# Security in Schools

## CFPA-E Guideline No 8:2016 S

CFPAEUROPE


## Foreword

The Security Commission of the Confederation of Fire Protection Association Europe (CFPA-E) has developed common guidelines in order to achieve uniformity of interpretation of protection recommendations in Europe and to give examples of acceptable solutions, concepts and models. The CFPA-E aims to facilitate and support fire protection and security aspects across Europe.

The market imposes new demands for quality and safety. Today fire protection and security aspects form an integral part of a modern strategy for survival and competitiveness.

The guidelines are primarily intended for management. They are also aimed at the rescue services, consultants, safety companies and the like so that, in the course of their work, they may be able to help increase fire safety and security in society.

These guidelines have been compiled by the Guidelines Commission and are adopted by all fire associations in the CFPA-E.

These guidelines reflect best practice developed by the members of CFPA-E. Where the guidelines and national requirements conflict, national requirements must apply.

## Content

# 1 Scope

This document assists those responsible for security in a school (e.g. school managers, school security personnel, authorities, etc.) as well as those wishing to see that students may learn in a safe and productive environment.

The scope of the document is to provide information and guidance on security aspects in schools, including measures to minimise risks for physical property damage and for asset protection.

The guidelines focus on security risks in schools consequent upon of any kind of damage, improper use, theft, and loss of property. Health and safety issues, personal injury, information security breaches and interpersonal violence are not within the focus of the guidelines but of course they are important aspects to be taken into account by the responsible persons.

While the guidelines can be applied to any school, this document was developed with typical "community schools" in mind, i.e. those institutions that are populated by students during daytime, may become a place for meetings and events in the evening, and are routinely closed during the night.

The risks and measures depend on the use of the school, so for different kinds of school, these guidelines should be adjusted to cover additional aspects, not mentioned herein that would need to be taken into account.

Furthermore this document is intended to provide best practise for existing schools. The outlined principles can be applied to the design of new schools but through assessment of the risks and possibilities at the planning stage, alternative, more cost effective and more practical solutions will be possible.

Numerous schools in every European country are located in old buildings and the security issues deriving from structural vulnerabilities are usually of great concern to the authorities. Economical difficulties frequently lead to schools suffering a lack of investment.

It is the aim of this document that communities and school managements acquire an appreciation of the risk management principles that are common practice in today's business and public sectors, i.e. the application of, in particular:

- To conduct a thorough risk analysis
- Defining the risk management aims and concept
- Describing the risk measuring method
- Highlighting the countermeasures to be adopted
- Identifying the priorities
- Setting deadlines.

This document is primarily intended to assist in highlighting some of the major risks and the possible countermeasures.

# 2 Risks

## 2.1 General

The whole school, staff and pupils, should have an awareness of safety and security issues.

In order to manage the risks, they must first be identified, then assessed and prioritised. The risk identification and assessment should not be a single event, but it must be kept under review particularly as the operating environment changes and has to be revisited periodically. A so-called safety and security walk should be done regularly in the school by the individuals responsible for security and safety aspects. Identified threats and safety related findings are to be written down to a risk analysis table in the security plan. All other safety- and security related findings should be recorded in writing.

The risk identification should consider the risks relating to the people and the property within the school as well as the buildings themselves. Examples concerning the risks relating to a school are illustrated in the Figure 2-1.

