



Department
for Education

Guidance

Potential security threats and preventative measures guidance

Updated 3 July 2026

Applies to England

Contents

Crime

Terrorist attacks

Information security

Cyber security

Personal security

Chemical and biological

OGL

© Crown copyright 2026

A876

This publication is licensed under the terms of the Open Government Licence v3.0 except where otherwise stated. To view this licence, visit nationalarchives.gov.uk/doc/open-government-licence/version/3 or write to the Information Policy Team, The National Archives, Kew, London TW9 4DU, or email: psi@nationalarchives.gov.uk.

Where we have identified any third party copyright information you will need to obtain permission from the copyright holders concerned.

This publication is available at <https://www.gov.uk/government/publications/school-and-college-security/potential-security-threats-and-preventative-measures>

While it is difficult to be prescriptive regarding the security threats faced by individual schools or colleges there are certain preventative measures which can be taken according to individual requirements arising from the security risk assessment.

Crime

Criminal activity may include:

- arson
- theft
- vandalism
- trespass
- malicious damage
- graffiti
- protest
- kerb crawling/loitering
- drug dealing/drug abuse
- threats from former pupils/residents
- carrying and use of offensive weapons, especially knives

Preventative measures could include:

- CCTV to monitor and record activity within and around the estate
- integrated access control systems to control, monitor and deny access when necessary
- intrusion detection systems, for example effective perimeter fencing to protect against intruders, security lighting and security glazing, intruder alarm systems

Terrorist attacks

Currently, terrorist attacks are most likely to take the form of:

- improvised explosive devices
- gun or knife attack
- vehicle as a weapon

Other less likely forms include:

- postal devices
- chemical substances

Preventative measures could include:

- increase staff ACT awareness (<https://www.gov.uk/government/news/act-awareness-elearning>) of what to do and how to react
- effective screening of staff, students and visitors to schools and colleges for prohibited items
- public address/voice alarm systems to enable direct communication to staff, students and intruders
- effective building controls including the ability to lockdown parts of the school or college, minimising direct access to school or college buildings in a vehicle with speed bumps, warning and directional signage and vehicle blocking using barriers and structural furniture

Information security

Information security breach might include:

- the theft and unauthorised access to significant confidential information, for example exam papers
- guidance, standards and policy documents
- the unauthorised access to personal information, for example bank and credit card details, health records

Preventative measures could include:

- policies to manage and monitor access to sensitive and personal information, including restricting access to authorised users, audit trails for changes to records
- training for all staff on General Data Protection Regulation requirements and cyber threats

Cyber security

A cyber security incident might include malicious software execution resulting in:

- outages
- data loss
- costs incurred to recover associated data and access to the system

Preventative measures could include:

- ensuring all software and devices have security patches applied regularly, including anti-virus, which should be automated and only use software and operating systems that are supported
- ensuring the network is securely configured, turn on firewalls and follow best practice for end user devices
- performing regular data backups, ensuring they are stored independently and/or appropriately protected
- understanding your reliance on IT and have a business continuity plan to enable you to operate without it
- regularly review policies to ensure cyber security standards are maintained
- implementing content filtering to prevent inappropriate content access
- verify email senders, do not circumvent your security processes
- having effective policies to educate staff and pupils on your cyber security
- consider looking at National Cyber Security Centre advice for small and medium sized organisations (<https://www.ncsc.gov.uk/section/information-for/small-medium-sized-organisations>) for further information

Personal security

Personal security breach might include:

- physical attack
- intimidation
- bullying
- lone working (staff, pupils and visitors)

Preventative measures could include:

- banning individuals who pose a threat to staff and pupils
- effective reporting and follow up of incidents and involving police if necessary
- lone worker risk assessments and laid out procedures to alert others, issue of personal attack alarms

Chemical and biological

Chemical and biological threats might include:

- throwing of a corrosive substance/acid to cause harm or targeted chemical attack

Preventative measures could include:

- safe and secure storage of chemicals in line with industry standards
- safe handling training for staff and pupils prior to use in lessons
- rehearsed response in line with local emergency/disaster plans and remove guidance





All content is available under the [Open Government Licence v3.0](#), except where otherwise stated



© Crown copyright