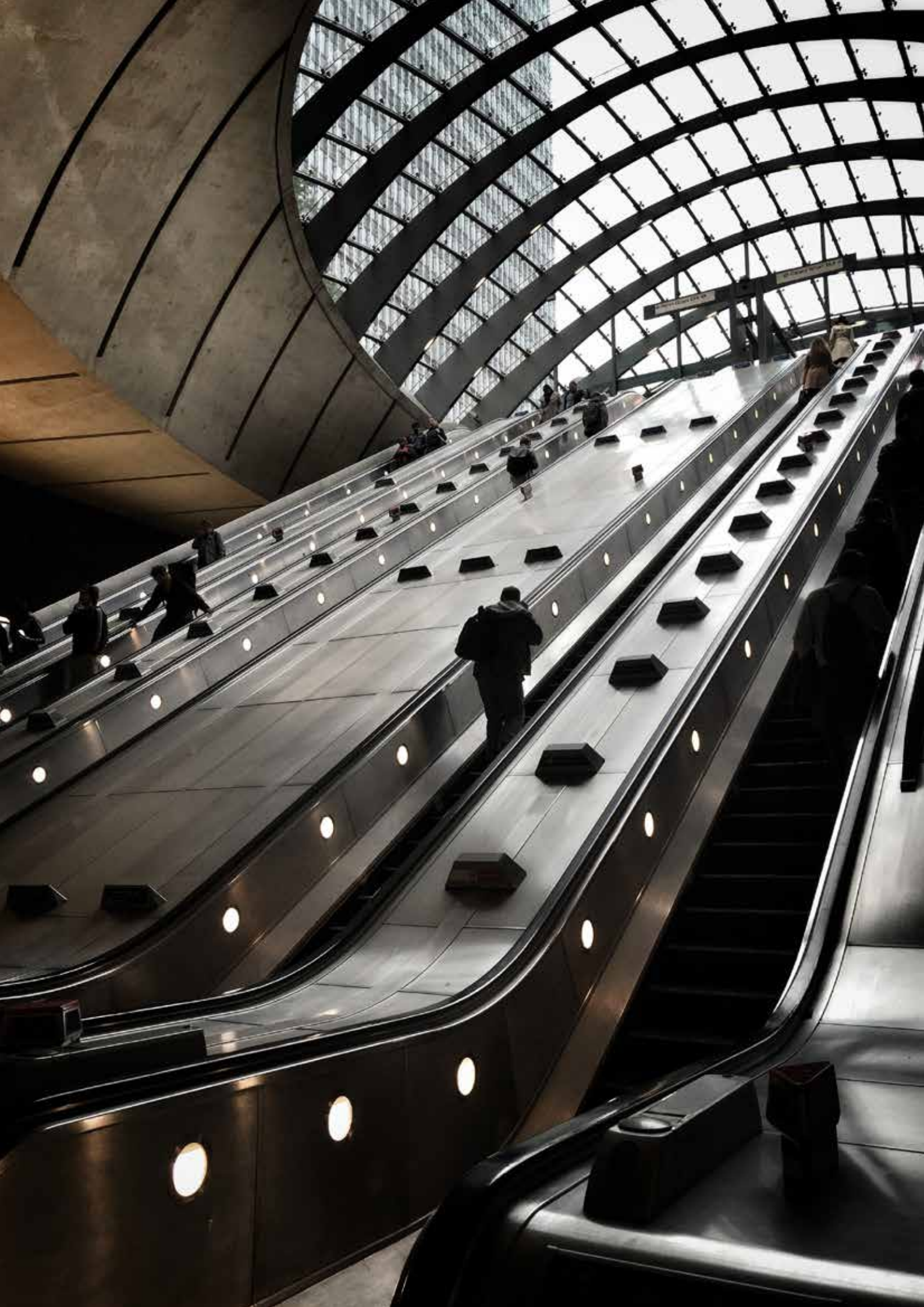
The Blue Book:

A Guide to Personal Security

NATIONAL
COUNTER TERRORISM
SECURITY OFFICE

Contents



Introduction

The aim of this booklet is to provide a suite of advice options when implementing a personal security plan.

This booklet may form part of a wider personal security package delivered by an accredited Counter Terrorism Security Advisor (CTSA) or a Designing out Crime Officer (DOCO) and should be referred to when refreshing your own personal security. DOCOs may also be known regionally as Crime Prevention Officers (CPO), Crime Prevention Design Advisors (CPDAs) or Architectural Liaison Officers (ALOs) depending on the local police force.

It is impossible to provide security for every eventuality; this guide provides generic advice to deter and to delay to give sufficient time to react and to mitigate risk

This booklet will also signpost you to other valuable sources of information and guidance.