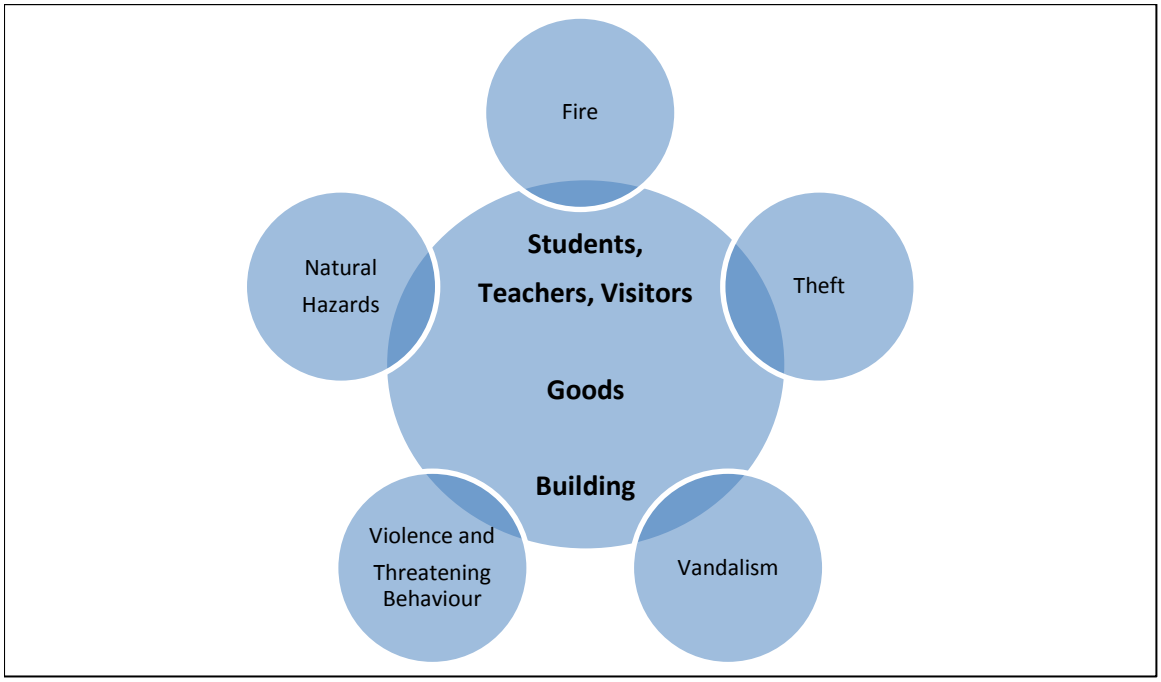


Figure 2-1 Risks relating to a school

A school that is seeking a good safety culture will use “near-miss” monitoring and teach it to its staff. A near-miss reporting should to be made as easy and convenient as possible. Near-misses are added to the risk analysis, and evaluated and corrective actions have to be implemented. The findings should be used to illustrate risks and solutions during staff training. Risk assessment is a starting point for the further improvement.

This requires commitment from the management and employees, flexible organizational culture and learning from mistakes. There are several risk assessment templates and models that schools can use in their own work.

In the following paragraphs different risks are described. The presence of large numbers of people and the particular social climate of the area severed by the school are factors to be taken into account.

## 2.2 Theft and Burglary

As well as the school’s property the property of those legitimately on the premises is at risk. Theft and robbery are often preceded by observation from the perpetrator, so strange behaviour and/or unauthorized persons and their acts should be monitored and reported.

The risk of theft can be aggravated by the exposure of, and easy access to, valuable assets.

## 2.3 Fire

Fires (fire as well as smoke and heat) may have disastrous effects on people and valuable assets and buildings. The following factors pose the risk of fire development and spread:

- Negligence (e.g. by unsuitable location for heaters, unsuitable waste disposal)
- Defective (or obsolete) electrical systems and equipment
- Activities prone to cause fire (welding, soldering, hot-glueing, abrasive cutting, using kilns, operation of laser printers, etc.)
- Radiant heat by lights
- Handling flammable substances (including the risk of auto ignition)
- Open flames (candles, for example, during Advent in the foyer).

In schools, special fire risks may be presented by:

- Technical work rooms
- Laboratories
- Kitchen
- Electrical installation and equipment

Fire might also be caused by arson. In a school building arson often is lit in the basement, in the roof void, in the waste disposal bins, or in a waste pile left against the wall.

Fire risk in schools requires to fulfil prevention measures concerning building design as well as building structure. Access for the fire brigade, fire compartment, fire prevention measures linked to fire risk and to escape the facilities etc. are to be considered. All these aspects should be considered through conducting fire risk assessment in each location.

*Remark: The guidelines "Introduction to Qualitative Fire Risk Assessment" (CFPA-Guideline 4/F) are dealing on this as a main topic.*

## 2.4 Vandalism

Vandalism against property can cause significant economical and/or personal injuries. This type of risk will often influence to the image of the school or

Vandalism in the broadest sense refers to deliberate damage or intentional destruction of a third party's property; it is common in different forms. Vandalism directed at buildings and/or assets, includes graffiti as well as physical damage and arson.

Vandalism is an offence to which there can be different underlying motivations. As well as rebellious behaviour vandalism may arise from the mental imbalance of the offender.

## 2.5 Violent and Threatening Behaviour

A dangerously behaved third person can come in the school area or inside the school and through his/hers actions and behaviour cause panic and disorder among the students and personnel. In the risk identification should also be noted that a student might also behave in such a violent or threatening manner.

It should also be noted that a mere threat can also lead to uncertainty and insecurity in the school. The threat can be presented in many ways, for example, on the Internet, as writing on the wall of the school, on a phone call, on a paper found in the school facilities, or just mentioned by a friend. Most of the threats are made in malicious purposes, and often by a student in the school. In all cases the threat must be taken seriously and addressed in accordance with the instructions of the school.

## 2.6 Natural Hazards

At worst, floods, storms and earthquakes can cause significant property damage and even threaten human life and health, as well as interfere with school activities by disrupting electricity, communication and transportation links. Even a cold and snowy winter may pose a threat and lead to serious disruptions in traffic and technical systems.

# 3 Protection Measures

## 3.1 General

The careful risk assessment is essential to control loss through crime and criminal damage and match solutions to the challenges presented by a school. In a school these challenges are unique – quite different from say an industrial or retail premises. Above all, arson and vandalism can be a major security challenge in many countries. Traditional, "tried and tested" security measures, such as perimeter fencing, physical devices, lighting, intruder alarm systems and video surveillance systems (VSS) are all applicable to a school but they need to be employed in a more selective and "tailored" way than a typical site requiring protection. Additionally, in common with other locations, removal/reduction in vulnerable assets in the first place should be considered ahead of potential security solutions and the strength of security management, particularly in relation to vandalism/arson, is more important than generally the case.

