Burnt Oak Junior School
School Security Policy

Revised: April 2024
To be reviewed: April 2027

Contents:

Statement of intent
Legal framework
Roles and responsibilities
Working with other agencies
Physical security arrangements
Cyber-security
Equipment and belongings
School events
Access to the premises
Removing people from the premises
Violent crime
Reporting security concerns
Emergency procedures
Staff training and informing pupils
Testing security procedures
Information security
Monitoring and review

Appendix
A Lockdown procedures
B Bomb threat guidance

Statement of intent

Burnt Oak Junior School recognises its duty, under the Health and Safety at Work etc. Act 1974, to identify, assess and keep under review health and safety related risks, and to eliminate or reduce risks. We are dedicated to ensuring the safety and wellbeing of all people within the school community through implementing effective security measures, including e-safety and electronic control measures. Under this policy, a security risk includes risks to staff and pupils.

To identify the most prominent risks facing us, a thorough risk assessment has been conducted, which has been used to frame this policy to ensure that the control measures are appropriate and relevant.

The aim of this policy is to inform staff, pupils, parents and visitors of the security arrangements and controls in place and encourage them to help ensure that these are implemented effectively, while maintaining an open and welcoming environment for all.

This policy and the associated procedures apply to all individuals entering the school premises. The policy will be distributed to staff and pupils, so they can recognise and understand the need to be more vigilant about their own safety and security.

Legal framework

This policy has due regard to all relevant legislation and statutory guidance including, but not limited to, the following:

- Section 547 of the Education Act 1996
- Section 40 of the Local Government (Miscellaneous Provisions) Act 1982
- Health and Safety at Work etc. Act 1974
- Management of Health and Safety at Work Regulations 1999

This policy has due regard to the following statutory and good practice guidance:

- DfE (2018) 'Controlling access to school premises'
- DfE (2023) ‘School and college security’
- DfE (2023) ‘Site security guidance’
- DfE (2023) ‘Good estate management for schools’

This policy operates in conjunction with the following school policies and documents:

- Visitor Policy
- Health and Safety Policy
- Complaints Procedures Policy
- Child Protection and Safeguarding Policy
- Data Protection Policy
- Cyber-security Policy
- CCTV Policy
- Lettings Policy
- Records Management Policy
- Business Continuity Plan
- PSHE Policy

Roles and responsibilities

The headteacher will be responsible for:

- Explaining who is accountable for the school estate at a board and school level.
- Undertaking necessary security risk assessments in conjunction with the headteacher.
- Monitoring the performance of the school’s security measures.
- Reviewing the effectiveness of this policy on an annual basis.
- Delegating the day-to-day implementation of this policy to the headteacher.

- Ensuring that the school's security is accounted for when considering requests to hire the premises, in line with the school's Lettings Policy.
- Appointing one or more competent persons to lead on school security – the school's competent person is the site manager.
- Establishing relationships with local security networks and working with the police, LA and others in the wider community to gather and share security-related intelligence.
- Ensuring that all staff members are aware of the procedures set out within this policy and are provided with the required training.
- Informing parents, pupils, visitors and contractors of the school's security procedures.
- Establishing a system for reporting, recording and managing breaches of this policy.
- Budgeting for security measures effectively.
- Ensuring that security is taken into account when considering any proposed changes to the school premises.
- Undertaking necessary security risk assessments in conjunction with the governing board.
- Reporting any crimes to the police.
- Reporting security incidents to the police or emergency services where appropriate.
- Conducting a Security Risk Assessment in collaboration with the site manager and governing board on an annual basis.

