The STAR Multi Academy Trust
SECURITY POLICY

This policy has been adopted by the Board of Directors of the STAR Multi Academy Trust and is applicable across all schools that make up the STAR Multi Academy Trust. In line with the MAT's Scheme of Delegation, this Policy must be duly applied by each Local Governing Board and the Head Teacher of each school that is part of the STAR Multi Academy Trust.

Where there are specific details or any discretions in the policy that apply to an individual school or Local Governing Board this has been made clear within the wording of the policy.

This policy will be monitored regularly by the MAT Headteachers' Group and reviewed formally by the STAR MAT Board of Directors in line with the agreed timetable for policy review or sooner as events or legislation changes require.

DATE ADOPTED: 29 September 2020
DATE FOR REVIEW: September 2023
Approved by the Trust Board: 17 October 2023
Review Date: October 2026

Contents

* In this document:

- the term ‘parent’ includes guardian and primary carer
- the term ‘student’ includes pupil

1 Introduction

Our most common security problems are general nuisance, disturbance, abusive behaviour, vandalism and thefts by young people visiting the site. However, response to unacceptable behaviour may lead to confrontation, escalating to a more serious incident.

Our aim is to ensure the safety of everyone on the site, to:

a. allow them to work without distraction
b. prevent violence
c. protect property against theft, fraud and damage
d. prevent or minimise security problems

The underlying principles are: -

a. we do not expect or accept visitors being threatening, violent or abusive. We do not expect or accept visitors to cause damage or loss. We will work with staff to prevent or, if necessary, respond to unacceptable behaviour.

b. an acknowledgement that crime can never be completely prevented but can be significantly minimised with care and vigilance.

c. prevention is the most effective approach so forward planning and risk assessment are a priority in our work.

There is a need for an immediate and appropriate response by staff when there is an incident. This requires everyone on the site to know of, and to follow the security policy.

To be read in conjunction with following DFE guidance:

School and college security - GOV.UK (www.gov.uk)

2 Roles and responsibilities

The Trust Board is responsible for:

- Undertaking necessary security risk assessments in conjunction with the Headteachers and Head of Estates & Facilities.
- Monitoring the performance of the school's security measures.
- Reviewing the Trust Security Policy on an annual basis, amending procedures where necessary.
- Delegating the day-to-day implementation of this policy to the LBGs/Headteachers

The LGBs/Headteachers are responsible for:

- Ensuring that all staff members are aware of the procedures set out within this policy and are provided with the required training.
- Informing parents, visitors and contractors of the school's security procedures.

- Establishing a system for reporting, recording and managing breaches of this policy.
- Budgeting for security measures effectively.
- Nominating specific staff members with designated security roles.
- Ensuring that security is taken into account when considering any proposed changes to the school premises.
- Undertaking necessary security risk assessments in conjunction with the Trust Board.
- Ensuring appropriate arrangements are in place for the storage of money at the school.
- Reporting any crimes to the police.

All staff members are responsible for:

- Securing windows and doors when rooms are not in use.
- Ensuring that visitors sign in and out at the school reception.
- Challenging any unidentified individuals.
- Securing valuable equipment after use.
- Ensuring the security of school equipment when taken off the school premises, such as laptops.
- Accessing the school premises in accordance with the school procedures.
- Acting in accordance with the Trusts GDPR Policy, ensuring that data and information is secure.
- Reporting any security concerns to the Headteachers.
- Carrying their ID with them at all times.
- Their own property which they bring to the school site.

The Site teams are responsible for:

- Maintaining the safe operation of physical and electrical security systems, including school fencing.
- Securing school entrances and exits.
- Liaising with the other members of the Site Team, ensuring that the school is effectively secured at the end of each day.
- Carrying out security checks on a regular basis and maintaining a record of these checks.
- Raising any security concerns with the Headteachers immediately.

Pupils and parents are responsible for:

- Reporting anyone without an ID badge to a staff member.
- Reporting any activity which they believe to be suspicious or of a concern to a member of staff immediately.