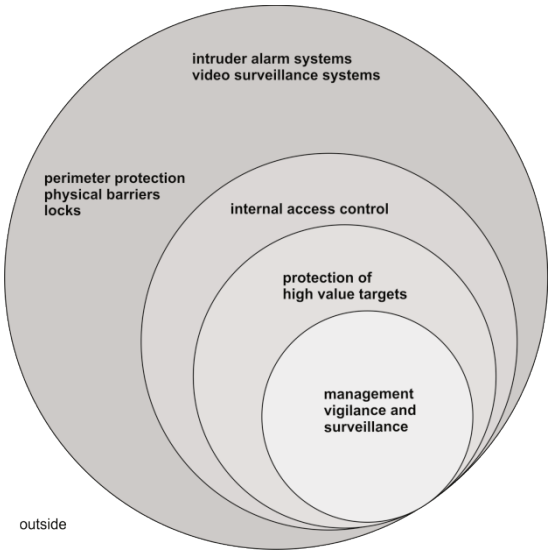


Figure 3-1 Onion skin strategy

Only well-coordinated overall prevention can achieve an adequate level of protection which makes the risk of loss, damage, destruction of property or interruption of school business calculable. When implementing the protection strategy the various operations of the school need to be distinguished.

Optimum protection of a school is usually achieved by tailoring the protection levels to these operations (classrooms, laboratory, stores, gymnasium offices, etc.).

A highly effective security strategy, often referred to as 'protection-in-depth' or the 'onion skin' strategy, layers security in concentric rings of measures as represented in Figure 3-1.

The protection strategy should be agreed with any insurer (and, if applicable, with the authorities as well) and this will help to avoid avoidable costly security upgrades.

The protection and surveillance measures suitable for schools are summarised and explained below. Mechanical safeguards should constitute the protection basis; they should be supplemented by electronic, organisational and personal surveillance measures.

National and local requirements may overrule European recommendations as named in the following.

The probability of a property theft can also be affected through own operations, so valuable equipment and money and sensible products (as e.g. chemicals) are to be kept out of the sight and handbags and wallets in a locked cabinet. Someone might try to steal school´s or persons property pretending to be from the maintenance, so company logos in the workwear cannot be trusted.

## 3.2 Mechanical Safeguards

Mechanical safeguards can be installed to protect the building on the one hand, and the assets within on the other. Mechanical safeguards must not be neglected, even when buildings or objects are protected by electronic surveillance. Mechanical safeguards and electronic security technology complement one another. Replacing mechanical safeguards with intruder alarm technology is not acceptable judging by the experience of burglary insurers and the police.

Mechanical measures are the basic prerequisite for a viable protection strategy as they effectively prevent potential perpetrators from easily entering the building and/or a protected area and gaining access to the school's assets. Moreover, they make casual or opportunist theft more difficult.

A member of staff with sound practical knowledge of basic security techniques should be entrusted with responsibility for the continued effectiveness of both the mechanical and electronic security technology. He/she should have access to the school management at senior level.

### 3.2.1 Walls

Building features such as recessed doorways, concealed areas and low roofs may be favoured by architects and planners but they create difficulties for the security designer. Flat roofs in particular will form both a security and safety hazard, especially where younger intruders are concerned, as schools' experience shows that to children, gaining access to the roof is a challenge and an adventure. Such roofs can contain dangerous and vulnerable features such as glazing. Climbing aides should be eliminated as far as possible but "aggressive" anti-climb solutions that could injure a child cannot be considered. Electronic detection solutions may ultimately be the only serious option.

Computer or information technology (IT) equipment is often the main target for thieves - laptops, tablets, PCs, servers, 'whiteboards', projectors, monitors, etc. Wherever possible, stores and IT centres should be located in an internal part of the building with solid masonry walls but without external doors or windows.

### 3.2.2 Doors

All accessible doors must have strong locks, meeting the sensible requirements of the relevant standard (EN 12209). The locking cylinders should confirm with EN 1303 Building Hardware – Cylinder Locks – Requirements and Test Methods. The following classes should be met at least:

- Durability: class 5
- Locking security: class 5
- Attack resistance: class 2
- Pulling protection: class 2
- Torsion protection: class 2

Emergency or panic exit doors should conform to EN 179 or EN 1125 plus alarm devices that operate on a 24 hour basis.

Note: Doors in escape routes must generally open easily from inside and with a single push across the full width at any time. For further information cf. Guidelines CFPA No 2/F and take into account national regulations.

Recessed doors etc. might be improved with fixed or opening barriers and gates provided they are not impeding a fire exit.

External doors to target locations such as information technology (IT) equipment stores need to be to a very high intruder resistant standard. All internal doors giving access to such assets need to be to similar strength. Preferably the doors protecting such target locations should be tested and approved burglar-resistant doors featuring at least class RC 2

The main characteristics of a tested and approved burglar-resistant door include:

- Stable design of door leaf
- High-quality braces
- Sophisticated locking system (in general multipoint locks)
- Burglar-resistant door plate
- Lock cylinder, protected against unlocking techniques, e.g. drilling and pulling, and resistant against picking and other manipulation methods
- Construction elements of potential weakness (e.g. glazed panels) are as solid as the entire door element
- Competent installation of the entire assembly (anchoring to the brickwork) in line with manufacturer’s instructions.

If no burglar-resistant doors are installed then (e.g.) additional locks and braces/lateral enforcements should be fitted to the existing doors to increase the protection level.

When upgrading a door or specifying a new one, it is vital to see to it that the old design and the new security elements are compatible. Any security upgrades must not obstruct escape and evacuation routes or render them ineffective. This must be taken into consideration during the planning stage.