All staff members are responsible for:

- Securing windows and doors when rooms are not in use.
- Ensuring that visitors sign in and out at the school office.
- Challenging any unidentified individuals and notifying the headteacher of any unauthorised person.
- Securing valuable equipment after use.
- Ensuring the security of school equipment when taken off the school premises, such as laptops.
- Accessing the school premises in accordance with the school's Key Holder Policy.
- Acting in accordance with the school's Data Protection Policy and Cyber-security Policy, ensuring that data and information is secure.
- Reporting any minor security concerns to the headteacher.
- Reporting major security concerns directly to the police or emergency services, where appropriate.
- Carrying their school ID with them at all times.
- Being responsible for the security of any of their own property that they bring to the school site.

As the competent person, the site manager is responsible for:

- Ensuring the school estate is well maintained, including the physical and electrical security systems.
- Securing school entrances and exits.
- Liaising with the named key holder, ensuring that the school is effectively secured at the end of each day.
- Carrying out security checks on a daily basis and maintaining a record of these checks.
- Raising any security concerns with the headteacher immediately.
- Ensuring a Business Continuity Plan is in place.

- Considering the type, frequency and probability of an incident or event, so that effective control measures can be established.
- Prioritising risks and, in line with the school's and locally agreed procedures, implementing control measures to mitigate priority risks.
- Reviewing CCTV systems to monitor activity, ensuring that CCTV is used in accordance with the school's Surveillance and CCTV Policy.
- Ensuring all access control systems, e.g. intruder alarms, are in good working order and are activated once the school has closed.
- Seeking professional advice on security issues where necessary.

Pupils and parents are responsible for:

- Reporting anyone without an ID badge to a staff member.
- Reporting any activity that they believe to be suspicious or concerning to a member of staff immediately – this can be done anonymously, if preferred.
- Familiarising themselves with the requirements of this policy, to ensure they know what to do in an emergency.
- Taking responsibility for their own security.

Working with other agencies

The headteacher will establish relationships with local services such as the police, the LA and others in the community.

The site manager will be responsible for maintaining these relationships to gather and share security-related information.

Strong links will be developed with the police to enable the school to put arrangements in place to share information quickly and to help with the review of this policy and related security plans.

The site manager will seek expert security advice where necessary and use this information when reviewing this policy.

Physical security arrangements

The school will incorporate measures as outlined in the DfE's 'Site security guidance' to ensure that it is taking all the appropriate steps to protect the security and safety of the school premises.

Intrusion detection systems, including fencing, security lighting, security glazing and intruder alarms, will be installed throughout the school estate.

The school perimeter will be protected with a secure fence or railings of a sufficient height to deter intruders. Gates will be the same height as fencing where possible, fitted with anti-lift hinges, and contain a suitable locking mechanism.

The site manager will undertake daily visual checks of the school fencing, security glazing, gates and locks on any doors and windows, ensuring that they are maintained to a high standard.

All ground floor or other easily accessible windows above ground floor level will have suitable key operable locks fitted for additional security. Glazing to doors and ground floor windows will include one pane of attack resistant laminated glass.

The school will be able to lock down parts, or all, of the school, in accordance with the Lockdown procedures (Appendix A).

Vehicle access will be restricted via the use of building controls that enables part of the school to be locked down, minimising direct access to school buildings e.g. by using speed bumps, warning and directional signage, barriers and structural furniture.

There will be directional signage so that individuals can find the school office with ease.

There will be warning signs around the school that state the expected behaviour of individuals, and that the police will be contacted following any inappropriate or threatening behaviour.

Chemical and biological materials will be stored safely and securely, in line with industry standards.

Between the times of 9:00am and 3:20pm, the headteacher will ensure the school gates are closed.

Where access to the school is required, such as for a large delivery, permission will be sought from the headteacher or SBM prior to the event and the site manager will oversee the access.

Staff cars are safely secured in the school car park, which is locked and only accessible by keypad or if Reception give you entry. The car park will be well lit with good natural surveillance.

If the staff car park requires unlocking, staff will request that the site manager opens it – the site manager will lock the car park upon the individual's departure.

There will be an intercom system on the car park fence, in case individuals need to access the car park in between the hours of 9:00am and 3:15pm.