3 Security measures

Each school has the following measures in place -

a. Intruder alarms in all blocks, linked to a national monitoring station and the police.

b. Security fencing which is locked.

c. Surveillance cameras.

d. Secure stores.

e. Maglock doors to prevent access out of hours.

f. Barred windows where relevant.

g. An inventory and security coded marking for property valued above £1000 or lower if the goods are 'attractive' or portable, e.g. printers, cameras.

h. Site team, senior staff and technicians responsible for areas.

i. Staff members have a mobile phone/system when working alone.

j. Personal alarms available in Reception.

k. All staff wear name badges at all times and sign in and out of the school.

l. All visitors have use signing in system and wear the appropriate badges

l. Laptops in use by staff are signed out and back in with ICT staff end of contract

m. Private use of Assets Policy

Staff, students and visitors are responsible for the safety of their own property. Cars, bicycles, classrooms, offices and desks should be locked whenever possible. Ideally, valuable personal items should not be brought to the school but if necessary, this is at the owner's personal risk. Items should be locked away out of sight and certainly not left unattended.

Staff have a responsibility for securing the school property during and at the end of the day. Particular attention should be paid to the security of school keys which should not be left unattended, for example in a pigeon hole. Desirable equipment must be locked away out of sight at the end of the day: this is particularly important in ground floor rooms.

Staff must take great care of any money they collect or, for example, jewellery or mobile phones they may confiscate. As soon as is practicable, and certainly within a day, money should be handed in to the Bursary/Admin Office and jewellery and other valuables should be sealed in a labelled envelope for storage in the school safe. Until then it should be kept secure as the School must compensate for loss.

Fire doors should not be opened for normal access, but if opened, they should be closed by staff at the end of the lesson/day. Staff are asked to close windows at the end of the day.

During school time, staff should sign in and out of Inventry/Quick scan/Inventry App if they leave the site.

Staff working alone out of school hours or in the holidays should alert the Site Team or SLT member directly or via Reception. They will be told which exits are open, in line with the fire policy, and make any arrangements for securing the building. Staff working in the holidays should sign in and out in the Reception area. A personal alarm can be borrowed from Reception and all staff should know the sound of, and the need to, respond to the alarm call.

On evenings such as Parents' meetings or performances senior staff will ensure that no teacher is left in the building alone.

Staff meeting with visitors who are expected to be angry, or not in control in some way, should not conduct the meeting alone, should use a central office, should borrow a personal alarm and should warn nearby colleagues. If necessary, the interview should be stopped and if it needs to be reconvened then, in consultation with the Headteacher, a letter should be sent stressing our requirements for reasonable behaviour, at the new appointment. In extreme cases, refer to a member of SLT who may alert the police in advance.

4 Visitors

Schools are not public places with an unrestricted right of access. We welcome visitors with legitimate business in the school, but they must comply with our security arrangements.

All visitors in school hours (i.e. anyone not on the staff or student database) should be booked in the school calendar and must report to Reception on arrival at the site. There, they sign in and receive a visitors' badge which must be worn at all times.

Reception staff will contact the appropriate member of staff to arrange for a visitor to be collected, escorted or directed. Only regular visitors with DBS clearance such as peripatetic staff will be unescorted.

Although we try to be helpful, a visitor without an appointment may need to wait or to see a different member of staff, as lessons will not normally be interrupted.

Former students may not come back to visit their friends. If a former student comes into the school, s/he should not be given a visitor pass but should wait in Reception until the teacher s/he wishes to see is available.

Students may meet with professionals from other agencies by arrangement but would not normally receive visitors. If a visitor asks to see a student for a personal reason this is only allowed with the permission of a member of the Senior Leadership Team or Year Leader.

At the end of the visit, the visitor must go to Reception to sign out and return their badge. If Reception is closed the badge should be collected by the member of staff taking responsibility for them.

Anyone not wearing a badge should be questioned. If they do not have legitimate business, ask them politely to leave and follow the policy for intruders.

Students will be instructed not to speak to strangers or anyone without a name badge.

5 Trespass

An intruder is anyone entering the school without permission, legitimate reason or without complying with our security arrangements.

It is an offence for anyone to come on to a school site without the permission of the Headteacher under the Education Act 1996, section 547.

Staff should ask intruders to leave the site. This should be polite and non-confrontational. Staff should walk away if the response is unacceptable and contact a senior member of staff either directly or via Reception.

