Chelmsford County High School For Girls

Security Procedure

Last Amended: September 2022	Committee Responsible for Review: Facilities and Finance	
Last Approved:	Date of Next Review: September 2024	Model: School

Change Log

Date	Summary of Changes	Amended By
4/11/20	Change of alarm responders to remove Business Manager & add 3rd site team member, updated alarm zones following Bancroft removal	Richard Free
5/11/20	Inclusion of link to GDPR privacy policies	Melissa Mulgrew
27/09/22	Changes made to Locations (buildings, page 9), Locking procedure, page 10/11. Update to Appendix E regarding online reporting.	Richard Free / Melissa Mulgrew

SECURITY PROCEDURE

INDEX

1.	**Introduction**	**4**
2.	**Procedure Objectives**	**4**
3.	**Responsibilities**	**4**
4.	**Reporting and Recording**	**7**
5.	**Personal Security**	**7**
6.	**Premises Security**	**7**
7.	**IT Security**	**7**
8.	**Training**	**8**
9.	**Monitoring and Evaluation**	**8**

Appendices:

A.	Intruder alarm management	9
B.	Locking up procedures	10
C.	Maintenance of security protections e.g. locks, lighting, fencing and gates CCTV etc	12
D.	Access control and identification of all visitors	13
E.	Recording all security breaches and incidents in a log book and the responses to those breaches	14
F.	Contact list for security	15
G.	IT security	16
H.	Out of hours use of facilities	17

1. INTRODUCTION

This procedure is to be reviewed on a bi-annual basis to review its effectiveness and to take into account any changes or developments affecting the site.

2. PROCEDURE OBJECTIVES

2.1 To develop a culture which recognises the importance of security.

2.2 To provide and maintain a working environment that is safe and secure for staff, students and all users of the site.

2.3 To prevent loss of or damage to assets and property.

2.4 To provide support for any staff involved in a security incident and supply up to date information for all parties especially after any incident.

2.5 To continually improve performance with regard to security through the support of all staff to ensure security of its premises, staff, learners and visitors to the site.

3. RESPONSIBILITIES

3.1 The Headteacher

Has overall responsibility for:

3.1.1 The organisation and management of security measures

3.1.2 Monitoring the implementation of this Procedure

3.2 The Business Manager

Has responsibility within the school for

3.2.1 The implementation and maintenance of an effective Security Procedure, in consultation with the Headteacher and the Site Manager.

3.2.2 Ensuring that all staff adhere to the Procedure in their respective areas.

3.2.3 Reviewing and amending this Procedure to ensure compliance with any current guidance.

3.2.4 Carrying out periodic checks highlighting the importance of security and the responsibilities of all staff.

3.2.5 Identifying security initiatives for improving the security across the school.

3.2.6 Ensuring that all provisions of the CCTV section of the Data Protection Act are complied with and all systems are registered with the relevant Data Protection Authorities.

3.2.7 Ensuring that security risk assessments are carried out and for ensuring that staff are aware of these risks. Identified risks are controlled and/or minimized.

3.2.9 Ensuring staff awareness of this Procedure and their responsibilities and also ensure that staff receive training appropriate to the risks involved.

3.2.10 Ensuring that security arrangements across the school are being observed and that any deficiencies are reported.

3.2.11 Actively reviewing the security arrangements by carrying out routine audits.

3.2.12 Ensuring that every member of staff is issued with a Chelmsford County High School for Girls security ID badge + fob and that the badge is worn and visible at all times whilst the staff member is on school premises.

3.4 Managers

Managers are responsible for:

3.4.1 Ensuring compliance with the Security Procedure requirements in the areas for which they are responsible.

Site Manager is responsible for:

3.4.2 The appropriate use of security equipment (including secure doors, CCTV systems, alarms and detectors) provided for the health and safety of the staff.