School security alarms are tested on a monthly basis by the site manager. The key holder or site manager ensures that the school alarm is set on a nightly basis. Confidential information will be stored in locked filing cabinets, which only authorised staff have access to.

The school office will be secured whenever it is unattended, as it is the main entrance point to the school. Main vehicle and pedestrian access points will be overlooked by the school reception. The main entrance door to the school will be suitably signposted to visitors and contain an appropriate means of access control, e.g. a remote electronic lock release device with an intercom and visual verification. Secondary site access points will be kept locked from the outside unless required, e.g. to receive deliveries, but will be able to be unlocked from the inside in the event of an emergency. Classrooms will be locked when they are not in use.

Fire exit doors will be kept free of external door furniture.

Where possible, CCTV cameras will be in use and monitored by the site manager.

All visitors will be escorted to and from their destination within the school by a member of staff.

The school's security lighting will be maintained by the site manager. Security lighting will be provided around the perimeter of school buildings with dusk to dawn lighting on all elevations where there is an entrance door. Lighting will be designed to eliminate and minimise potential hiding points.

Appropriate mechanisms will be in place to prevent unauthorised access to the roof and courtyard areas.

The site manager will be responsible for ensuring that the school's security lighting motion detector is switched on every night but turned off each morning.

Cyber-security

The ICT technician will be responsible for ensuring that appropriate and effective online security systems are in place, including malware, internet gateways, firewalls and virus control software.

The school uses a secure network that is password protected.

Staff members and pupils are aware of the school's Cyber-security Policy and the measures that are in place to effectively manage risks caused by internet use.

All staff members will be responsible for identifying risks posed to pupils and themselves, including those in relation to the use of the internet.

Staff members and pupils will not use their personal devices for school-related work.

The school will only use CCTV cameras that are able to be remote access capability password protected.

The Cyber-security Policy will be reviewed in light of any new cyber security risks, e.g. a rise in targeted phishing attacks on schools, or statutory guidance, and updated where appropriate.

Equipment and belongings

The school's ICT suite will be located in a position, e.g. the centre of the school, that makes it harder for an intruder to gain access. The suite will be thoroughly secured and covered by a monitored alarm and CCTV.

An inventory will be kept on Parago of high-value items and items considered to be most at risk with photographic evidence, serial numbers and identification marks.

All electronic equipment will be stored in a secure location at the end of each day. Tablets and laptops will be stored in a lockable cabinet that is bolted to the floor. Computers that cannot be moved will be secured to the desk.

After using school equipment, staff members will be responsible for ensuring that it is returned to the appropriate storage location and secured.

Staff members will be responsible for any personal belongings, including teaching equipment, they bring on to the school premises.

Pupils, parents, visitors and contractors will be responsible for their personal belongings and the school will not be liable for any damage or loss which may occur.

Pupils will be advised not to bring valuable items to school unless absolutely necessary.

Where a pupil requires a valuable item to be brought to school, they can arrange with the headteacher in advance for a secure place to store the item.

Any equipment that someone wishes to take off the school site will be approved by the headteacher in advance and a record of the loan kept.

Any equipment that is loaned out to staff or pupils will be inspected upon its return, e.g. laptop that could carry viruses.

Outside play equipment, as well as sporting equipment, will be tidied away and secured inside the building at the end of use.

The school will provide an area for pupils to store bikes during school hours. Pupils are responsible for providing their own lock and effectively securing their bikes. The school is not responsible for any loss or damage that may occur.

Lost property will be stored in the school office, where it will be kept for half a term before disposal.

School events

During school events, all rooms except those required will be locked. Unless needed for the event, all equipment will be securely stored away.

The event organiser will be responsible for recording what equipment is being used for the event and ensuring that it is returned.

The site manager and the headteacher will carry out an extensive risk assessment for each event. The site manager will lock the school after the event has finished.

During off-site events, the school premises will be secured.