Senior staff should reinforce the message for the intruder to leave the site. At no point should staff try to remove intruders physically.

If the intruder leaves the site or stays without causing any disturbance, then staff should record or give as full details as possible to Reception staff. This should be noted on an intruder report and a formal warning letter will be issued if personal details are known. This is also copied to the Police.

If the person is a persistent intruder, or he/she stays on site and causes disturbance, appears threatening, is suspected of having an offensive weapon or if there is physical injury then a Senior member of staff should contact the Police. In an emergency requiring an immediate response, dial 9-999 and then immediately inform Reception staff and SLT.

If Police are called, full details should be passed to Reception staff, including the expected whereabouts of witnesses in case police need to speak to them.

Reception staff will keep an up to date, systematic record of incidents.

Where appropriate, students should be moved from the vicinity of a potential/ongoing incident.

6 Theft or damage to property

If there is theft of, or damage to, personal property the victim will be encouraged and supported to contact the police. Whenever possible, there will also be an internal investigation.

If there is theft of, or damage to, school property then this must be reported immediately to the Site Team so the police can be contacted, time-limited insurance claims can be made, an internal investigation can be started, the inventory updated, and our security plans can be re-assessed.

7 Bomb Threats/Aggressive Intruders/Terrorist

It is vital that staff who deal initially with any reports of a bomb threat understand their responsibility in assisting the School and conduct the correct response that is proportionate to the risk and ensures the safeguarding of the School.

Schools have the option to evacuate, internally evacuate, or take no action.

Each School has their own procedure for managing 'internal Evacuation' (Lockdown) and a drill will be carried out twice a year.

No action- this could be reasonable if, after evaluation by the venue, the threat is deemed implausible or a hoax. Police may provide additional advice and guidance. A proportionate search of the venue should be considered.

Following a series of malicious hoax communications to schools across the UK, which are not being investigated as terrorism related offences, it is important that you are alert, but not alarmed. This is an opportunity for you to review your security plans to confirm that the arrangements you should already have in place are still current and have been tested to ensure staff and students are prepared and confident.

8 Bomb threats: Procedures for handling bomb threats.

The vast majority of bomb threats are hoaxes designed to cause alarm and disruption. As well as the rare instances of valid bomb threats, terrorists may also make hoax bomb threat calls to intimidate the public, businesses and communities, to draw attention to their cause and to mislead police. While many bomb threats involve a person-to-person phone call, an increasing number are sent electronically using email or social media applications. No matter how ridiculous or implausible the threat may seem, all such communications are a crime and should be reported to the police by dialling 999. It is important that potential recipients – either victims or third-parties used to pass the message - have plans that include how the information is recorded, acted upon and passed to police.

The bomb threat message.

Bomb threats containing accurate and precise information, and received well in advance of an actual attack, are exceptionally rare occurrences. Precise motives for hoaxing are difficult to determine but may include revenge, extortion, a desire to impress, or a

combination of these and other less understandable motives. In the vast majority of cases are hoax and the intent is to socially engineer, provoke a response, cause disruption or inconvenience the victim.

Communication of the threat. National Counter Terrorism Policing Headquarters

A bomb threat can be communicated in a number of different ways. The threat is likely to be made in person over the telephone; however, it may also be a recorded message, communicated in written form, delivered face-to-face or increasingly, sent electronically via email or a social media application e.g. Twitter or Instagram. It should also be noted that a threat may be communicated via a third-party, i.e. a person or organisation unrelated to the intended victim.

What you should do if you receive a bomb threat communication.

Any member of staff with a direct telephone line, mobile phone, computer or tablet etc., could conceivably receive a bomb threat. Such staff should, therefore, understand the actions required of them as the potential first response to a threat call.