Whilst this guidance does provide some technical detail, it is advisable to seek the support of a security professional, or from the appropriately qualified body accredited to the British Standards Institute (BSI) (where required) to ensure the standards are up to date and suitable in order to mitigate risk.

This guide will provide advice on how to stay safe at home, at work, on-the move and online.

It is important to be mindful of the risks. These will be dependent on your personal circumstances and the type of environments you are likely to encounter.

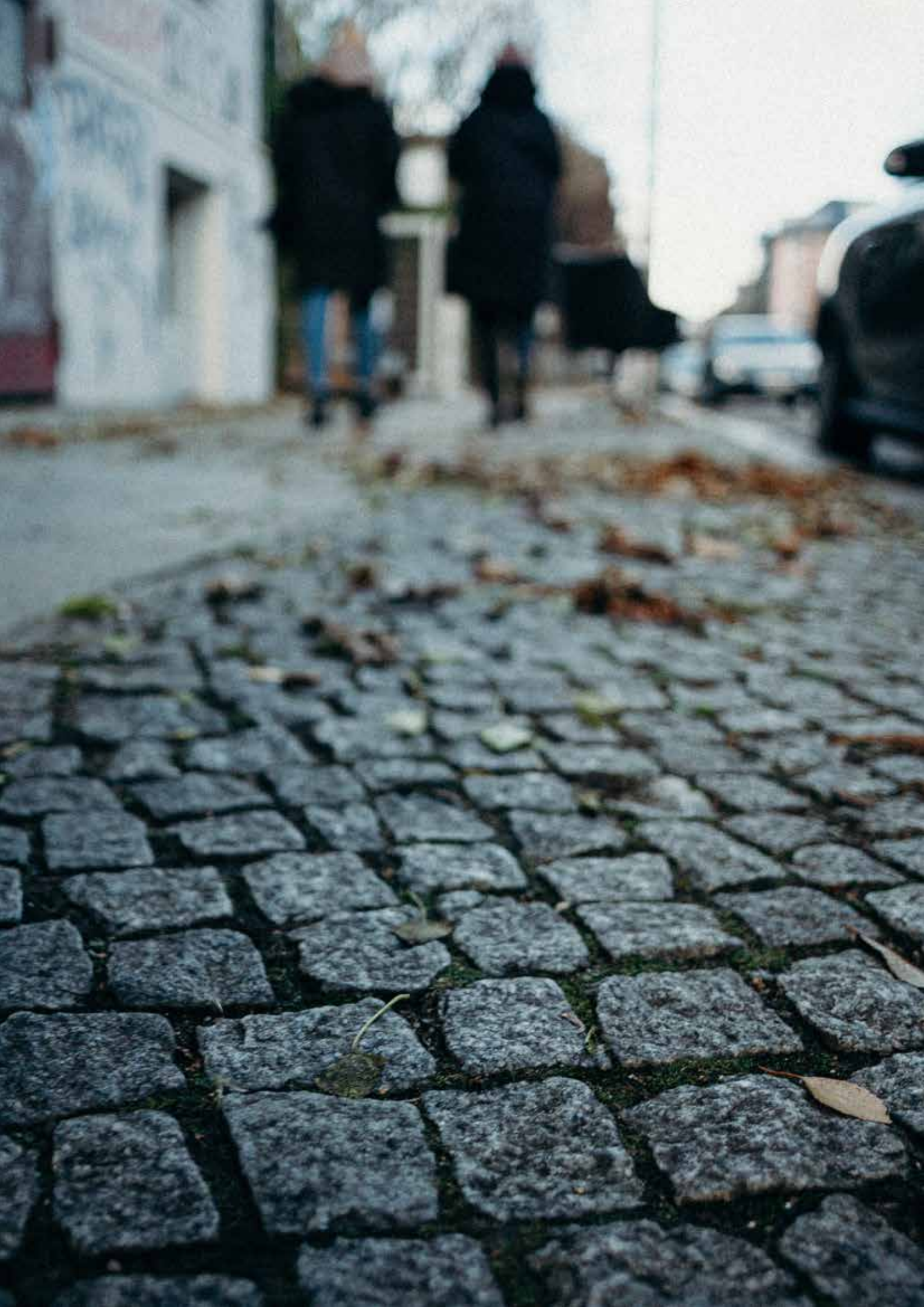
In reading this guidance, you will need to consider your type of work and home life.

Consider the following points:

Profession: Does the role/position make you or your place of work an attractive target?

Specific threats: Is there information to suggest that you, your family or associates are at risk of serious harm?

Personal history: Have you, your family or associates been targeted in the past?