Individual staff members will not be left alone on the school premises with a parent or visitor. Where lone working is necessary, e.g. a parent meeting with a teacher, a lone worker risk assessment will be carried out.

There will be a minimum of 2 staff members on site at all times.

Access to the premises

The school premises are private property; however, parents of enrolled pupils have an 'implied licence' to access the school premises at specified times.

All staff members will be issued with an ID badge during their induction process, which must be worn at all times.

Upon arrival at the school, visitors will be directed to the school office where they must sign in, giving a reason for their visit, and wait for further direction from a member of the office staff.

All visitors will be made aware of, and will be expected to act in accordance with, the school's Visitor Policy.

All visitors and contractors who are authorised to be on the school premises will be provided with a school ID badge, which will be kept visible at all times.

The office staff will be responsible for ensuring that contractors and visitors sign out when they leave and return their ID badge.

Anyone who does not have an ID badge or is suspected to be an intruder will be challenged.

Individuals who are hiring the school site will act in accordance with the Lettings Policy and their hire agreement.

Integrated access control systems will be installed to control, monitor and deny access when necessary.

The site manager will ensure that all access control systems are in place and effective – where problems are identified, the site manager will rectify them immediately.

Removing people from the premises

In the event of abuse or threats to staff, pupils, parents or visitors, the school holds the right to bar an individual from entering the premises.

Where an individual has accessed the premises in a way that exceeds their 'implied licence', the school has the right to remove them from the premises; this includes any individual causing a nuisance or disturbance.

Unidentified individuals who refuse to report to the school office, become aggressive or are deemed to be a threat to the safety of the school community, will be escorted from the school premises and, where necessary, the police will be called.

In terms of barring particular individuals, the headteacher will make a proposal in writing to the governing board and all parties involved will be given the opportunity to formally express their views.

Letters and documentation concerning barring an individual will be signed by the headteacher, unless otherwise specified by the Trust.

Following formal representations being made by the parties involved, the bar will either be confirmed or removed.

All bars will be subject to review within a reasonable timeframe.

The school has the right to take civil action through the courts to stop persistent trespassers.

If a crime is committed on the school premises, the school has the right to remove the individual in question from the site and report the incident to the police.

Violent crime

All staff will be made aware of the indicators which may signal that pupils are at risk from, or are involved with, serious violent crime. All staff will be made aware of the associated risks and will understand the measures the school has in place to manage these, which are outlined in the Child Protection and Safeguarding Policy.

Where there are concerns about weapons being brought on to the school premises, the headteacher and site manager will consider additional security mechanisms, consulting the police where appropriate, to ensure the school community is kept safe.

The headteacher will liaise with the local police, community safety partners and other educational institutions in the area on how to address youth violence.

Pupils will be taught about the impact of violent crime and how to protect themselves from becoming involved in criminal acts.

Reporting security concerns

Missing or stolen equipment will be reported immediately to the SLT.

Unidentified individuals will be challenged immediately and reported to the school office.

Concerns regarding the security of the school will be reported directly to the site manager.

The headteacher will promptly risk assess and discuss security concerns with the governing board to

identify effective resolutions, e.g. installing CCTV systems.

Complaints about the school's security measures will be dealt with in line with the school's Complaints Procedures Policy.

The school will implement procedures to enable pupils, parents and the local community to report any security concerns anonymously – a Security Reporting Form can be accessed from the school office.

If the DfE is made aware of an extremist or counter terrorism-related incident at the school, it will work with the LA and other partners to ensure the school is provided with the relevant support.

Emergency procedures

The school will establish formal procedures to responding to emergencies linked to the security of the school estate and will conduct an estate risk assessment which considers emergency scenarios.

The school will draw on the expertise provided by the LA, police and other agencies when developing emergency procedures.

In the event of an emergency or a breach of security, the procedures outlined in the school's Lockdown Procedures or Fire Management Policy – staff members will be made aware of when it is appropriate to implement these procedures.