### 3.2.3 Windows

All ground floor level and other easily accessible windows must have strong locking and glazing (e.g. windows, doors) should contain glass conforming to EN 356:2000 Glass in Building. Security glazing – resistance to manual attack, and should meet at least category P4A. Where necessary, as a compromise steel security shutters should be installed. Shutters are best fitted on the inside but if there is a problem with vandalism and glass breakage, the shutters may have to be external, which unfortunately weakens their value.

Windows in intensely targeted locations such as information technology (IT) equipment stores need to be permanently shuttered or eliminated. In such situations, windows without burglar-resistant features can easily be overcome with simple tools in a matter of seconds. This is why tested and approved burglar-resistant windows of at least class RC 3 (EN 1627) should ideally be installed.

The main features of a tested and approved burglar-resistant suitable for target locations window include:

- Stable construction of leaf and frame of the window
- Attack resistant glazing
- Sophisticated fastening of glazing to leaf
- Wraparound burglar-resistant ironwork in combination with a lockable handle
- Competent installation of the entire assembly (anchoring to the brickwork) in line with manufacturer's instructions.

If burglar-resistant windows cannot be installed, the protection level of the windows needs to be enhanced by additional, tested and third party certified locks, for instance, or replacement of security furniture or, if possible, security glazing.

In terms of protection, domelights should be treated like windows. This also applies to glazed areas of the roof, (northlights, lantern lights, etc.). When planning the safeguards, special attention must be paid to smoke and heat exhaust ventilation systems or other ventilation openings. These openings must usually comply with specified technical requirements while at the same time, may need to be incorporated into the detection capability of the intruder alarm system (cf. 3.3.1).

### 3.2.4 Other Openings

Other openings that allow access to highly sensitive/targeted locations (openings e.g. required for ventilation and air conditioning systems) also need to be secured by e.g. bars. Openings that are not used should be closed permanently by e.g. bricking up.

The maximum clear diameter of wall openings and spacing of bars should not exceed 12 cm and/or be reduced to that size. In general, openings with the following dimensions can be exploited by intruders:

- Rectangle of 400 x 250 mm
- Ellipse of 400 x 300 mm
- Circle of 350 mm diameter.

### 3.2.5 Roller Shutters

Conventional roller shutters often have limited burglar-resistant qualities. The installation of tested and approved roller shutters according, at least, to RC 3 (EN 1627) might be a solution not only for targeted stores but also for areas which have to be mechanically protected only outside opening hours.

### 3.2.6 Fencing

The value of perimeter fencing should not be underestimated – many school intruders are young and far from being hardened criminals. Security fencing is effective in deterring such uninvited visitors. Strong fencing to the site, or around the buildings, forms a secure environment both inside and outside hours of occupation. The gates within the fences must be to the same quality and height as the fence. Where necessary agreement must be reached with the fire and police authorities as to how they will gain access if required outside school hours.

## 3.3 Electronic Surveillance

### 3.3.1 Intruder Alarm

The larger schools at least will need to have intruder alarm protection. Intruder alarm systems (IAS) and intruder and hold-up alarm systems (I&HAS) should be designed in such a way that intrusions/attempted intrusions are detected and notified as early as possible. In this context, mechanical safeguards and surveillance by an IAS, taking into account the expected intervention time, need to be harmonised in such a way that upon an alarm, intervention forces are able to arrive at the scene before the perpetrator has managed to overcome the safeguards. It is vital, that the whole intervention cascade is thoroughly planned and arranged. The interaction of electronic and mechanical measures needs to be fine-tuned to so that false alarms are avoided as far as possible.

Detectors should cover external doors plus all rooms accessible from the outside, all high risk rooms, staircases and all circulation areas. Arrangements for a speedy and effective response must be made. Acoustic systems that allow the monitoring centre to listen to sounds being made inside the buildings via microphones are often effective in schools since the interior does not usually contain much absorbent material.

Intruder control and indicating equipment – the IAS' brain – must be installed in the monitoring range of an intruder detector and a place which is not generally accessible to unauthorised personnel. It needs to be installed in such a way that it, or any displayed indications, cannot be observed by unauthorised people within or outside the protected zone, and such unhindered access to it is prevented.

In the case of intruder control and indicating equipment featuring hold-up detectors (see below), it is important to ensure that the perpetrator is not made aware of the activation of a hold-up alarm device through visual or audible indications made by the control equipment.

A major challenge for those designing IAS in schools is that, without allowing parts of the school to be left unoccupied without intruder alarm protection, the various parts of the school may need to have the alarm protection set at different times. For example, the classrooms and equipment stores might be ready to be set first followed later in the evening by the offices, then the sports facilities and finally by rooms used by the local community for meetings or adult education. In addition, these zones will of course all be visited by cleaning and maintenance teams during the protected period. This requires careful technical design to ensure that each zone is capable of being set independently in a safe way (i.e. in a way that suppresses false alarms) and that a zone cannot be entered in error during the period the protection is set. This also needs to be taken into account when designing emergency escape routes and the movement of people (e.g. local citizens unfamiliar with the layout) who may be on the premises outside normal school hours. Ideally the securing of parts of the school that have been in use outside working hours should be assigned to security personnel.

