

School Security Policy

Roselyn House School

2026 – 2027



Approved by:	Rachel Smith	Date: 17/07/2026
---------------------	--------------	-------------------------

Last reviewed on:	July 2026
--------------------------	-----------

Next review due by:	July 2027
----------------------------	-----------

1. Introduction

It is important for Schools and Colleges to have a policy and plan in place to manage and respond to security related incidents.

This policy complements our Safeguarding Policy and works alongside Emergency Planning Policy and contingency Emergency Plan, Health and Safety and Safety Arrangements, Violence in the Workplace Policy, Bomb Threat Policy, Online Safety Policy, E-Safety Policy and Electronic Information and Communication Policy, Behaviour Policy, Educational Visits Policy, Sexual Violence and Sexual Harassment Policy, Social Media Policy, Transport Policy and Violence in the workplace Policy.

It follows guidance laid out in DfE School and College Security Guidance November 2019 and Emergency Planning and response for education, childcare and children's social care settings May 2023. It draws on resources produced by Local Authority and NEU Union guidance.

This policy should also be read alongside Keeping Children Safe in Education (KCSIE) 2026, the current Prevent Duty guidance and relevant cyber security guidance. Security incidents involving a child protection concern, unexplained injury, weapon, criminal exploitation, threat of serious violence, extremist concern or other safeguarding matter will be managed in accordance with the school's Safeguarding and Child Protection Policy.

At Roselyn House School, Mrs Rachel Smith is responsible for Health and Safety. Mr Jack Birkenhead is the Designated Senior Lead for Safeguarding. Other DSLs include, Mr Howard Dickinson, Mrs Sarah Trent and Miss Karen Brunskill.

Site addresses:

Roselyn House School KS3/4 site, Moss Lane, Leyland, PR25 4SE

Roselyn House School KS5 site, 26 Hastings Road, Leyland, PR25 3SP

Staff and, where appropriate, students should take personal responsibility for both their own security and the security of those they work and learn alongside. This, along with the effective management and handling of security related matters, should help to ensure that staff and students are able to work and be taught in a safe and secure environment, including the online environment.

Staff and students should be familiar with what is required by our Security policy and plan. Senior staff should have an awareness of relevant security networks and be able to

evaluate and assess the impact of any new initiatives in this Security policy and its day-to-day operation.

We consider security alongside our safeguarding responsibilities and the legal obligations under the Health and Safety at Work Act 1974 (HASAWA) and the Management of Health and Safety at Work Regulations 1999 (MHSWR).

2. Health and Safety at Work Act

The basis of British health and safety law is the HASAWA, and the regulator in schools is the Health and Safety Executive (HSE). The HASAWA sets out the general duties employers must follow to ensure the health and safety of their employees and others on school and college premises.

The law requires employers to take a common sense and proportionate approach to identify, assess and keep under review health and safety related risks and take steps to reduce or eliminate those risks. This includes security risks where there is a threat of attack on staff and students from within or outside the school or college.

3. Management of Health and Safety at Work Regulations

The MHSWR set out what employers are required to do to manage health and safety on a day to day basis. This includes a requirement for employers to appoint one or more competent persons to oversee workplace health and safety and to support compliance with the regulations. The HSE has also published Employer's responsibilities: Workers' health and safety and Education: health and safety in schools, further and higher education on managing risks in the education sector. Mrs R Smith has overall responsibility for the management of Health and Safety across both sites and is classed as our 'competent person.'

4. Responsibility

Mrs Smith has the subject knowledge, is trained in matters related to handling risks and has the experience to apply that subject knowledge correctly in the workplace. It is possible that certain aspects of security will be outside of her scope and in this instance further professional advice is sought through Peninsula. She is supported as part of the Senior Leadership Team, NAHT in her Business Manager Role and the Headteacher. All staff receive training in Health and Safety and specific training relating to Safeguarding. We work alongside further partners in the local authority, Social Care and Police.

The competent person should consider matters of security in consultation with the SLT, including areas regularly used for off-site education and those related to our educational visits policy. Our Security Policy:

- identifies the likelihood of a security related incident occurring

- assesses the level of impact
- develops plans and procedures to manage and respond to any threats

The competent person along with the Directors ensures that business continuity plans are in place to enable staff and students to react appropriately and promptly in the event of a serious incident. This should include arrangements to respond to the immediate crisis as well as short, medium and long term issues that may subsequently arise.