All staff members, pupils and volunteers, will be made aware of the school's emergency procedures as part of their induction, including those in relation to security alerts, trespassers and unidentified objects.

The headteacher will ensure that the appropriate authority is notified about any incidents and the need for emergency procedures, e.g. the police.

If it is necessary for the school to be locked down, the headteacher will contact the police for advice.

The headteacher, or their delegate, will be responsible for communicating with parents while the school's emergency procedures are being implemented.

The headteacher, or their delegate, will be responsible for dealing with any media enquiries about an incident.

Where appropriate, the school's social media channels will be used to keep the public informed during a serious incident. The headteacher will liaise with the police on how to share this information effectively.

If emergency procedures are carried out, the headteacher is responsible for ensuring that these are properly recorded.

This policy, and all associated plans and procedures, such as the Business Continuity Plan, will be reviewed and evaluated following any incident, to ensure that they remain effective.

Staff training and informing pupils

Staff members will receive cyber-security related training on an annual basis.

All staff members and pupils will receive training in the school's emergency procedures and will be aware of what to do.

As the competent person, the site manager will have relevant subject knowledge, e.g. security, be trained in matters related to handling health and safety risks and have the experience to apply subject knowledge correctly in the workplace.

Staff will receive safe handling training for chemical and biological materials, in line with the school's COSHH Policy.

Staff will be made aware of relevant security networks and be able to evaluate and assess the impact of any new initiatives on the school policy and its day-to-day operation, as well as how to protect themselves and pupils from harm, safeguard the school estate and be able to determine when it is appropriate to contact the police/emergency services.

Staff members will receive training in communications handling, particularly in relation to the press and media, on an annual basis.

External providers and visitors will be invited into the school when necessary to help deliver security-related messages to staff and pupils. When determining whether an external provider should be invited into school, the headteacher will consider the following:

- What the desired learning objectives and outcomes of the session are
- Why an external provider needs to be used rather than an internal member of staff
- Whether the messages can be delivered in line with the school's Child Protection and Safeguarding Policy
- Whether the external provider has the required skills and knowledge
- How the impact of the session will be evaluated

Pupils will be taught about security-related issues, e.g. staying safe online, through the PSHE curriculum, in line with the PSHE Policy.

Testing security procedures

The site manager will develop a schedule of testing the school's security and emergency procedures.

These tests will be used to identify where improvements can be made and to enable the school to assess what the wider residual effects of an incident are likely to be.

The headteacher will determine whether neighbouring schools, the local police or other agencies

should be involved in helping to evaluate practise drills.

Information security

The DPO will be responsible for ensuring that there are policies and procedures in place to manage and monitor access to sensitive and personal information, including the Data Protection Policy and Records Management Policy.

The DPO will provide training to staff on school policies and procedures in relation to information security.

Policies relating to information security will be reviewed in light of any new information on security risks or statutory guidance, and updated where appropriate.

Monitoring and review

Staff members will be notified of any changes made to this policy or to the school's security system.

Appendix A

Lockdown procedures

A lockdown is necessary when pupils and staff need to be **locked** within buildings for their own safety, such as in situations where there is a hostile intruder, terrorist attack or other criminal activity.

It is important to remember that it is **the exception** to evacuate a building in the event of a hostile intruder. Unless the location of the intruder is known, an evacuation may put people at risk of further danger, e.g. from an intruder or device at one of the exits.

In the interests of safety, it is important to make sure that items that could be used as weapons, e.g. kitchen implements, tools, cleaning products, are securely locked away when not in use.

Incident control officers and response team		
Role	**Nominated person**	**Emergency contact number**
Incident control officer		
Deputy incident control officer		
Communications officer		

Signals	
Full lockdown signal	
All-clear signal	
Evacuation signal	

Other arrangements		
Safe areas		
Outdoor safe area		
Evacuation point		
Pre-arranged alternative place of safety if required to leave the site	Venue name	
	Venue type	
	Point of contact	
	Contact number	

Useful information about the alternative place of safety	
Communication arrangements	

Wherever possible, use silent communications and keep noise to a minimum, especially if there are any intruders close by. Make sure any communication devices are secure and cannot be intercepted, e.g. turning devices off when not in use.