If you receive a telephone threat, you should:

a) stay calm and listen carefully
b) have immediate access to a checklist on key information that should be recorded (see bomb threat checklist - attached)
c) if practical, keep the caller talking and alert a colleague to dial 999
d) if displayed on your phone, note the number of the caller, otherwise, dial 1471 to obtain the number once the call has ended
e) know who within your organisation to contact upon receipt of the threat, e.g. building security/senior manager
f) if the threat is a recorded message write down as much detail as possible
g) if the threat is received via text message do not reply to, forward or delete the message. Note the number of the sender and follow police advice

If the threat is delivered face-to-face:

a) try to retain as many distinguishing characteristics of the threat-maker as possible. If discovered in a written note, letter or as graffiti:
b) treat as police evidence and stop other people touching the item

If the threat is received via email or social media application:

a) do not reply to, forward or delete the message
b) note the sender's email address or username/user ID for social media applications
c) preserve all web log files for your organisations to help the police investigation (as a guide, 7 days prior to the threat message and 48 hours after)

REMEMBER Dial 999 and follow police advice. Seek advice from the venue security/operations manager as soon as possible.

The Credibility of Bomb Threats.

Evaluating the credibility of a threat is a critical task, particularly if the attack being threatened is imminent. This is a tactic used to place additional pressure on decision makers. When specific intelligence is known to police, advice will be issued accordingly; however, in the absence of information, it will be necessary to consider a number of factors-

- is the threat part of a series? If so, what has happened elsewhere or previously?
- can the location of the claimed bomb(s) be known with precision? If so, is a bomb visible at the location identified?
- considering the hoaxer's desire to influence behaviour, is there any reason to believe their words?
- if the threat is imprecise, could an external evacuation inadvertently move people closer to the hazard?

9 Evacuation considerations.

Responsibility for the initial action taken at a venue subject to a bomb threat sits with the establishment, not police. However, all bomb threats should be reported to the police and their advice followed accordingly. Venue option include: -

External evacuation.

Leaving the venue will be appropriate when it has been directed by police and/or it is reasonable to assume the threat is credible and evacuation will move people towards a safer location. Appoint people, familiar with evacuation points and assembly (rendezvous) points, to act as marshals and assist with this procedure. At least two assembly points should be identified in opposing directions, and at least 500 metres from the suspicious item, incident or location. Where possible the assembly point should not be a car park. You may wish to seek specialist advice, which can help to identify suitable assembly points and alternative options as part of your planning. Where there are large numbers of people consider a phased evacuation, initially from the immediate area of the device. This will avoid unnecessary alarm and promote a safer evacuation. Each venue is unique and should plan and exercise for different threat scenarios.

The police will establish cordons depending upon the size of an identified suspect device. Always follow police directions and avoid assembly close to a police cordon.

Minimum police cordon distances are: -

100m – small items e.g. rucksacks or briefcases

200m – medium items e.g. suitcases, wheelie bins or cars

400m – larger items e.g. vans or lorries

Internal or inwards evacuation (Lockdown).

Staying in your venue but moving people away from external windows/walls and is relevant when it is known that a bomb is not within or immediately adjacent to your building. Also consider that if the location of the device is unknown, is an evacuation necessary. If a suspect device is outside your building it may put people in danger if the evacuation route takes them past the device. A safer alternative maybe the use of internal protected spaces. Inwards evacuation needs significant pre-planning and may benefit from expert advice to assist in identifying an internal safe area within your building.

No action.

This will be reasonable and proportionate if, after the evaluation by the venue, the threat is deemed implausible or a hoax. Police may provide additional advice and guidance. A proportionate search of the venue should be considered.

Remember: it is vital that regular drills are carried out to ensure all are familiar with bomb threat procedures, routes and assembly points. (See Fire Policy)

10 Search Considerations

Regular searches of your establishment, proportionate to the risks faced by an organisation, will enhance a good security culture and reduce the risk of a suspicious item being placed or remaining unnoticed for long periods.

- ensure plans are in place to carry out an effective search in response to a bomb threat
- identify who in your venue will coordinate and take responsibility for conducting searches
- initiate a search by messaging over a public address system (coded messages avoid unnecessary disruption and alarm), by text message, personal radio or by telephone cascade
- divide your School into areas of a manageable size for 1 or 2 searchers. Ideally staff should follow a search plan and search in pairs to ensure nothing is missed
- ensure those conducting searches are familiar with their areas of responsibility. Those who work regularly in an area are best placed to spot unusual or suspicious items
- focus on areas that are open to the public; enclosed areas (e.g. cloakrooms, stairs, corridors, lifts etc.) evacuation routes and assembly points; car parks, other external areas such as goods or loading bays
- develop appropriate techniques for staff to be able to routinely search public areas without alarming any visitors or customers present

- under no circumstances should a suspicious item found during a search be touched or moved in any way. Immediately start evacuation and dial 999
- ensure all visitors know who to report a suspicious item to and have the confidence to report suspicious behaviour

11 Media and Communication

Avoid revealing details about specific incidents to the media or through social media without prior consultation with police. Do not provide or give details of the threat or the decision-making process relating to evacuation, internal evacuation, or taking no action.

