



Estates Security Policy

Author:	Group Director of Premises
Consultation:	Health and Safety Committee
Approval:	Board of the Corporation
Version Date:	August 2026
Approved Date:	October 2026
Next Review:	September 2027

Contents

1.	Policy Statement	3
2.	Purpose	3
3.	Scope.....	3
4.	Security Principles.....	4
5.	Governance.....	4
6.	Roles and Responsibilities.....	5
7.	Security Framework	5
8.	Security Risk Management	6
9.	Safeguarding and Security	6
10.	Security Systems and Physical Security	7
11.	Security Incident Management	7
12.	Counter-Terrorism and Protective Security.....	7
13.	Emergency Preparedness and Business Continuity.....	8
14.	Training and Awareness.....	8
15.	Monitoring, Assurance and Review	9
16.	Related Policies and Procedures.....	9
17.	Legislative and Regulatory Framework.....	9
18.	Review Arrangements.....	10

1. Policy Statement

- 1.1. Trafford & Stockport College Group (the Group) is committed to providing a safe, secure, welcoming and inclusive environment for all students, apprentices, staff, visitors, contractors, governors and stakeholders.
- 1.2. The Group recognises that effective security management is fundamental to safeguarding, health and safety, business continuity, organisational resilience and the delivery of high-quality education. Security arrangements will be proportionate, risk-based and integrated with the Group's safeguarding, emergency planning and risk management frameworks.
- 1.3. The Group will take all reasonably practicable measures to protect people, premises, assets, infrastructure and reputation from security threats including crime, violence, abuse, exploitation, unauthorised access, theft, vandalism, disorder and acts of terrorism.
- 1.4. Security is a shared responsibility. Everyone who studies, works or visits the Group has a role in maintaining a safe and secure environment and must comply with security arrangements, remain vigilant and report concerns promptly.

2. Purpose

- 2.1. The purpose of this policy is to:
 - Establish the Group's strategic approach to security management.
 - Protect people, premises, assets and reputation.
 - Support safeguarding and the protection of children, young people and vulnerable adults.
 - Support organisational resilience and business continuity.
 - Define security governance, responsibilities and accountability.
 - Support compliance with relevant legislation, including the Terrorism (Protection of Premises) Act 2025 (Martyn's Law).
 - Promote a culture of vigilance, preparedness and continuous improvement.

3. Scope

- 3.1. This policy applies to:
 - All Trafford & Stockport College Group campuses, premises and facilities.
 - All Group-controlled activities and events.
 - All staff, students, apprentices, governors, contractors, visitors and partners.
 - All physical security measures, systems and security-related procedures.

* This policy does not apply to cyber security or information security arrangements, which are governed through separate policies.

4. Security Principles

4.1. The Group shall manage security in accordance with the following principles:

4.2. Prevention

4.2.1. Implementing proportionate measures to deter, detect and reduce security risks before incidents occur.

4.3. Protection

4.3.1. Maintaining appropriate physical, procedural and technological controls to protect people, assets and premises.

4.4. Preparedness

4.4.1. Ensuring effective arrangements exist to respond to foreseeable security threats and emergencies.

4.5. Response

4.5.1. Providing a coordinated and proportionate response to incidents and emergencies.

4.6. Recovery

4.6.1. Supporting the restoration of normal operations and learning following security incidents or disruptions.

4.6.2. Security arrangements shall be proportionate to risk and designed to support an environment that remains safe, welcoming, accessible and inclusive.

5. Governance

5.1. Security forms part of the Group's wider governance framework and is closely aligned with safeguarding, health and safety, risk management, emergency planning and business continuity.

5.2. Corporation Board

5.2.1. The Corporation Board provides strategic oversight and receives assurance regarding significant security risks, compliance and performance.

5.3. Executive Leadership Team

5.3.1. The Executive Leadership Team is responsible for ensuring appropriate security arrangements are in place across the Group and for reviewing significant risks, incidents and improvement actions.