Initial implementation
The school is made aware via the agreed communication arrangements of the incident that requires the full lockdown procedure to be implemented.
The Head Teacher makes the decision to implement the full lockdown procedure.
A full lockdown signal is given.
Staff use an internal messaging system to ensure all staff members are aware of the incident that has occurred and the type of lockdown procedure to be implemented, and that the lockdown is not a practice.
The site manager is contacted to ensure they are aware of the implementation of the full lockdown.
The Head Teacher contacts the relevant emergency services to alert them of the incident and they are kept up-to-date, as necessary.
The Head Teacher informs the Regional Director, CEO or CFOO
Immediate action
All outdoor activity is ceased immediately; pupils, staff and visitors return inside the school building, unless it is unsafe to do so, and staff ensure all doors are securely locked.
Any lifts are disabled without returning to the ground floor.
The ventilation systems are turned off to prevent the spread of contaminates, e.g. sarin.
Staff, pupils and visitors that remain outside during the lockdown hide in the designated outdoor safe area until the emergency services arrive.
Staff escort pupils and visitors to the nearest safe area.
The Head Teacher and site manager check outdoor areas and ensure all pupils, staff and visitors are inside the school building.

When everyone is inside, all external doors and windows are locked, and blinds or curtains closed; doors and windows remain locked until the 'all-clear' signal is given or unless otherwise instructed by the Head Teacher or emergency services.
The Head Teacher and site manager check all external doors and windows are locked.
All internal doors to safe areas are locked and any windows on doors are covered.
Access points to safe areas are blocked off by moving furniture to obstruct doorways.
Lights in all safe areas are turned off.
Classroom teachers conduct a register or headcount. Staff notify the Head Teacher if any pupils, members of staff or visitors are not accounted for via two-way radio, and an immediate search is instigated by the Head Teacher, where appropriate and safe to do so.
Verbal communication via two-way radios or mobile phones is kept to essential communication. All mobile phones are turned onto silent and communication devices are not used if it would be unsafe to do so, e.g. if usage would lead to the location being revealed.
Pupils, staff and visitors sit quietly, away from doors and windows, and out of sight, e.g. under a desk.
All staff, pupils and visitors remain in their safe area unless otherwise stated by the Head Teacher or emergency services.
All pupils, staff members and visitors are made aware of their nearest exit point in case a hostile intruder manages to gain access to a safe area.
If possible, the Head Teacher will check for missing or injured pupils, staff or visitors.
Pupils and visitors are kept calm during the lockdown.
No pupil is released to their parents during the lockdown.
The office staff answer telephone calls from parents and inform them that pupils will not be released while the lockdown is in place. Alternatively, an automated answer machine message informs callers that a full lockdown procedure is in place.
The Head Teacher keeps in contact with the relevant emergency services to assess the best course of action in respect of the incident.
The Head Teacher sounds the evacuation signal if it is necessary to evacuate the building. The rest of the building is evacuated to the designated evacuation point if someone is taken hostage on the school site.

Further action after the lockdown
Parents are informed of the incident.
The SLT reviews the full lockdown procedure for its effectiveness and make changes as necessary.

Appendix B

Bomb Alert / Threat Template

There are important differences between the fire (or other whole building) evacuation and bomb instructions. Most notably in a bomb threat situation it is unusual to evacuate the entire building. To do so can be more hazardous than moving people within the building to areas away from the suspect package or incident.