All staff and students must be able to work in a safe and secure environment. Whilst education establishments continue to be amongst the safest places, we should not ignore the potential threat of, and impact arising from, security related issues, such as vandalism, arson, cyber-attack, a serious incident involving a weapon or terrorist attacks.

This Security policy:

- reflects the balance between maintaining an open and welcoming environment for learners, parents and the wider community and protecting them from harm
- helps create a culture in which staff and students recognise and understand the need to be more vigilant about their own and the safety and security of others
- demonstrates an understanding of the issues that could impact on our school and wider community

Our plans and supporting procedures:

- Are based on a realistic assessment of the threats relevant to Roselyn House School.
- Demonstrate that there is a shared and common understanding about how to respond to identified threats.
- Are clear about what is expected from the staff, students and the local community should an incident occur.
- Draw on experience and expertise provided by our local authority, police and others, such as local resilience forums.

In a rapidly changing world where security threats are becoming more prevalent and diverse, it is essential we consider and routinely review our security arrangements, policies and plans. These are reviewed annually or following an evaluation of an incident.

We aim to put in place measures that are sensible and proportionate to the security threats that we have identified and follow this policy, Emergency Planning Policy and Emergency Plan.

5. Building partnerships

We have established relationships locally and work in partnership with the police, local authority and others in the wider community to gather and share security related information.

This enables us to put arrangements in place to share information quickly and help with the development and review of our policies and plans. In most cases, you are best placed to make decisions about how to respond to incidents on our premises.

Due to the likelihood of an external incident having an impact on our school we have security risk assessments which extend beyond.

We have Emergency Planning, Risk Assessment for Educational Visits, Educational Visits Policy and Cyber security audit against Cyber Security Standards along with a Electronic, Information and Communication Policy. These are communicated to staff, available on the website, to Parents/ Carers and help in understanding how to respond to an emergency or incident at school.

6. Risk assessment - identifying internal and external security risks and implementing preventative measures

At Roselyn House School we undertake health and safety surveys and risk assessment. We follow the same approach when considering security. We determine the type, frequency and probability of an incident or event happening and then put in place measures either to eliminate or reduce the risk of it occurring. We have dedicated risk assessments which deal with indoor areas, outdoors, lone working, PREVENT, Violence and aggression, Home working, management of infectious diseases, Transporting students, alternative provision, educational visits and visitors.

We have a Safeguarding Policy and addendum which describes the indicators which may signal that students are at risk from, or are involved with, serious violent crime. All staff should be aware of the associated risks and understand the measures in place to manage these. This contains specific advice on violence, drugs and child exploitation.

Any security incident which raises safeguarding concerns will be recorded on CPOMS and reviewed by the Designated Safeguarding Lead. This includes concerns relating to serious violence, weapons, exploitation, online threats, repeated incidents, unexplained injuries, or any matter which may indicate risk to a pupil's welfare.

We have laid out some of the preventative measures which are generic and specific to both sites.

We have considered the following points:

- Perimeter security
- External environment security

- Building security
- Contents security
- Lockdown procedure
- Advising suitable students about counter terrorism
- Staff training
- Safeguarding walks
- Cyber security audit
- Emergency planning, procedures and training
- Trespassers and intruders

There is not an exhaustive list of generic security threats but these may include:

7. 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:

- intrusion detection system including alarm system, security lighting and security glazing
- integrated access control systems to control, monitor and deny access when necessary
- staff supervision at break times and before and after school, monitoring entrance/exit to site
- searching, screening and confiscation where the Headteacher or any authorized member of staff has reasonable grounds to suspect that a student may have a prohibited item in school. They have statutory powers to search pupils and their possessions without consent and can seize prohibited items found as a result of the search. (See [Searching, screening and confiscation at schools](#))

The Home Office provides [Preventing youth violence and gang involvement guidance](#) for staff in schools affected by gang or youth violence.

The [Serious Violence Strategy](#) sets out the government's response to serious violence and recent increases in knife crime, gun crime and homicide.

There is also guidance on [Criminal exploitation of children and vulnerable adults: county lines](#), which outlines what county lines and associated criminal exploitation is, the signs to look for in potential victims, and what to do about it in partnership with the police and community safety partners. Further information is available on [Safeguarding children who may have been trafficked](#).