A hold-up (sometimes termed 'panic' or 'personal attack' alarm) device can be provided for the use of designated staff in the event of a serious incident. These can be stand-alone systems or are, more usually, incorporated within an I&HAS. They are used to silently alert police or a security response service via an Alarm Receiving Centre (ARC), of the need for an emergency response e.g. threatening behaviour, assault or robbery (theft with actual or threatened violence). This measure must not be permitted to activate an audible warning device. These are permanently live devices which are activated by users simply pressing a switch, or inputting a special code to indicate 'duress' when unsetting all or parts of a system. In some jurisdictions additional conditions are placed on the inclusion of duress facilities due to the number of false alarm calls they generate through user error.

Hold-up facilities can be a crucial measure in certain types of school but because of the resource implications to those responding, (often the police), they should only be proposed if a security risk assessment can demonstrate a real risk at the school of an incident requiring their use. The assessment should outline the required type and best location for any hold-up devices, e.g.:

- use of dual action hold-up buttons (to prevent accidental activation)
- siting hold-up buttons away from the immediate area where an incident is expected to occur (to allow for their safe use by persons viewing the scene but not directly involved)

Consideration should then be given as to who is expected to respond, how quickly and how the request for response will be communicated. In a few cases, on-site security guards may respond, but in other cases a police response will be received (local and national variations apply).

Alarm confirmation or verification techniques designed to manage-out false alarms can be incorporated. For example, the ARC may make a telephone call to a designated number at the school to have the alarm confirmed as genuine or sounds and/or video images from the location of the device can be transmitted to the ARC.
Alarm systems must be certificated and the installer must be accredited by a competent inspection body. Often these formalities are made mandatory by the local or national police. The certification will usually evidence conformity with one of the grades in the European standard EN 50131 - Alarm systems - Intrusion and hold-up systems. It is the responsibility of the installer and/or the school to identify the grade of the system (recommendation grade 3 or higher) deemed to be required according to a structured risk assessment. Guidelines on carrying out this risk assessment are found in EN 50131-7 Application Guidelines.

### 3.3.2 Intervention

Alarm activations of intruder and hold-up alarm systems can only be effective if they lead to suitable intervention measures. In most schools there is a caretaker or site manager living at the location and this individual will be briefed to liaise with the responders (e.g. police or security personnel) on their arrival. At smaller schools, such as primary schools, there may be no one on the premises outside normal operational hours. For these schools it will be necessary to agree intervention measures and nominate school key-holders unless keys are held by the responding service. In order to ensure the swift and effective operation of the intervention team in the case of an alarm activation, intervention plans need to be formulated in advance.

The school, the security company (if applicable) and, where possible, the police should agree how the intervention will be made on arrival at the premises in line with prioritised actions designed to protect school property and personal safety. These procedures need to be documented. It is vital to regularly check all data recorded in the intervention measures to see whether they are still up to date since telephone numbers and names of contacts etc. may change.

### 3.3.3 Access Control

Access should be restricted during hours of operation. If there is a secure perimeter, then it is best practice, at a suitable time in the morning, to secure all gates apart from one and channel visitor access via a single, restricted, path. Visitors should be able to follow a clearly marked route and find themselves in a supervised reception area where they can be "screened" before being handed over to the custody of a staff member. The reception area should be staffed or supervised at all times with access into the main school controlled through use of access control systems (ACS) and/or remote controlled locking. The ACS is considered separately from the intruder alarm system and provides security for assets that are not monitored during normal business when the IAS is deactivated. Access to rooms that require a higher security level are ideally managed by an ACS. These include high risk stores, server and IT rooms, laboratory etc. ACS mainly meet organisational aspects. If there is a need for physical security, motor-operated locks and/or self-locking electromechanical locks are necessary in contrast to electrical door openers only.

The ACS needs to be configured in such a way that access authorisation and keys issued (including keycards or mnemonic codes such as combinations of numbers or letters) are assigned only to responsible persons and it is vital that these privileges are kept up to date. This makes it possible to identify and record with accuracy when someone enters or leaves a room, which access device he/she is using and who is the “owner” of that device.

Visitors should be required to display a badge whilst they remain on the premises and unknown persons not wearing a badge should be challenged. Pupils' recreational areas should be within the secure perimeter.

Subject to preservation of approved safe emergency escape, all other external doors, and strategic internal doors, should have security during the working day which, ideally, should be in the form of an ACS. Outside working hours external doors should be secured with high quality burglar resistant locks as the average access control system is inadequate against brute force and use of tools where intruders can work unobserved.

Careful planning of the arrangements and controls is essential if the buildings are used for community purposes (e.g. school clubs, adult education, sports, etc.) to minimize the impact on good security. This requires close attention to (e.g.) internal layout and external access so that the users do not

compromise the security of the school assets and other users. Space made available to community users should be limited and physically separated from the remainder of the selected building.

Security patrols outside working hours, either visiting at variable times or permanently present, may be necessary. Large schools with a record of serious disruption/aggression during school hours may require the presence of security staff during the school day.