3.4.3 Ensuring use is compliant with Data Protection and Human Rights legislation.

3.4.4 Reporting any faults to the Business Manager.

3.5 Staff Responsibilities

Every member of staff has a responsibility:

3.5.1 To familiarise themselves with:

- any special security requirements relating to their place of work or work practices
- the action to take in the event of a security incident

3.5.2 To safeguard themselves, colleagues, students and visitors, so far as is reasonably practicable, and ensure that neither equipment nor property are put in jeopardy by their actions, either by instruction, example or behaviour.

3.5.3 To follow prescribed working methods and security procedures at all times.

3.5.4 To co-operate with management to achieve the aims of the Security Procedure.

3.5.5 To comply with all training requirements concerning security issues.

3.5.6 To ensure that, where appropriate, the CCHS ID security badge is worn and visible whenever on school premises.

3.5.7 To notify their Manager of any potential security problems and report all incidents to the appropriate Manager.

In accordance with their job descriptions, individual members of staff may have responsibilities for:

3.5.8 Arming/disarming security alarms, following the set procedure, when required.

3.5.9 Monitoring/ensuring security on site car parks and traffic management.

3.5.10 Ensuring that outside lighting is adequate for staff, students and visitors requirements.

3.6 Cash Movement/Handling

3.6.1 The Business Manager must ensure that there are suitable and effective procedures in place for the movement of cash/valuables around the locality.

3.6.2 The procedures must take into account the security of the staff as well as the security of the cash/valuables.

3.7 Funding

The Business Manager in liaison with the Headteacher must take into account security issues including cost implications when:

3. Developing schemes for minor improvements.
4. Developing schemes for new premises, major upgrading etc.
5. Introducing new services or changes to existing services, which may have implications for staff security.

3.8 Key Holding

The Business Manager will clearly document the arrangements in place for the safe holding of keys to each site and the method of access to this service. The responsibility for the arrangements for daily opening/closing premises rests with the Site Manager, Assistant Site Manager or the Assistant Caretaker.

4. REPORTING, RECORDING AND INVESTIGATION

All security incidents should be reported to, recorded and, when necessary, investigated by the Business Manager using the School's established Health & Safety Incident Reporting Procedure.

5. PERSONAL SECURITY

5.1 Specific risk assessments for particular groups and activities, such as class visits, lone working, peripatetic workers, to be carried out and action plans developed and implemented.

5.2 All staff must follow existing Health & Safety Policies and guidelines.

5.3 Staff should be aware of all potential dangers.

6. PREMISES SECURITY

6.1 A procedure for the reception of visitors will be used at the school.

6.2 All members of staff have responsibility for internal security.

6.3 External areas should have appropriate lighting, fencing, gates, etc.

6.4 Car parks should have appropriate security and lighting. It is the responsibility of staff not to leave valuables in vehicles.

6.5 A security risk assessment of the school premises is carried out and reviewed annually.

7. IT SECURITY

It is the responsibility of individual managers to ensure that their staff complies with the School's 'Staff Code of Conduct' and the 'eSafety and Data Security Policy.

8. TRAINING

The content of this Procedure will form part of staff induction training.

8.1 Managers should receive the training necessary to ensure this Security Procedure is properly implemented.

8.2 Personal safety training should be made available to all staff, including those changing roles/jobs.

8.2.1 All staff should be made aware regarding their individual responsibilities, the particular hazards/risks and the important safety procedures and precautions affecting their area of work.

8.2.2 The school is committed to support the continuation and development of systematic training of Personal Safety and the relevant legislation.

9. MONITORING AND EVALUATION

9.1 The procedure will be regularly monitored to ensure that it is effective.

9.2 The School's Incident Reporting Procedure will provide baseline information on security incidents.

9.3 All incidents should be analysed to establish underlying trends.

9.4 The Business Manager in liaison with the Site Manager undertakes to evaluate the effectiveness of this Procedure. Key success areas will include:

- Optimum use of the Incident Reporting System.
- Maintaining a low level of security incidents.
- A positive evaluation of the effectiveness of training programmes.