As part of its response to violent crime the [Home Office has also developed a resource pack for teachers and other professionals working with young people at risk of involvement in knife crime](#). These resources can be used in lessons or alongside other relevant materials to deliver messages and advice to young people on the consequences of knife crime. The campaign signposts teachers and young people to support services.

Dealing with intruders

Schools are not public places to which anyone can have access. People entering without permission are trespassers and a variety of approaches are available for dealing with trespassers under the law. The first thing a school should do is to make clear exactly who has authority to be on the premises.

Some people, in particular staff, students and parents/carers, will have 'implied' authority to be present if they would normally be allowed access to the premises. There can be limits to their implied authority to be present. For example, there may be limits on the times and places when their presence is authorised. Parents/ Carers might expect to be allowed on site only when invited.

Other people, including visitors, need specific authority to be present if they are not to be regarded as possible trespassers.

At Roselyn House School, this is clearly communicated to students and Parents/ Carers which helps in ensuring everyone knows who has authority to be present in school. Anyone can have their authority to be present withdrawn by letting them know by letter. Any implied authority of individuals to be present does not extend to circumstances when they are causing a disturbance.

Special legal provisions govern steps to be taken against trespassers in schools. Section 547 of the 1996 Education Act provides that trespassers who are making a nuisance or

disturbance and refusing to leave school premises are committing a criminal offence. 'Nuisance or disturbance' has a wide interpretation and includes, for example, riding motorbikes or exercising animals in such a way as to disturb the normal running of the school. Such trespassers cannot be arrested but they can be removed by a police officer or anyone authorised by the 'appropriate authority' – the Proprietors. They can also be prosecuted and fined up to £500 or, if under 16, their parents can be bound over.

School staff should not themselves take on responsibility for removing intruders. The recommended course of action is:

- to advise trespassers that they are on the premises without authority and ask them to leave
- if they ignore the warning, to advise them that the police will be called
- report immediately to a member of SLT
- to call the police and arrange for a police officer to come and remove them from the premises (serious incidents should, of course, be reported to the police at once).
-

The general criminal law applies where other criminal offences are being committed. Anyone committing a criminal offence, such as threatening behaviour, causing a breach of the peace, assault or committing criminal damage, can be arrested and prosecuted.

Finally, the school may take action under civil law. Injunctions can be sought against persistent trespassers and these can, for example, prohibit named individuals from coming on to school grounds or within a certain distance of the school. Anyone causing loss or damage can be sued by the school. Police and local authorities have used Criminal Behaviour Orders to exclude particular people from a school or schools where their behaviour is identified as likely to cause harassment, alarm or distress, which are a criminal offence if breached.

Controlling access to school premises

Signage

Appropriately worded signs are displayed directing visitors to the school office/reception. In addition, appropriately worded warning signs regarding the presence of an alarm system, monitored CCTV (KS4/5 site), trespassing and the fact that all property of value on the school premises is property marked is displayed.

Visitors

Visitors to the school should not be allowed to wander about the school unaccompanied. Identification provided by local authorities, utilities or other organisations should not be accepted as an alternative to the school's own system.

All staff are to wear ID badges and anyone not wearing a badge should be challenged.

Good access control is essential to the security of the school during the school day. Procedures are in place to ensure that, no one is able to access through the locking of doors and staff only access routes. Once in the building, systems are in place to notify SLT to protect or help students and staff should support become necessary. This is the responsibility of everyone.

All visitors, should initially report to the school office/reception, where the purpose of their visit can be established prior to them signing in and being issued with a visitor's badge, valid only on the day of issue.

[Controlling access to school premises](#) provides guidance on handling incidents and restricting access to, and barring of abusive or threatening individuals from, school premises and clarifies what a school is able to do should such an incident occur.

Safeguarding Walks

(See Child Protection and Safeguarding Policy)

Audits are carried out to monitor areas which may be of concern internally and externally, which may be hidden to staff sight. These are recorded and procedures put in place to minimise these areas where students may be unseen. In addition, this helps advise security risk.

