keeping.

Where provided, Pupils / Students have lockers for storage of personal property.

## **6.0 Access control**

All staff and Trustees / Governors will be issued with photographic identification (ID) which will be worn at all times whilst at Trust schools.

6.1 All visitors, including supply and student teachers, will report to Main Reception and will be issued with a visitor's pass (recording personal and vehicle details) which will be displayed at all times whilst at the school and returned to reception on departure. Visitors will be accompanied at all times whilst at the school. Visitors who park a vehicle on site must inform Main Reception of the vehicle registration upon arrival.

6.2 External support services staff must wear their badge with a photograph identifying both themselves and their service to the school. However, if not in possession of it, they will be issued with a visitor's pass.

6.3 Any unauthorised person found on the site will be challenged by a member of staff and any necessary action will be taken. Pupils / Students should not approach any unauthorised person but immediately notify a member of staff.

6.4 There will be occasions where there are numerous visitors on site eg Open evenings, school productions, Parents/Carer evenings and during these times it will be impossible to maintain a normal daily security level. It is accepted that during these events the school could be vulnerable however it is expected that all staff will be especially vigilant.

6.5 Lanyards:

- Staff have a black lanyard for their ID badge. This shows they have a current valid DBS check and are free to access the site.
- Regular visitors / contractors have a green lanyard for their ID badge. This also shows they have a current valid DBS check and are also free to access the site unsupervised.
- Visitors not on the approved list, are issued with a red lanyard for their temporary visitor's pass. Visitors with a red lanyard must be supervised at all times. Any visitor with a red lanyard that is seen on their own, ie not under the supervision of a member of staff should be challenged. Anybody without a lanyard should also be challenged.
- Sixth Form students have a yellow lanyard.

This lanyard system applies between the hours of 7.00 am (opening time) to 4.30 pm, Monday to Friday. Outside of these periods, schools may be open for community use. However, anybody issued with the above lanyards should wear them at all times.

## **7.0 Contractors**

All regular contractors are DBS checked and are authorised to work unsupervised on site. They wear a green lanyard and ID badge.

7.1 All casual contractors will be supervised at all times by a Site team member or a 'Regular' Contractor who is DBS checked.

7.2 In the event of major building work where the 'building site area' is secure and there is no access to/from other areas of the school, casual contractors do not need to be supervised. They will, however, be subject to a 'booking-in' system under the control of the contractor's site agent.

## **8.0 Community Users**

The use of the school site for all community lettings are managed by the Site Officers.

8.1 The Trust accepts no responsibility for any property brought onto school sites.

## **9.0 Incident reporting and recording**

Any incident giving cause for concern than may affect the security of the Trust schools or any user will be recorded on the Incident Form (appendix A).

All reports will be collated by the Site Manager who, in conjunction with the SMT, will assess the need for any action and report to the Trustee Resource Committee where appropriate.

## **10.0 School trips and visits**

The security of staff and students for all out of school activities will be covered by the respective risk assessment for each event.

## 11.0 CCTV (where installed)

Schools uses closed circuit television (CCTV) images to reduce crime and monitor the school buildings in order to provide a safe and secure environment for students, staff and visitors, and to prevent the loss or damage to school property.

The system comprises multiple cameras; it does not have sound recording capability.

The CCTV system is owned and operated by the school, the deployment of which is determined by the Senior Management Team. The CCTV is monitored centrally from the school by designated users approved by the Headteacher.

The school's CCTV Scheme is registered with the Information Commissioner under the terms of the General Data Protection Regulation (GDPR) and the Data Protection Act 2018. The use of CCTV, and the associated images is covered by the General Data Protection Regulation (GDPR) and the Data Protection Act 2018. This policy outlines the school's use of CCTV and how it complies with the Act.

All authorised operators and employees with access to images are aware of the procedures that need to be followed when accessing the recorded images. All operators should comply with this policy and the CCTV Code of Practice. All employees are aware of the restrictions in relation to access to, and disclosure of, recorded images.

### 11.1 Statement of Intent

The school complies with Information Commissioner's Office (ICO) CCTV Code of Practice to ensure it is used responsibly and safeguards both trust and confidence in its continued use. The Code of Practice is published at:

[http://www.ico.org.uk/~media/documents/library/Data\\_Protection/Detailed\\_specialist\\_guides/ICO\\_CCTVFINAL\\_2301.ashx](http://www.ico.org.uk/~media/documents/library/Data_Protection/Detailed_specialist_guides/ICO_CCTVFINAL_2301.ashx)

CCTV warning signs are clearly placed in prominent positions around the school, including external gates if coverage includes outdoor areas. Signs do contain details of the purpose for using CCTV. Signage directs stakeholders to log on to [www.whoiswatchingme.org](http://www.whoiswatchingme.org) in order to make contact with the school should there be queries or concerns.