This document should be read in conjunction with the following:-

- CCTV Surveillance Policy
- Data Protection Policy
- e-Safety and Data Security Policy
- Health & Safety Policy

And all relevant privacy notices available at http://www.cchs.co.uk/about-us/privacy-notices/

Appendix A

INTRUDER ALARM MANAGEMENT

Intruder alarm management at CCHS, is administered by Abacus Fire and Security. The full alarm system is set when no person is on site, and protects the buildings and its surroundings against unauthorised entry. CCHS subscribes to the Essex Police fully confirmed response function.

The alarm system adopts the following devices to detect entry:

- Motion sensors (heat & movement)
- Door sensors
- Timeout' on the alarm panels

Motion Sensors are located within every ground floor classroom and the majority of the school's corridors. Door sensors are located on the majority of the external doors. If one of these systems should become "live" an automatic alert is sent to the Abacus alarm receiving centre. Abacus will then contact a key holder from the school's callout list, who will attend site to investigate the alarm call-out.

If more than one alarm sensor is triggered or the same alarm sensor is triggered within a one hour period, then the alarm will be classified as a confirmed activation. With a confirmed activation Abacus will call the police who will meet a key holder on site to investigate the alarm activation.

Nominated persons to contact in the event of alarm activation are **Richard Free** (Site Manager); **Bryan Field** (Assistant Site Manager); **Kevin Clark** (Assistant caretaker).

The schools alarm system is divided into 2 zones covering 9 areas.

- Zone 1
  - Main Building
  - New English / Dining Halls / School Hall
  - Music Centre
  - Drama Building
  - 6th Form House
  - Language Building
  - New Common Room/Bancroft
  - Sports Hall
- Zone 2
  - Science Building

The account is password protected and this password will be requested when contact is made with Abacus. The alarm company are contracted to provide maintenance and at least annual checks on the system for security purposes.

Appendix B

LOCKING UP PROCEDURES

The following procedures are followed by Site Staff when unlocking and locking up the site:

Unlocking in sequence

1. 3 entrance gates & bin enclosure.
2. Site office, **unset alarms for Zone 1.**
   New Library ext
3. School main doors.
4. Door near staff kitchen leading to quad.
5. Junior door.
6. Reprographics
7. V10
8. V9
9. New Common Room
10. Swimming pool.
11. Bancroft
12. Sports Hall
13. Science building, **unset alarms for zone 2.**
14. Seymour House gates.
15. Drama building.
16. Languages Side Door
17. 6th Form House
18. Languages Front Door
19. 3 x Pond Doors
20. Door leading to music.
21. Music building.
22. Quad door.
23. New dining entrance.

Locking up in sequence

3.40pm

1. Close all windows, turn off fans, lights, projectors and air conditioning where applicable.

5.30pm

1. Door to quad.
2. Music Centre.
3. Door leading to Music Centre.
4. 6th Form Study Area.
5. Art rooms.
6. Reprographics
7. Pond doors x 3
8. Languages Door opposite Drama

9. V9
10. V10
11. V8
12. New Common Room.
13. Swimming pool.
14. Bancroft
15. Sports Hall
16. Seymour House gate.
17. Science Building, set alarms for zone 2.
18. Drama building.
19. 6th Form house.
20. Languages front door
21. Check all Main Building,1st floor rooms (windows/occupants)
22. Door near staff kitchen leading to quad.
23. Main door.
24. Library door
25. New dining entrance.
26. Site office, set alarms for zone 1.
27. Bin enclosure and 3 x gates.

Appendix C

MAINTENANCE OF SECURITY PROTECTIONS

The maintenance of all security protections is the responsibility of the Site Manager.

The Site manager will, where applicable:

- Monitor and maintain the condition of all security protections- locks, lighting, fences and gates.
- Adequately repair / replace reported defected security protections in a timely manner.
- Liaise with the CCTV / Alarm companies to ensure the contracts are kept up to date and that regular maintenance checks are carried out.
- Deal with any damaged / missing security protection devices.