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

(See Bomb Threat Policy)

Preventative measures include:

- [increase staff ACT awareness](#) of what to do and how to react
- effective screening of staff, students and visitors to schools and colleges for prohibited items
- direct communication to staff, students and intruders
- effective building controls including the ability to lockdown parts of the school, minimising direct access to school in a vehicle with a gate or in the case of the KS4/5 site a carpark directly in front of the building.

Counter terrorism advice for students aged 11 to 16

Security experts from Counter Terrorism Policing have commissioned the creation of an animated core film designed to teach young people how to react if caught up in an a gun or knife terror attack. The film aimed at 11 to 16 year olds will also show them what to do if they see suspicious behaviour or a suspicious item.

Counter Terrorism Policing have collaborated with specialists from the PSHE Association and Girlguiding to produce ACT for Youth. The [Run Hide Tell resource pack](#) provides a comprehensive toolkit, including lesson plans, posters and short films. You can use it to introduce security awareness into your school or college, to actively and openly engage with students about the impact and consequences of violent crime and terrorist activity on themselves and others and equip them with good advice and strategies to use outside of your school or college.

In circumstances where the DfE are made aware of an extremist or counter terrorism-related incident at an education institution, they will work with the local authority and other partners to ensure that the relevant support is provided. This would include, if appropriate, support from a Prevent Coordinator or the Prevent Education Officer.

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:

- policies to manage and monitor access to sensitive and personal information, including restricting access to authorised users, audit trails for changes to records **(See Data Protection Policy, Exams Policy and Electronic Information and Communication Policy)**
- training for all staff on General Data Protection Regulation requirements and cyber threats ongoing and induction.

8. 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:

- 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 reliance on IT and have a business continuity plan to enable us to operate without it- back up externally and have some access via paper records
- regularly review policies to ensure cyber security standards are maintained (See Cyber Security Standards audit)
- implementing content filtering to prevent inappropriate content access
- verify email senders, do not circumvent our security processes
- having effective policies to educate staff and students on our cyber security
- utilise [National Cyber Security Centre advice for small and medium sized organisations](#) for further information

9. 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

(See Lone Worker Policy, Behaviour Policy, Restrictive Physical Intervention Policy, Violence in the Workplace Policy, Anti-Bullying Policy, Single Equality Policy).

Personal security concerns may also include online harassment, cyberbullying, threats through social media, threats towards staff outside school hours and incidents arising from restrictive physical intervention. Any injury, threat, weapon-related incident or security concern arising during restrictive physical intervention will be recorded and reviewed in accordance with the school's Behaviour Policy, Physical Intervention Policy and Safeguarding Policy.

10. 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 students prior to use in lessons
- rehearsed response in line with local emergency/disaster plans and remove guidance.

In determining the type of preventative action to be taken, we ensure that any measures put in place are proportionate to the type of threat when assessed alongside the likelihood of it occurring and the impact that it would have on school. Where significant risk is identified, we review our existing measures and where necessary update them. For

example, review invacuation and evacuation procedures, or consider whether to introduce dynamic lockdown procedures in order to help manage an increased level of risk.

Roselyn House School policies, plans and procedures in place deal effectively with health and safety responsibilities and security matters. These:

- reflect both sites' size and location
- considers our unique circumstances, character, ethos, educational needs and local priorities

11. Site security.

Protection of premises against a potential criminal, terrorist and other unlawful action is an important issue. We consider how both local and national security incidents might impact on our day-to-day business and the safety and security of staff and students.

School security is ever changing and needs to be kept under constant review, with vulnerable areas identified and remedial actions implemented to address them.

No two schools are identical, and the design of the buildings and the layout of the site will differ from school to school. However, many of the issues revolving around security are generic.

12. Site specific security may include:

Perimeter

RHS KS5 site: There is a front entrance which leads off the car parking area which is lined with 2m fencing to divide the site from other businesses. The rear door leads onto the car park for the business downstairs and is utilised for emergencies only. This area is locked at night.

RHS KS3/4 site: The site is bordered by railings, established trees and shrubs on three sides. There is a wooden fence dividing from the neighbouring property and low-level mesh fencing to the remainder. There is a metal electric gate to the drive which is closed after 9.25am and reopened at 3.25pm (gates open throughout the day for vehicles, this is managed by staff). There are existing unused, secured gates and posts behind the Art cabin which is joined with the low level meshing. Tree canopies are kept cut back and fall higher than 2metres from the ground so as to maintain open sight.