The planning and design has endeavoured to ensure that the Scheme gives maximum effectiveness and efficiency but it is not possible to guarantee that the system covers or detect every single incident taking place in the areas of coverage.

### 11.2 Siting the Cameras

Cameras will be sited so they only capture images relevant to the purposes for which they are installed (described above) and care will be taken to ensure that reasonable privacy expectations are not violated. The school will ensure that the location of equipment is carefully considered to ensure that images captured comply with the General Data Protection Regulation (GDPR) and the Data Protection Act 2018.

The school will make every effort to position cameras so that their coverage is restricted to the school premises, which may include outdoor areas.

Upon request to the Site Manager, members of staff should have access to details of where CCTV cameras are situated, with the exception of cameras placed for the purpose of covert monitoring.

### 11.3 Covert Monitoring

The school may in exceptional circumstances set up covert monitoring. For example:

- Where there is good cause to suspect that an illegal or unauthorised action(s), is taking place, or where there are grounds to suspect serious misconduct
- Where notifying the individuals about the monitoring would seriously prejudice the reason for making the recording.

In these circumstances authorisation must be obtained from a member of the Senior Management Team.

Covert monitoring must cease following completion of an investigation.

Cameras sited for the purpose of covert monitoring will not be used in areas which are reasonably expected to be private, for example toilet cubicles.

### 11.4 Storage and Retention of CCTV images

Recorded data will not be retained for longer than is necessary. While retained, the integrity of the recordings will be maintained to ensure their evidential value and to protect the rights of the people whose images have been recorded.

All retained data will be stored securely.

### 11.5 Access to CCTV images

Access to recorded images will be restricted to those staff authorised to view them, and will not be made more widely available.

### 11.6 Access to and Disclosure of Images to Third Parties

There will be no disclosure of recorded data to third parties other than to authorised personnel such as the Police and service providers to the school where these would reasonably need access to the data (eg investigators).

Requests should be made in writing to the Headteacher.

The data may be used within the Trust's discipline and grievance procedures as required, and will be subject to the usual confidentiality requirements of those procedures.

### 11.7 CCTV Complaints

Complaints and enquiries about the operation of CCTV within the school should be directed to the Headteacher in the first instance.

### 11.8 CCTV Further Information

Further information on CCTV and its use is available from the following:

- CCTV Code of Practice Revised Edition (published by the Information Commissioners Office) : <https://ico.org.uk/about-the-ico/ico-and-stakeholder-consultations/cctv-code-of-practice-revised/>
- [www.ico.org.uk](http://www.ico.org.uk)
- Regulation of Investigatory Powers Act (RIPA) 2000
- General Data Protection Regulation (GDPR) and the Data Protection Act 2018.



## APPENDIX A



# FOUR CS MAT

## INCIDENT REPORT FORM



Includes trespass, nuisance or disturbance on school premises, verbal abuse, sexual or racial abuse, threats, aggression, physical violence and intentional damage to personal property. This does not include by students during school hours. This form should be completed as fully as possible. A member of staff should complete the form for an incident involving or witnessed by a student. Please use continuation sheet if necessary.

<b>1. Member of staff reporting incident:</b>
Name:
Position:
<b>2. Personal details of person assaulted/verbally abused (if appropriate):</b>
Name:
Address (if not staff)
<b>3. Details of trespasser/assailant(s) if known:</b>
<b>4. Witness(es) if any:</b>
Name:
Address (if not staff):
Other information:
Relationship between member of staff/pupil/student and trespasser/assailant (if any):
Name:
Address (if not staff):
Other information:
Relationship between member of staff/student and trespasser/assailant (if any):
<b>5. Details of incident:</b>
a) Type of incident (eg if trespass, was the trespasser causing a nuisance or disturbance and how; if assault, give details of any injury suffered, treatment necessitated, etc).
a) Location of incident (attach sketch if appropriate).
b) Other details (describe incident, including where relevant, events leading up to it; relevant details of trespass/assailant not given above; if a weapon was involved, who else was present.
<b>6. Outcome</b> (eg whether police called; whether trespasser was removed from premises under Section 547; whether parents contacted; what happened after the incident; any legal action)
<b>7. Any further information/sketches etc (as attachments):</b>
Signed: _____ Dated: _____