Appendix D

ACCESS CONTROL AND IDENTIFICATION OF ALL VISITORS

Visitor management within the locality takes into account the following requirements:

1. The location of the reception is clearly signed and easily identifiable from entry into the building. The visitor entrance is controlled by a door access system and is also the main entrance.

2. At the reception desk visitors are asked for identification, the nature of their business, and the identity of the person they are visiting. Where possible people are encouraged to make prior appointments.

3. An electronic visitor management system is in place to record the following details for each visitor:

    i. Name
    ii. Company Name
    iii. The person whom they are visiting
    iv. Car registration
    v. Time In
    vi. Time Out

Staff are encouraged to be aware of those who may be visitors to the locality and who are not displaying a visitor's badge. They should approach them and signpost them to the reception area, if appropriate.

Appendix E

RECORDING AND RESPONDING TO SECURITY BREACHES AND INCIDENTS

Reporting accidents and ill health at work is a legal requirement and is also in line with the Health & Safety in Secondary Schools COP (Code of Practice) 1 and CCHS's own Health and Safety Incident Reporting Procedure. It is therefore important that up-to-date records are kept of security breaches occurring in the school.

The procedure set out below should be followed when reporting any security breach or incident:

- All security breaches and incidents whether occurring on the school site or on hired accommodation must be reported to the Business Manager.

- Please complete a Health and Safety Incident Form as soon as possible after the occurrence and certainly within one day. This form is available on the staff intranet http://staffintranet/

- The person reporting the breach/incident and the First Aider involved should complete the form, this will then be submitted to the Business Manager who will review the circumstances and any arising actions that need to be taken.

- If you think the incident may need to be reported to RIDDOR (Reporting of injuries, diseases and dangerous occurrences regulations 1995) please contact the Business Manager immediately for further guidance.

- If you need any assistance or guidance completing the form, please contact the Business Manager.

Appendix F

CONTACT LIST FOR SECURITY

(the information below should be used for site emergencies ONLY)

Key Holders
1st Richard Free (Site Manager) 07432 540406 or 01245 269945 **2nd Bryan Field (Assistant Site Manager)** – 07812 060444 or 01245 423176 **3rd Kevin Clark (Assistant caretaker)** – 07933 255198
Alarm Monitoring **Abacus Fire & Security** 01473 824601 - Quote the password (known to key holders)

Appendix G

IT SECURITY

Information

All Staff are expected to be aware of, and comply with the CCHS 'Staff Code of Conduct' and the 'eSafey and Data Security Policy'. Additionally, Information must be held within the organisation in compliance with the Data Protection Act (1988) and General Data Protection Regulations 2018. Personal data on file must be kept secure and up to date. The school adopts the following procedures to ensure that the principles of the Act are adhered to:

- Levels of access to student information are restricted as necessary. Staff only have authority to remove or change records where it is key to their job role to do so.

- The eSafety and Data Security Policy outlines the access rights to information and staff should make themselves aware of this procedure.

- All Staff and students have a unique login and password, which must be kept secure at all times. In no circumstances should an individual's password be disclosed to another person.

- Passwords must be regularly changed for security reasons - this is prompted by an automatic expiry reminder-.

- Requests for new login details will be submitted through the IT department.

Equipment

Equipment should be kept in locked rooms/cupboards when not in use, and only appropriate persons should have access to these stores. All IT suites should have secure door locks which should be used when necessary to prevent security breaches. Students should not be allowed to access rooms unaccompanied, although it is recognised that there may be instances just before the class starts and at the end when this is unavoidable. All staff must remain vigilant and report any issues or concern to the Business Manager.

At the end of a school day and during the school holidays, staff laptops must be kept locked in the bank of laptop lockers located outside the Staff Workroom, or taken home and stored securely.

Appendix H

OUT OF HOURS USE OF FACILITIES

Staff, students and visitors are not permitted on site without the presence of a member of the Site Staff.