Main site entrances

RHS KS5 site: The front door leading from the car park is left open with stairs leading up to reception which is locked with a code opening entrance. There is a hatch opening to main reception.

RHS KS3/4 site: doors are secured during the day (unless required to be open for a specific, agreed purpose) and office staff meet visitors at the front door.

Lighting

RHS KS5 site: There is security lighting to the front and rear entrances.

RHS KS3/4 site: Security lighting is provided around the perimeter of the school building with dusk to dawn lighting on all elevations where there is an entrance door. The lighting is designed to eliminate potential hiding points.

Car parking areas

RHS KS5 site: It is well lit and has natural surveillance at the front of the premises.

RHS KS3/4 site: It is well lit and facing the front door.

Doors and windows (generic to both sites)

See previous section on **main entrances**. The main entrance door incorporates some degree of access control such as a remote electronic lock release device incorporating an intercom/ visual verification.

Other entrance points should be kept locked to prevent them being opened from the outside but able to be unlocked from the inside in the event of an emergency.

There is one entrance to the school building via the office/reception, with clear directional signs indicating its location to visitors. In turn this door incorporates suitable access control with a remote electronic lock release, intercom and visual verification.

All windows and doors are checked and assessed to ensure that the locking mechanisms are in working order and are fit for purpose.

All fire exit doors are devoid of external door furniture.

All ground floor or other easily accessible windows above ground floor level have suitable key operable locks fitted for additional security.

Glazing to doors and ground floor windows includes at least one pane of attack resistant laminated glass.

Steps are taken to prevent access to the roof by locking of loft hatches and external means of climbing up.

Alarm systems and CCTV

Both Roselyn House School are fitted with type 'A' monitored alarms. Type 'A' alarms are monitored by a central monitoring station and have the facility for immediate response to any security breaches. This is contacted to G4S.

IT equipment:

RHS KS5 site: The IT suite is located in the centre of the school to make it harder for an intruder to gain access. It is covered by a monitored alarm. There are PC's across the site. Laptops are stored in a lockable cabinet.

RHS KS3/4 site: There are PC's across the site including external Cabins which are covered by a monitored alarm. Laptops are stored in lockable cabinets.

We avoid advertising desirable IT equipment to thieves. We refrain from mentioning IT assets on the school website and social networking sites. **(See IT Asset register)**

Members of staff have individual log ins to protect data stored. This could be cancelled in the event of theft. There are back up systems including the cloud.

Property Security (generic to both sites)

Secure storage is in place for money with locked boxes and safes at both sites. There are asset registers for IT equipment and school vehicles.

The school maintains an Automated External Defibrillator (AED). The location of each AED is clearly identified on site and staff receive awareness information regarding its use as part of emergency response arrangements.

13. School security lockdown

This information is generic and is based on government advice. The Headteacher or member of SLT will be responsible for judging the level of response required.

The requirement for a security lockdown may result from a reported incident in the local community which could pose a potential physical risk to students and staff.

There are similar measures suitable for environmental issues such as air pollution, fire in the area or a chemical incident which would be agreed with the appropriate agency.

In the event of a risk from an intruder or if a security warning is received the school goes into a full lockdown mode as follows:

Close the school and activate the school's Security Lockdown Plan.

This includes the following steps:

- Ensure that all students are brought into school quickly but calmly using the agreed signal '**LOCKDOWN**' (**this may be done in a discreet manner due to the needs of the students**) - they should be sent/escorted to their form classrooms and accounted for using the register.
- Fully secure the premises, locking all doors, and windows, this should be done by staff in the classrooms and checked by designated individuals (where safe to do so). These are:

Mrs Wilson and Year Leads at RHS KS5 site.

Mr Birkenhead and Year Leads at RHS KS3/4 site.