### 3.3.4 Video Surveillance Systems

A coherent rationale must exist if installation of a Video Surveillance System (VSS) is contemplated. VSS should not be automatically regarded as a *substitute* for physical security and/or an intruder alarm system. At the outset ask:

- Is VSS necessarily the best, or only, solution?
- What is it we need to see?
- Why do we need to *see* it?
- Do we need to see it as it happens?
- Who will observe the images and where?
- What response is required to events observed?
- Who will make that response?
- Do the images need to be captured on a recording device?
  - If yes, is the resolution of the stored pictures adequate?
  - If not, is the response really and adequate arranged?

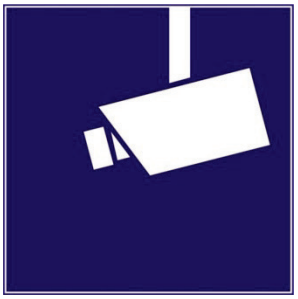

Figure 3-2 Sign informing on video surveillance

A threat analysis needs to be completed in terms of likelihood and impact and there should be a written objective for the task(s) that the system is required to perform. This Operational Requirement (OR) needs to be clear and as detailed as necessary for all stakeholders to understand what is required. Ideally, the OR will be drafted with the assistance of a VT expert or consultant as it is important that it uses the *terminology* that the VT sector of the particular country will recognise. Alternatively the terms in use in the applicable international standards (EN 50132/IEC 62676) should be employed. These include for example:

*Observe:* (25 % screen height)*
Some detail can be seen e.g. distinctive clothing.

*Recognise:* (50 % screen height)*
Viewer is likely to be able to judge if an individual is someone they have seen before.

*Identify:* (100 % screen height)*
Sufficient picture quality and detail to identify an individual.

*space on screen occupied vertically by a 1.7 m tall figure


Figure 3-3 Examples for image resolutions

Obviously the ongoing costs of a system that is continuously monitored by staff or security personnel are substantial in contrast to a system with image recording alone. If the system is to be monitored only at selected times, can this be justified in relation to the cost of the system? Will such selective viewing be rigorously managed?

National data protection provisions and privacy legislations must be observed. Suitable warning signs (cf. Figure 3-2 for a typical example) must be placed in prominent positions.

In some countries there may be laws or regulations that only special areas (e.g. storage rooms for high value assets, laboratories) may be observed by VSS.

An option that may be suitable is to install remotely monitored VT known also as 'Detector-Activated VSS (DA VSS). 'Secure areas' are defined within which a change (e.g. movement) is detected through connection of movement detectors or Video Motion Detection. Notification of this event, along with the associated CCTV images, is transmitted to an on-site security post or a remote monitoring centre. A voice warning ('audio challenge'), audible in the secure area, may also be triggered to deter trespassers or intruders.

'Video analytics' performs analysis on video information within selected zones in a more "intelligent" way than simply registering movement. It is capable, for example, of detecting loitering; e.g. persons, objects or vehicles remaining in an area for a suspicious time; removal detection: detects when an object has been removed; unexpected/unwanted behaviour e.g. detects and tracks for the observer people or vehicles moving in the wrong direction, erratically, excessively fast.

Use in security applications. In addition, in some countries, national standards or codes exist for 'DA VSS'.

Video material can provide useful information for the police investigation after an incident but national guidelines for format and image quality must be observed.

### 3.3.5 System Certification

VS systems must be certificated and the installer must be accredited by a competent inspection body. These formalities may be made mandatory by the local or national police. The certification will usually evidence conformity with one of the grades in the European standard EN 50132/IEC 62676: CCTV/Video surveillance systems for use in security applications. It is the responsibility of the installer and/or the school to identify the overall grade of the system deemed to be required according to a structured risk assessment. Guidelines on carrying out this risk assessment are found in the Application Guidelines of the European standard.

## 3.4 Organisational Aspects

### 3.4.1 General

Aside from the mechanical safeguards and electronic measures (e.g. intruder alarm system and video technology, access control), organisational measures constitute the third element of the security system.

Organisational measures include instructing personnel on potentially threatening situations, administering keys and allocating access authorisation, drawing up an inventory of valuable assets and developing evacuation and lock-down plans (cf. 3.2.2). Moreover, clear procedures for operation of mechanical safeguards and electronic surveillance measures need to be defined. The best security system is useless if it is not properly operated and/or activated.

In order to implement security policies, it makes sense to appoint a member of the senior staff to have overall responsibility for security and report directly to the school's head. He/she may gather a group to identify and assess potential risks and define appropriate protection measures. In addition an individual with clear responsibilities in an emergency situation should be appointed.

Ideally the school will employ a caretaker who ensures the security implementations are maintained fully and effectively on a day to day basis.

A reporting system should be established through which staff and pupils may report any security issues they become aware of.

### 3.4.2 Keys and Key Authorisation

Whenever a key is issued, this must be logged, which can be done manually in a keys' log or a so-called key management and/or transfer system. Access authorisation and key allocation should be granted according to staff responsibilities. It is vital to ensure that unauthorised individuals are not allowed access to keys, even for a short while (danger of copies being made). To this end, keys need

to be locked away in a suitable key cabinet (recommended: Product following EN 14450 or EN 1143-1) and be located in a monitored area.

Only assigned staff should have the right to use a master key; they are also responsible for its safekeeping.

In general, master keys should only be issued to security personnel in case of an emergency. It may be necessary to place restrictions on the issue of keys to cleaning staff.

### 3.4.3 Contractor Service Providers

Where contractors are hired such as cleaners, transport and/or security personnel, special requirements need to be taken into account.

