GLOBAL ACADEMY
MAKEUP • HAIR • PRODUCTIONS

VENUE INTRUDER POLICY

1. Introduction

Global Make Up, Hair & Productions Academy is committed to ensuring the safety, security, and wellbeing of all students, staff, visitors, and contractors within its premises. This policy outlines the academy's approach to preventing, identifying, and responding to unauthorized individuals—referred to as intruders—who may attempt to access the site without permission. It is designed to align with statutory safeguarding responsibilities, health and safety legislation, and the UK Government's guidance on school and college security.

Security is not only a matter of physical protection but also a key component of safeguarding. Therefore, this policy is integrated with the academy's safeguarding framework and is reviewed regularly to ensure it remains effective and responsive to emerging threats.

2. Legal and Regulatory Framework

This policy is underpinned by the following legislation and statutory guidance:

- **Health and Safety at Work Act 1974**: Requires employers to ensure, so far as is reasonably practicable, the health and safety of employees and others who may be affected by their activities.
- **Management of Health and Safety at Work Regulations 1999**: Mandates risk assessments and the appointment of competent persons to oversee health and safety.
- **Keeping Children Safe in Education (KCSIE)**: Emphasizes the importance of safeguarding and security in educational settings.
- **School and College Security Guidance (GOV.UK)**: Provides best practice for managing site security and responding to threats.

The academy also complies with data protection legislation when handling personal information related to security incidents.

3. Policy Objectives

The objectives of this policy are to:

- Prevent unauthorized access to academy premises.
- Protect students, staff, and visitors from potential harm.

- Ensure a swift and proportionate response to intruder incidents.
- Minimize disruption to learning and operations.
- Promote a culture of vigilance and responsibility.

4. Definition of an Intruder

An intruder is defined as any individual who enters academy premises without authorization, without a legitimate purpose, or who refuses to comply with academy protocols. This includes individuals who:

- Bypass reception or access controls.
- Provide false or misleading identification.
- Refuse to leave when asked.
- Exhibit threatening, suspicious, or disruptive behaviour.

5. Prevention and Access Control

The academy employs a layered approach to site security, including:

- **Controlled Entry Points**: All external doors are secured and monitored. Entry is permitted only through designated access points.
- **Visitor Management**: All visitors must sign in at reception, present valid identification, and be issued a visitor badge. They must be accompanied by a staff member at all times.
- **Staff and Student Identification**: All staff and students are issued with photo ID badges, which must be worn visibly on site.
- **CCTV Surveillance**: Strategically placed cameras monitor key areas of the premises. Footage is stored securely and reviewed following incidents.
- **Physical Barriers**: Fencing, gates, and secure doors are used to prevent unauthorized access.
- **Alarm Systems**: Intruder alarms are installed and maintained in accordance with manufacturer guidelines.

6. Staff Roles and Responsibilities

All staff have a duty to remain vigilant and report any suspicious individuals or behavior. Specific responsibilities include:

- **Reception Staff**: Verify the identity and purpose of all visitors. Challenge individuals who attempt to bypass sign-in procedures.
- **Teaching and Support Staff**: Monitor student movement and report any unfamiliar individuals to reception or senior staff.
- **Designated Safeguarding Lead (DSL)**: Coordinates the response to intruder incidents and liaises with external agencies.
- **Site Manager**: Oversees physical security measures and maintenance of access control systems.
-

7. Intruder Response Procedure

In the event that an intruder is suspected or identified, the following steps must be taken:

Step 1: Initial Assessment
Staff should remain calm and avoid direct confrontation unless it is safe to do so. They must immediately notify the DSL or a member of the senior leadership team.

Step 2: Secure the Area
If the intruder poses a threat, initiate lockdown procedures. This may include securing classrooms, restricting movement, and alerting staff via internal communication systems.

Step 3: Contact Authorities
If the intruder refuses to leave or exhibits threatening behavior, the police must be contacted immediately. Staff should provide a clear description of the individual, their location, and any observed actions.

Step 4: Incident Documentation
An incident report must be completed within 24 hours, detailing the nature of the intrusion, actions taken, and outcomes. CCTV footage should be preserved and reviewed.

Step 5: Communication
The Academy Director will determine whether parents, guardians, or external stakeholders need to be informed. Media inquiries must be directed to the designated communications lead.

8. Post-Incident Review

Following any intruder incident, a formal review will be conducted. This includes:

- Debriefing involved staff and students.
- Reviewing CCTV and access logs.
- Identifying any breaches in protocol.
- Updating risk assessments and security procedures.
- Providing support to affected individuals, including access to counseling services.

Lessons learned will be used to strengthen future responses and inform staff training.

9. Training and Awareness

Security awareness is embedded into the academy's culture. All staff receive annual training on:

- Identifying and responding to intruders.
- Lockdown, evacuation, and invacuation procedures.
- Safeguarding and reporting protocols.

Students are educated on personal safety and encouraged to report concerns. Emergency drills are conducted at least twice per year and evaluated for effectiveness.

10. Partnerships and Intelligence Sharing

The academy maintains active partnerships with:

- Local police and community safety teams.
- Local authority safeguarding boards.
- Counter-terrorism and resilience forums.

These partnerships support intelligence sharing, coordinated responses, and access to specialist advice. The academy also uses anonymous reporting tools to allow students and staff to flag concerns confidentially.

11. Business Continuity and Crisis Management

In the event of a serious intrusion, the academy's business continuity plan will be activated. This includes:

- Maintaining essential operations.
- Communicating with stakeholders.
- Coordinating with emergency services.
- Managing reputational risk.

The crisis management team will oversee the response and recovery process.

12. Policy Monitoring and Review

This policy is to be reviewed annually, before the start of each new academic year, and also following any significant incident. Reviews are conducted by the Compliance & Quality Assurance Administrator in consultation with the DSL, Site Manager, CEO and external advisors. Updates are communicated to all staff and incorporated into training materials.

Reviewed by	Compliance & Quality Assurance Administrator
Reviewed	Annually, before start of a new academic year
Last Review	29/10/2025
Review Date	30/08/2026

Reviewed: Signed: B Levy..... **Date: 29/10/25**

Benjamin Levy
Compliance & Quality Assurance Administrator