- This should be practiced regularly to ensure that all locks operate properly and you may need to take advice from the DOCO to ensure that all aspects are covered.
- The designated individuals should call 999 if not already in contact with the police.
- Visitors should be asked to stay, not leave, they should be taken to a designated location of shelter (main office at both sites if safe to do so) by a nominated member of staff and asked to remain quiet, turn phones to silent and stay out of sight.
- Once all students are accounted for in their classrooms, classroom doors should be locked and students asked to sit quietly away from sight.
- Any unaccounted students should be reported immediately to designated individuals.
- If you think or if you are told there is danger of explosion, ensure that any blinds and curtains are closed or classrooms where there are window coverings sit under desks.
- In the event of a chemical , pollution, biological or radiological contaminants use anything to hand to seal up cracks around doors and any vents in the room- you aim to minimize possible ingress of pollutants.
- Turn off all lights.
- Turn mobile phones to silent and ask everyone to remain quiet.
- You should wait for instructions which will come via the group email which can be accessed via individual mobile phones in the event of IT equipment not being accessible. These may also be followed by text messages.
- The primary method of communication during lockdown will be group email, supported by text message where required. Where electronic systems are unavailable, staff will follow the school's agreed emergency communication procedures and instructions from SLT or emergency services.
- Parents/ Carers will be notified as soon as is practicable. It is obvious Parents/ Carers will be concerned but regular communication will help to alleviate this anxiety. This will be done via email so as not to tie up the phone lines.

The school should remain in a state of lockdown until a senior member of staff or the emergency services confirm that it has been lifted.

The lockdown procedure is to be practiced at the start of each term and the Headteacher should ensure that all staff are trained and aware of their roles should a lockdown be required.

Lockdown arrangements may include full lockdown, partial lockdown, evacuation or dynamic lockdown, depending on the nature and location of the risk. Each lockdown exercise will be formally evaluated and lessons learned will be recorded and acted upon through the school's health and safety, safeguarding and emergency planning monitoring systems.

14. Communication between Parents/ Carers and School

This will be authorised directly from the Headteacher, SENCO, Year Leads and performed by the admin team.

Communications with parents and carers will identify the key information that can safely be shared, the expected method of communication, and any actions parents and carers should or should not take during the incident.

Arrangements for communicating with Parents/ Carers in the event of a lockdown are routinely shared either via newsletter or the school website. In the event of an actual lockdown, any incident or development is communicated to Parents/Carers as soon as is practicable.

Parents/ Carers should be given enough information about what will happen so that they:

- Are reassured that the school understands their concern for their child's welfare, and that it is doing everything possible to ensure their safety
- Do not need to contact the school. Calling the school could tie up telephone lines that are required for contacting emergency support providers.
- Do not come to the school. They could interfere with emergency support provider's access to the school and may even put themselves and others in danger
- Wait for the school to contact them about when it is safe to collect their children, and where this will be from.
- Are aware of what will happen if the lockdown continues beyond school hours.

It is vital that Parents/ Carers are reassured that this lockdown plan has their child's welfare at its centre and that everything that can possibly be done to ensure children's safety will be done. However, we should reinforce the message that 'the school is in a full lockdown situation.' During this period the switchboard and

entrances will have no staff available, external doors locked and nobody is allowed in or out.

Should parents present at the school during a lockdown under no circumstances should members of staff leave the building to communicate directly with them or let them in.

15. Managing risk

Risk assessments undertaken in a proportionate way help us reach a balanced view of the risks we may face. Each approach is based on a 5 stage risk management cycle that offers practical advice on how to rate and put in place plans and measures to eradicate, lessen and manage risks.

We prioritise the identified risks and put in place appropriate control measures to manage and monitor them. These are kept up to date and under review so we can risk assess any emerging issues early and update our plans.

16. Adopt a whole school approach

Not all security incidents are triggered by external factors. In determining the likelihood of a security risk materialising from within our school, for example an argument getting out of hand in a classroom, we have preventative measures which will help to avoid the risk of negative behaviour quickly and unexpectedly escalating to a more serious incident. **(See Behaviour Policy and Behaviour Support and Physical Intervention Policy).**

Effective behaviour management strategies can help to reduce the likelihood of such escalation occurring. Staff are trained in TEAM TEACH which utilises de-escalation and physical intervention techniques.

Staff should seek immediate assistance where a pupil presents with behaviour or circumstances that place themselves or others at immediate risk of significant harm, including serious self-harm, suicide concerns, ligature incidents, overdose, missing pupil concerns or other high-risk mental health crises. Such incidents will be managed in line with safeguarding, behaviour, physical intervention, first aid and emergency response procedures.

Alongside the development of robust behaviour management policies it is important to acknowledge that serious incidents, whilst rare, do occur. Lessons learned from dealing with such incidents have identified that young people should know how to share information in their possession about the possibility of a serious incident occurring and they should be actively supported so they feel safe to do so.