Consequently, security companies that provide security and supervising personnel should be certified in line with national standards or rules. Companies may offer other services such as gatekeeping certified in line with national requirements for security services.

The responsibilities entrusted to the security personnel need to be defined clearly and unambiguously and should be checked for proper implementation.

The security company employed must have adequate third party liability insurance that covers potential loss. The terms of this insurance must be agreed with the school insurer.

### 3.4.4 Contingency and Evacuation Plans

Contingency and evacuation plans need to be tailored to the nature of school operations and it may be appropriate to involve the responsible fire authority. The plans need to be rehearsed regularly in accordance with the national regulations.

## 3.5 Special Aspects

### 3.5.1 Exterior Lighting

Tailored security lighting is valuable in deterring intrusion and criminal damage. Local illumination (lamps, floodlights) increases the risk for a perpetrator of being detected and recognised and consequently apprehended. Moreover, exterior lighting may be effectively combined with video surveillance technology. Investment in this needs careful planning to match the unique conditions at the school location.

For example, good lighting is particularly effective in areas of the school site which are easily visible from nearby houses or roads. The facades of these buildings should be bathed in a good and even overall level of light, subject to the control of excessive light pollution affecting neighbours. Uneven lighting assists intruders by providing light to work with and shadows to hide in. However, lighting provided in an accessible part of the site that is not overlooked can have the counter productive effect of attracting undesirable gatherings.

Carefully located, purpose designed security fittings should be used and vandal resistant products are available where required. Reliable switch-on when light levels fall must be assured. This is usually automatic by timer and/or photocell. Poor quality, self-contained sensor activated (passive infrared) products should be avoided as they can be erratic and are easily interfered with.

Any supplementary lighting required for the optimum operation of a VT system needs to be specified in conjunction with the VSS company or consultant.

### 3.5.2 High Value Assets and Sensitive Locations

High value assets such as IT equipment and sensitive operations such as the Chemistry lab and the Video lab need focussed security in designated stores and zones.

Measures to be considered include:

- personal computers (PCs) should be anchored down with proprietary security brackets or cables.
- all valuable items should be security-marked using a method that cannot easily be removed e.g. chemical etching or engraving.
- ceiling projectors need to have strong fixings and, preferably, a proprietary alarm device sounding an alert when interfered with.

- laptops should be locked in a secure room with intruder alarm protection outside school hours.
- all critical doors to be locked or subject to access control to combat "sneak thieves". This includes school hours as well as times of partial occupation.
- establish security procedures so that equipment is never exposed in an insecure room or next to glazing. Provide security cupboards or cabinets if necessary.

### 3.5.3 Car Parking

Ideally, a dropping off point for pupils arriving by car and school bus should be provided.

Separate parking, limited to staff use, preferably with access automatically controlled (e.g. fob/card reader controlled barrier) should also be provided if space allows. This facility will ideally be overlooked by occupied parts of the school and/or be viewed by monitored VSS and it must be suitably lit. If the local crime rate demands, the car park should also have a secure perimeter.

Entry to the main school site for staff using their car park should not differ from the security set-up for staff arriving on foot but if a separate entrance is provided for convenience it should be no less secure than the main entrance.

Allowance must be made at larger schools for emergency vehicle access including adequate space for manoeuvring.

### 3.5.4 Bicycle Parking

Bicycles left in unobserved sheds are certain to fall victim to theft. Secure bicycle parking must be provided consisting of steel stands allowing owners to employ their own cycle locks. The location needs to be suitably lit and in view of occupied parts of the school and/or viewed by monitored VSS.

### 3.5.5 Violent and Threatening Behaviour

Health and safety requirements and good practice extend to the exposure of staff and pupils to threat, violence and assault on, or close by, the school premises.

This may be a low frequency event but the consequences are serious enough for the school to give time to developing a strategy and action plan.

If a receptionist is employed he/she is on the "front line" and some thought should be given to his/her physical protection and fall back strategy if an incident seems unavoidable. Staff in the reception area should have access to fixed or wireless hold-up devices that alert managers to any potentially dangerous situation developing. If there is a CCTV installation at the school, operation of a device may be made to display images of the scene to school managers and this could be accompanied by live sound. These safeguards can be replicated at any other location considered a focus for trouble e.g. an interview room or head teacher's office.

Staff should receive thorough training in the use of alarm devices so that are not used casually but only in circumstances of clear threat. This is particularly important if the devices are also linked to the outside world (e.g. security company) as excessive, unjustified use will damage the credibility of the alarm system and may involve costs for pull-outs of police staff or security personal.

In extreme circumstances, vulnerable (e.g.) inner city schools may have "lock down" action plans for implementation in situations of near-by threat whereby all openings in the secure perimeter are quickly sealed and children are brought indoors and supervised.

Further details are very often available from the authorities responsible for schools and/or the relevant national body. Information is also available from various European and international sources (for examples cf. Annex A).

### 3.5.6 Vandalism and Arson

Vandalism and arson can be the result of different, even minor, underlying motivations, e.g. rebellious behaviour or mental imbalance of the offender. Therefore all responsible persons as e.g. teachers must be aware of the problem and always be ready to take appropriate action.

A school wide policy should – as far as possible – describe procedures how to deal with such incidents. A process of permanent awareness and improvement to reduce risks should be implemented.