Signal	
Signal for bomb threat (this must be different to the fire alarm, or general evacuation alarm/signal)	Public Address (PA) announcement – Code purple
Signal for stand down / all-clear	Public Address (PA) announcement – All Clear

Incident Control Officers & Response Team		
Role	**Name**	**Emergency Contact Number**
Incident Control Officer		
Deputies		
Communications Officer		

Other useful contacts	
Name	**Emergency Contact Number**

It is important to remember that it is very much **the exception** to evacuate a building in the event of a bomb threat or incident. Unless the location of the bomb is known, a "blind" evacuation may be putting people in more danger (e.g. from a device at one of the entrances/exits) than if they had remained within the building.

Primary Assembly points
1
2
3
4

Secondary (alternative) assembly point / place of safety (for example partner school/college / leisure centre) must be pre-arranged	
Name of venue	
Type of venue	
Contact name	
Contact telephone number	
Include useful info such as distance from school, directions, capacity, opening hours	

Suspicious Items, Packages or Envelopes

It is important that you do not move a suspicious item, package or envelope. Do not cover or encase it in any way. Be alert to secondary devices, there may be more than one.

Indicators of a Suspicious Item
Is the item typical of what you would expect to find in this location?
Has the item been deliberately concealed or is it obviously hidden from view?
Does it have wires, circuit boards, batteries, tape, liquids or putty-like substances visible?
Do you think the item poses an immediate threat to life?

What to do if you see a Suspicious Item
Do not touch
Try and identify an owner in the immediate area
Confirm whether or not the item exhibits recognisably suspicious characteristics
If you still think it's suspicious (or in any doubt)
Clear the immediate area and adjacent areas (be mindful of the possibility of secondary devices)
Dial 999 ask for the police
Follow their advice and provide as much information about the item as possible (see indicators above)
Prevent others from entering these areas
If safe to do so check CCTV

Indicators of a Suspicious Package or Envelope
General indicators that a delivered item may be of concern include:
unexpected item, especially if hand delivered
additional inner envelope or other contents that may be difficult to remove
labelling or excessive sealing that encourages opening at a particular end or in a particular way
oddly shaped or lopsided
unexpected or unusual origin (postmark and/or return address)
poorly or inaccurately addressed address printed unevenly or unusually
unfamiliar writing or unusual style

unusual postmark or no postmark
more stamps than needed for size or weight of package
greasy or oily stains emanating from the package
Odours, liquid or powder emanating from the package

What to do if you identify a Suspicious Package or Mail Item
Do not touch
If holding place it down carefully ensuring that it remains sealed
Clear the immediate area and adjacent areas
Dial 999 ask for the police
Follow their advice and provide as much information about the package as possible (see indicators above)
Prevent others from entering these areas

Bomb Threat

No matter how ridiculous or implausible the threat may seem, all such communications are a crime and should be reported to the police by dialling 999.

What to do if you receive a Bomb Threat on the telephone
Stay calm and listen carefully
Try to attract the attention of a colleague who should immediately dial 999
Hold the caller on the line for as long as possible. Get as much information as you can and provide this to Security as this will assist the Incident Control Team in providing information to the police.
For example -
When is the bomb set to go off?
Where has it been planted?
What does it look like?
What kind of bomb is it?
What will cause it to explode?
Was the caller a man or a woman?
Was a code word given?
What was the exact wording of the threat?
Did the message sound as though it was being read from a prepared text or was it a taped message?
Did the caller sound intoxicated?
Was there any indication of the callers' mental state - did he/she sound excited, disturbed, incoherent etc.?
Was there any accent, was he/she well-spoken etc?
Was there any indication of the type of telephone being used – for example a public call box?
Was there any significant background noise - e.g. house noises, street noises, music?
If displayed on your phone, note the number of the caller, otherwise, dial 1471 to obtain the number once the call has ended

What to do if you receive a Bomb Threat electronically (email, social media etc)
Alert the police immediately - they may be able to identify where the threat has come from
Do not forward or reply to the message unless advised to do so by the police
Do not delete the message
If possible take a screen shot of the message and any contact details in case the message is deleted
If not note the sender's email address or username/user ID for social media applications
Preserve all web log files for your organisation to help the police investigation