There are a number of mechanisms being used to encourage and support young people to share information, including some that provide facilities for anonymous reporting by students, Parents/ Carers and staff.

It is widely understood that anonymous reporting can help to support a culture where young people can be encouraged and, without fear of recrimination, feel safe to leave information about issues of concern for adults to pick up and take action on. We have worry/ bully/ suggestion boxes within school and surveys.

These results are assessed and allow students, Parents/ Carers, Staff to say what they feel is good or bad. Where effective information sharing arrangements are used this prompts action to risk assess and reduces the likelihood of a related incident occurring. It provides timely action to intervene and may help to avert a serious incident.

Students need to know the difference between dialling 999 (emergency) and 101 (non-emergency), and other ways to interact with the police, for example through social media and reporting online.

17. The curriculum

The curriculum offers many excellent opportunities to help manage our security, inform young people about the dangers they may face, both in and around school and beyond, and provide students with the means to help keep themselves safe. We teach relationships education and relationships and sex education as part of PSHE programmes. These schemes of work support students, helping them prepare for modern life, including how to handle issues relating to relationships, mental and physical health and staying safe on line. **(See Personal, Social, Health and Economic Education and Spiritual, Moral, Social and Cultural Development Policy.)**

Many third-party partnerships contribute effectively to the PSHE curriculum and we work with outside agencies and also Police to support with:

- delivering messages that are of concern to the police, schools, and colleges
- early intervention with youth crime
- foster positive relationships between the police and young people

Many police forces work closely and collaboratively with schools and colleges making sure students understand the law and the consequences of risky behaviours. Further information and best practice about working in partnership with the police, and the benefits, can be found in [Police in the classroom - a handbook for the police and PSHE teachers](#), a joint publication by the PSHE Association and the NPCC.

18. Testing security plans

We regularly test emergency policies and procedures. Practice drills identify where improvements can be made and enable us to assess what the wider residual effects of an incident are likely to be.

19. Managing an incident or emergency

The aim of Roselyn House School's Security Policy, Emergency Planning Policy and Emergency Plan is to help staff respond effectively to an emergency at the school, or on an educational visit. It aims to be generic enough to cover a range of potential incidents that could occur. Examples include:

- serious injury to a student or member of staff (for example, transport accident (**See Transport Policy**))
- significant damage to school property (for example, fire (**See Fire Policy and procedures and Fire Setting Policy**))
- criminal activity (for example, bomb threat (**See Bomb Threat Policy**))
- severe weather (for example, flooding (**See Emergency Planning Policy**))
- public health incidents (for example, influenza pandemic (**See Emergency Planning Policy and Risk Assessment relating to Pandemic and epidemic**))
- the effects of a disaster in the local community (**Wellbeing and Therapy arrangements**)

Effective communication is essential for the efficient management of any incident. It is important that all staff know what to do in the event of an incident, or potential incident. They should know who to contact, and how, including how to raise an alarm to alert staff and students. It is important that all staff feel empowered to make decisions and know what action to take where they have a concern.

Social media can play an important role in dealing with critical incidents. Working in partnership with the police enables us to understand how the police use social media to help manage information and keep the public informed during a serious incident. Social media can also be a helpful source of information in preventing such incidents. It is important that intelligence is shared between schools, the police and other partner organisations where this is appropriate. More information on the use of social media by the police is provided in the [Police Foundation's briefing](#). The police can also advise on how you can maximise the use of social media when dealing with serious incidents.

Any communications with the media would be through the Headteacher, Deputy Headteacher and Business Manager.

Further information on handling media attention after a major incident is available in the [Handling media attention guidance](#).

20. Business continuity management

Roselyn House School's Business Continuity Plans are an integral part of a security policy and sets out how we will recover in the event of any security related incident. **(See Emergency Plan and Business Continuity Plan)**

The [Royal Society for the Prevention of Accidents \(RoSPA\) has some Safety and disaster management guidance](#) covering disaster plans and recovery.

Our business continuity plan explains what will be done to handle the emotional impact of such an event and includes information about the professional and specialist help available.

The difficulties we would face in restoring normality following any traumatic event should not be underestimated. Those leading the recovery will not only be facing and dealing with their own personal challenges but will also be dealing with the impact on staff, students and parents.