In addition the staff should be watchful if unknown visitors are on site. These persons should be challenged actively either to help them or to avoid any damage or losses.

The different risk scenarios and action plans should be discussed with trained and qualified personnel. Please refer to the CFPA Arson Document (Guidelines No 1S) and CFPA document Prevention Arson – Information to young People (Guidelines No 8F) for further information.

All protection measures described in this document measures should be considered to minimise the risk of vandalism and arson.

## 3.6 Fire

The risk of fire (fire, heat, smoke and fire gases, etc.) in schools poses a serious risk due to the possibilities of personal injuries, but also due to the damage resulting from partial or total loss of assets and the building.

Preventive fire protection measures are able to mitigate the fire risk in schools effectively. Intelligent investments in structural and technical features in combination with organisational measures ensure safe operation of schools. This not only applies to new buildings; suitable measures are capable of realising improvements in old buildings. Pursuant to the relevant legal standards of the national or local authorities (regional building codes, industrial health and safety laws), the operator is obliged to determine and implement the necessary precautions.

Effective fire protection can only be achieved by a holistic fire protection concept tailored to the respective school. This brings all individual protection measures into line. A fire protection concept includes measures of preventive fire protection (with individual structural, system-related and operational/organisational elements) as well as fire defence that consist of rescue and fire-fighting operations. All these necessary components interact with each other.

In the following, there are some special aspects listed with regard to risks and appropriate organisational measures typical for schools.

**General**

General cleanliness, orderliness and effective management of waste disposal ensure the daily fire safety of the school.

**Technical work rooms**

The dust near machinery and electrical equipment and packaging material in the work rooms can be a source of fire, as well as waste containers that have not been emptied or emptying the bins of fire hazardous waste elsewhere than in a lidded, non-combustible container. Fire risk is very high at work that causes sparks or when using a gas torch, flame or a hot-air blower. Anyone who is dealing with the hot work has to be aware of the fire risk. The class of the technical work is to be built taking into account the fixed hot work requirements. If it is necessary to do hot works elsewhere, the requirements of the temporary hot work instructions has to be taken into consideration.

**Laboratories**

Generally, the hazards encountered in laboratories are low to moderate because of the relatively small quantities of materials being involved. However, some facilities may present serious fire hazards from:

- Excessive quantities of flammable or reactive chemicals
- Uncontrolled ignition sources
- Inadequate procedures or equipment for handling hazardous materials

Schools need safe procedures for laboratories in order to control fire risks

In order to maintain business continuity is vital that in all laboratories an appropriate fire safety strategy is developed with staff receiving detailed instruction in the actions that they should take in an emergency. (more information Guideline Nº 28 Fire Safety in Laboratories:2012 F)

**Kitchen Area**

The Kitchen (which may include its storage area(s) and cold room(s)) is the part of a school which is the area of high hazard and it is dealt with thoroughly in the Guideline Nº9 Fire Safety in Restaurants:2012 F. It is essential that if fire breaks out in a kitchen it cannot spread to other parts of

the premises, and particularly not to the escape routes, hence the need for effective compartmentation.

The main fire hazard arising from food preparation is the use of heated fats and the risk of over-heating the fat due to operator error or failure of the thermostat in equipment. This can be particular problem if the kitchen is unattended.

**Electrical Installation and Equipment**

The safety of students, staff and others using electrical equipment is important and there are legislative requirements that must be followed to ensure electrical safety. All electrical equipment must be appropriate for the activity and conform to National Regulations.

Electrical Installations:

To ensure safety of electrical installation, the following measures shall be implemented:

- Inspection and test of electrical installations regularly conducted by a competent contractor
- Portable appliance testing undertaken at interval suitable for type of equipment and frequency of use by a competent person
- Any additional electrical appliances brought on to site by staff or pupils included in inspection/ testing regime
- Programme of remedial works arising from inspection and test recommendations
- Any damage noticed to sockets is reported and communicated to site manager
- Access to electrical equipment/switchgear restricted to authorised personnel ( e.g. contractors)
- Electrical and plant rooms are free of all combustible storage
- Visual check of equipment by staff before use / issue to pupils. Any damaged or defective electrical equipment taken out of service and removed from the area for repair or disposal.
- Staff to ensure sockets not overloaded and minimise use of extension leads

Boilers:

- Boilers are serviced regularly by a competent contractor
- The boiler room is kept clear of all combustible storage
- Access to the boiler room is restricted to authorised staff

Fixed / portable heaters:

- Located away from items that will burn, e.g. not close to coat racks. No items are stored on or above them and they are not used for drying clothing
- Heaters are not left on overnight, timer switch devices may be used to control this
- Maintenance and servicing of heaters is undertaken in line with the manufacturers recommendations
- All portable heaters are turned off when not in use or when the room is unoccupied

## Annex A Further Information

Lockdown Procedures; Guidance to schools and academies

- www.centralbedfordshire.gov.uk

Active Shooter Preparedness

- www.dhs.gov/active-shooter-preparedness

CFPA-Guidelines

- Introduction to Qualitative Fire Risk Assessment, CFPA No 4/F

## Annex B Changes (not marked)

- Abbreviations without further use in the text were deleted
  Wording for the abbreviation for video surveillance systems changed to VSS