Releasing details of the circumstances may: -

- be the objective of the hoaxer, providing them with a perceived credibility
- cause unnecessary alarm to others
- be used by those planning to target other venues
- illicit copycat incidents
- impact upon a subsequent investigation

12 Appendix 1

Date ..... Time ..... Intruder Name .....

Description

Age? 11-14 15-20 20+

Gender? Male Female

Height? Under 5’ 5’-5’6” 5’6” -6’ 6’ +

Hair? black brown ginger blonde grey

long short curly shaved natural

Clothes? trousers ..... jeans ..... shorts ..... skirt ..... (inc. colour)

shirt ..... T-shirt ..... jumper ..... jacket .....

cap ..... trainers ..... boots .....

Other clues to identity?

Full details of incident, including how did it leave staff feeling?

Name of witnesses .....

Contact places for next few hours .....

Report by .....

SLT alerted?

Previous intruder history?

Police called?

Other? .....

13 Appendix 2

ACTIONS TO BE TAKEN ON RECEIPT OF A BOMB THREAT

1 Remain calm and talk to the caller

2 Note the caller's number if displayed on your phone

3 If the threat has been sent via email or social media see appropriate section below

4 If you are able to, record the call

5 Write down the exact wording of the threat:

ASK THESE QUESTIONS & RECORD ANSWERS AS ACCURATELY AS POSSIBLE:

1. Where exactly is the bomb right now?	
2. When is it going to explode?	
3. What does it look like?	

4. What does the bomb contain?	
5. How will it be detonated?	
6. Did you place the bomb? If not you, who did?	
7. What is your name?	
8. What is your address?	
9. What is your telephone number?	
10. Do you represent a group or are you acting alone?	
11. Why have you placed the bomb?	
Record time call completed:	

INFORM BUILDING SECURITY/ COORDINATING MANAGER

Name and telephone number of person informed:	

DIAL 999 AND INFORM POLICE

Time informed:	

This part should be completed once the caller has hung up and police/ building security/ coordinating manager have all been informed

Date and time of call:

Duration of call:

The telephone number that received the call:

ABOUT THE CALLER:

Male	Female	Nationality?	Age?
☐	☐		

THREAT LANGUAGE:

Well-spoken	Irrational	Taped	Foul	Incoherent
☐	☐	☐	☐	☐

CALLER'S VOICE:

Calm	Crying	Clearing	Angry	Nasal
☐	☐	☐	☐	☐

Slurred	Excited	Stutter	Disguised	Slow	Lisp	*Accent
☐	☐	☐	☐	☐	☐	☐

Rapid	Deep	Familiar	Laughter	Hoarse	Other *(please specify)*
☐	☐	☐	☐	☐	

What accent?

If the voice sounded familiar, who did it sound like?

BACKGROUND SOUNDS:

Street noises	House noises	Animal noises	Crockery	Motor
☐	☐	☐	☐	☐

Clear	Voice	Static	PA system	Booth	Music
☐	☐	☐	☐	☐	☐

Factory machinery	Office machinery	Other *(please specify)*
☐	☐	

REMARKS:

ADDITIONAL NOTES:

ACTIONS TO BE TAKEN ON RECEIPT OF A BOMB THREAT SENT VIA EMAIL OR SOCIAL MEDIA

1 DO NOT reply to, forward or delete the message

2 If sent via email note the address

3 If sent via social media what application has been used and what is the username/ID?

4 Dial 999 and follow police guidance

5 Preserve all web log files for your organisations to help the police investigation (as a guide, 7 days prior to the threat message and 48 hours after)

DOCUMENT CONTROL

Author/Contact	Rob Holah	
Status	Issue 1.1	
Publication Date	September 2020	
Review Date	Annually	
Approved/Ratified by	Trust Board	Date: July 2021
History		