21. Recovery

Post incident evaluation is essential and time must be made to bring together key players to review and evaluate how the security plans in place stood up to the task. Time should be invested to debrief and elicit feedback from all those affected, including staff, students and Parents/ Carers. Undertaking a critical review of the security and business continuity plans should identify lessons learned and the actions needed to improve and ensure the ongoing development of the security policy and plan.

[RoSPA's Safety and disaster management guidance](#) provides a step by step approach to preparing, managing, recovering and learning from a serious incident.

22. NHS

The [NHS has produced a Coping with stress following a major incident leaflet](#) on how to recognise and deal with trauma after a major incident.

23. Staff training

Appropriate training is given to the persons with responsibility for health and safety, and security.

All staff receive appropriate security training relevant to the nature of the risk Roselyn House School may encounter. This may require a combination of formal and informal training.

Security training may include Prevent training, ACT Awareness, lockdown procedures, emergency response, safeguarding and contextual safeguarding, cyber security awareness, visitor management, lone worker procedures and de-escalation/physical intervention training where relevant to role and risk assessment.

24. Emergency incident and planning

All staff should know what to do to protect themselves and students from harm, safeguard the sites and be able to determine when it is appropriate to contact the police and other emergency services. **(See Emergency Planning Policy)**

Further guidance is available on [how schools and other educational settings should plan for and deal with emergencies, including severe weather and floods](#).

25. Monitoring Arrangements

This document will be reviewed every year, but may be reviewed and updated more frequently if necessary. It will be reviewed by ***Mrs Rachel Smith (Senior Business Manager)*** in consultation with the wider school community.

26. Linked Policies

This Policy is linked to the following policies and documents:

- Child Protection and Safeguarding Policy
- Behaviour Policy
- Restrictive Physical Intervention Policy
- Emergency Planning Policy and Emergency Plan
- Business Continuity Plan
- Bomb Threat Policy
- Cyber Security Policy and Online Safety Policy
- Educational Visits Policy
- Health and Safety Policy
- Lone Worker Policy
- Violence in the Workplace Policy
- Data Protection Policy

Resources

- [Managing risks and risk assessment at work \(Health and Safety Executive\)](#) - guidance on the 5 stage risk management process
- [Bomb threats guidance](#) - guidance on what to do if a bomb threat or other malicious communication is received
- [Mail screening \(Centre for the Protection of National Infrastructure\)](#) - advice on handling post
- [Counter terrorism e-learning \(Highfield Online Learning\)](#) - online course to help individuals within UK businesses better understand and mitigate against terrorism
- [Creating a culture: how school leaders can optimise behaviour](#) - highlights strategies you can use to design and maintain a culture that prevents classroom disruption, maintains good discipline and promotes students' education, focus and wellbeing
- [Use of reasonable force in schools](#) - provides guidance on the use of physical restraint in schools
- [Searching, screening and confiscation at school](#) - explains the powers schools have to screen and search pupils, and to confiscate items they find

Further guidance

Drugs

- [Drugs: advice for schools](#)
- [Drug strategy 2017](#)

Hate crime

- [Racist and religious hate crime \(Citizens Advice\)](#) - how to recognise and report a hate crime

Radicalisation

- [Prevent duty guidance](#) - guidance on how to protect children from radicalisation
- [Protecting children from radicalisation: the prevent duty](#)

Safety and disaster management

- [RoSPA's Safety and disaster management guidance](#) on planning in advance and anticipating as many health and safety scenarios in schools as possible (should be used in conjunction with local authority advice)

School staffing advice

- [Staffing and employment: advice for schools](#) - guidance on managing staff and employment issues

Support for victims of terrorism

- [Support for victims of terrorism](#) - details of official helplines and support services available to victims, survivors, witnesses, family members, and all those affected by a terrorist attack

Violence in the workplace and personal security

HSE provides numerous pieces of guidance about handling work-related violence including setting up policies, how it should be managed and providing support after a major incident:

- [Policies and procedures](#)
- [Work-related violence](#)
- [Risk assessment for work-related violence](#)
- [Reporting and recording violent incidents](#)
- [Violence - quick guide to control measures](#)
- [Violence - partnership working](#)
- [Providing support after an incident](#)