5.4. Group Director of Premises

5.4.1. The Group Director of Premises is the Policy Owner and has strategic responsibility for:

- Security management and planning.
- Protective security and resilience arrangements.
- Compliance with relevant legislation.

- Security risk management.
- Security contractor management.
- Coordination of security improvement programmes.
- Oversight of Martyn's Law preparedness and implementation arrangements.

6. Roles and Responsibilities

6.1. Managers

6.1.1. Managers are responsible for:

- Implementing security requirements within their areas.
- Ensuring staff and students understand local security arrangements.
- Escalating concerns and incidents appropriately.
- Supporting investigations, risk assessments and emergency responses.

6.2. Security Personnel

6.2.1. Security personnel shall:

- Provide security services in accordance with contractual requirements.
- Hold appropriate licences where required.
- Support access control, patrols, incident response and monitoring activities.
- Support safeguarding and emergency management arrangements.
- Report concerns and incidents promptly.

6.3. Staff

6.3.1. All staff shall:

- Comply with security arrangements and procedures.
- Display identification as required.
- Report security, safety and safeguarding concerns.
- Participate in mandatory training and emergency exercises.
- Follow security and emergency instructions.

6.4. Students

6.4.1. Students are expected to:

- Comply with College security arrangements.
- Carry and produce identification where required.
- Report concerns and suspicious behaviour.
- Follow security and emergency instructions

6.5. Contractors, Visitors and Partners

6.5.1. All visitors, contractors and external users must comply with Group security, safeguarding and site management arrangements whilst on Group premises.

7. Security Framework

7.1. The Group operates a risk-based security framework that integrates safeguarding, security, health and safety, emergency preparedness and organisational resilience.

7.2. The framework includes:

- Security risk management.
- Access control and visitor management.
- Physical security measures.
- Security personnel and contractor management.
- Incident reporting and investigation.
- Safeguarding arrangements.
- Counter-terrorism preparedness.
- Emergency response planning.
- Business continuity and recovery arrangements.
- Training, awareness and assurance activities.

7.3. Operational requirements are contained within supporting policies and procedures.

8. Security Risk Management

8.1. Security risks shall be identified, assessed and managed in accordance with the Group Risk Assessment Procedure.

8.2. Assessments shall consider, where appropriate:

- Terrorism and hostile acts.
- Violence and aggression.
- Safeguarding concerns.
- Unauthorised access.
- Theft and criminal activity.
- Vulnerable individuals.
- Public events and gatherings.
- Operational disruption.
- Site-specific risks and vulnerabilities.

8.3. Security risks shall be reviewed periodically and following significant changes, incidents or emerging threats.

9. Safeguarding and Security

9.1. The Group recognises that security and safeguarding are intrinsically linked.

9.2. Security arrangements shall support the Group's statutory safeguarding responsibilities, including:

- Protection of children and young people.
- Protection of vulnerable adults.
- Prevention of abuse, exploitation and harm.
- Compliance with Prevent duties.
- Identification and reporting of safeguarding concerns.

- 9.3. All employees, contractors and security personnel must report safeguarding concerns in accordance with the Safeguarding, Child Protection and Vulnerable Adults Policy.

10. Security Systems and Physical Security

- 10.1. The Group shall maintain proportionate physical security measures appropriate to the risks associated with each campus, facility or activity.

- 10.2. These measures may include:

- Access control systems.
- Identification and badge systems.
- Visitor management arrangements.
- CCTV systems.
- Intruder detection systems.
- Perimeter security measures.
- Security lighting.
- Life-safety and emergency communication systems.

- 10.3. All individuals attending Group premises must comply with applicable identification, visitor and access control procedures.

11. Security Incident Management

- 11.1. Security incidents shall be reported, recorded, investigated and reviewed through the Group's established reporting and incident management arrangements.

- 11.2. Security incidents may include:

- Violence and aggression.
- Criminal activity.
- Unauthorised access.
- Safeguarding concerns.
- Suspicious activity.
- Threats or acts of terrorism.
- Significant security system failures.
- Events requiring lockdown, evacuation or emergency response.

- 11.3. Where incidents involve students, associated behavioural or disciplinary matters shall be managed in accordance with relevant student procedures.

- 11.4. Lessons learned shall be used to strengthen security controls, training and risk management arrangements.

12. Counter-Terrorism and Protective Security

12.1. The Group is committed to maintaining appropriate preparedness for terrorism-related threats and supporting compliance with the Terrorism (Protection of Premises) Act 2025 (Martyn's Law).

12.2. The Group will:

- Promote vigilance and security awareness.
- Support Prevent responsibilities.
- Undertake terrorism-related risk assessments.
- Maintain appropriate protective security arrangements.
- Consider security requirements for events and activities.
- Maintain procedures for evacuation, invacuation, lockdown and emergency communications.

12.3. Protective security measures shall be proportionate to risk and aligned with recognised national guidance and good practice.

13. Emergency Preparedness and Business Continuity

13.1. The Group shall maintain arrangements to respond effectively to emergencies and significant security incidents.

13.2. These arrangements may include:

- Emergency response procedures.
- Evacuation procedures.
- Lockdown and hostile intruder procedures.
- Incident management arrangements.
- Business continuity plans.
- Recovery and resilience planning.

13.3. Arrangements shall be periodically reviewed, tested and exercised to ensure continued effectiveness.

14. Training and Awareness

14.1. The Group shall provide appropriate security awareness, instruction and training.

14.2. Training may include:

- Safeguarding.
- Prevent.
- Security awareness.
- Martyn's Law awareness.
- Emergency procedures.
- Incident reporting.
- Lockdown and hostile intruder response.
- Business continuity awareness.

14.3. Training requirements shall be proportionate to individual roles and responsibilities.

15. Monitoring, Assurance and Review

15.1. The effectiveness of security arrangements shall be monitored through:

- Security audits and inspections.
- Incident analysis and trend monitoring.
- Contractor performance reviews.
- Risk assessment reviews.
- Emergency exercises and testing.
- Business continuity exercises.
- Safeguarding and compliance reviews.

15.2. Findings shall be used to support continual improvement and inform future planning.

16. Related Policies and Procedures

16.1. This policy should be read in conjunction with TSCG documents:

- Safeguarding, Child Protection and Vulnerable Adults Policy
- Staff Safeguarding Code of Conduct
- Health and Safety Policy
- Risk Assessment Procedure
- Incident Reporting Procedure
- Lockdown and Hostile Intruder Procedure
- Business Continuity Policy
- Business Continuity Incident Response Plan
- CCTV Policy
- ID Badge Procedure
- Prevent Procedures
- Relational Behaviour Policy
- Reflective Conduct Review Procedure
- Visitor Management Procedures
- Contractor Management Procedures
- Fire Safety Procedures

17. Legislative and Regulatory Framework

17.1. This policy supports compliance with, but is not limited to:

- Terrorism (Protection of Premises) Act 2025 (Martyn's Law)
- Counter-Terrorism and Security Act 2015
- Health and Safety at Work etc. Act 1974
- Management of Health and Safety at Work Regulations 1999
- Regulatory Reform (Fire Safety) Order 2005

- Civil Contingencies Act 2004
- Children Act 1989
- Children Act 2004
- Education Act 2002
- Safeguarding Vulnerable Groups Act 2006
- Equality Act 2010
- Human Rights Act 1998
- Data Protection Act 2018
- UK GDPR
- Protection of Freedoms Act 2012
- Private Security Industry Act 2001
- Corporate Manslaughter and Corporate Homicide Act 2007
- Modern Slavery Act 2015
- Keeping Children Safe in Education (Current Edition)
- Prevent Duty Guidance for Further Education Institutions

18. Review Arrangements

18.1. This policy shall be reviewed at the earlier of:

- Every two years.
- Following significant legislative change.
- Following a major security incident.
- Following significant organisational or estate change.