Personal Security

Our own security, and the safety of those close to us, is of great importance. The more you do to protect yourself, the better protected you and your family will be.

Whilst we cannot predict or control everything that might happen to us, there are some steps we might choose to take to mitigate and avoid risk.

The recommendations contained within this guidance are based on research, historic events, expert advice and best practice, but it should also be recognised that these are primarily common sense precautions, albeit not exhaustive, and will depend on personal circumstances.

In an emergency, the advice is always call 999.

An emergency is described as;

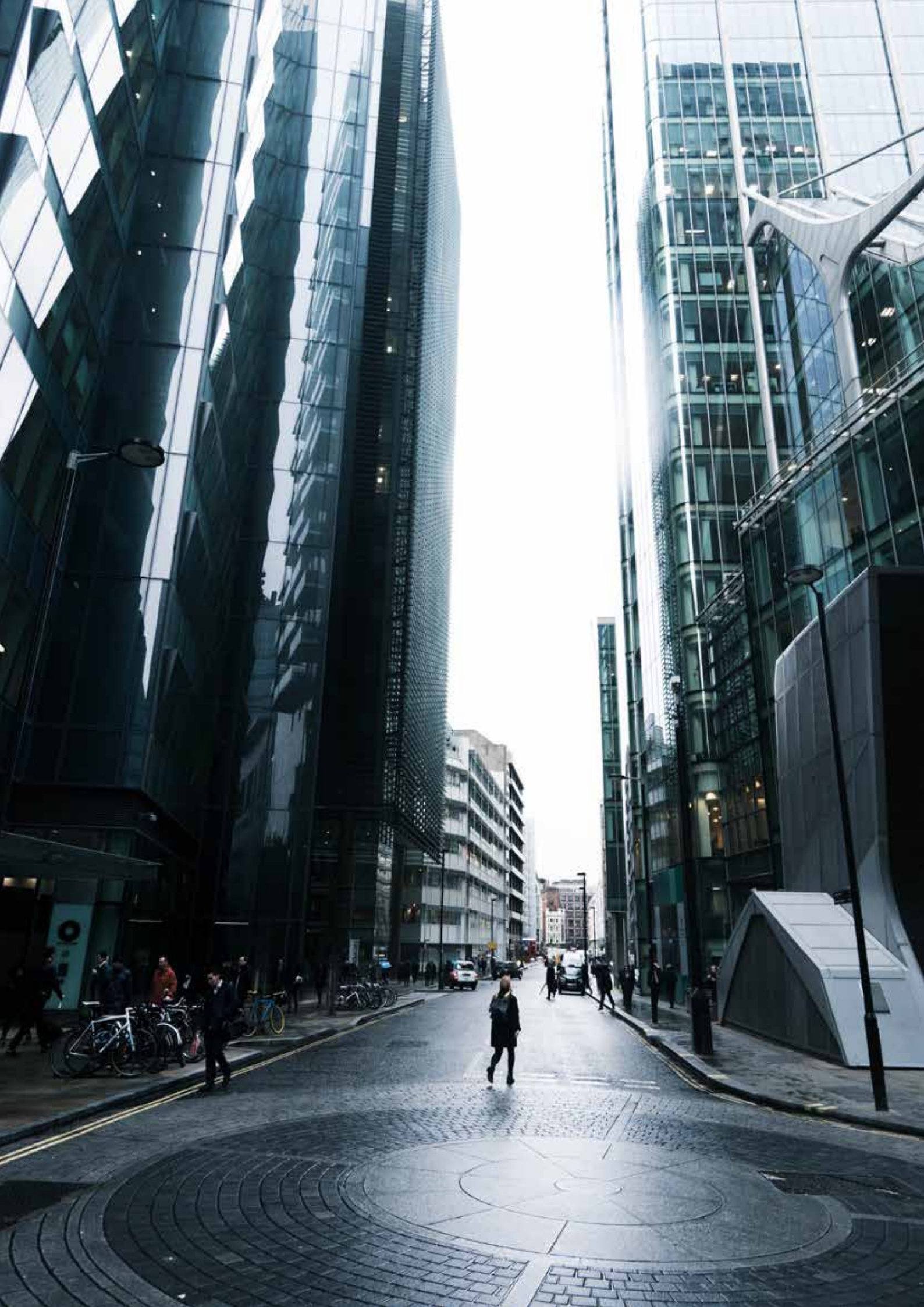
- A crime is in progress
- Someone suspected of a crime is nearby
- When there is danger to life
- When violence is being used or threatened

In the event of an attack

If, in spite of the precautions adopted, an attack has happened or is attempted, it is essential that:

- Police are alerted immediately
- You follow their advice/instruction
- Maintain the integrity of the scene (do not touch or clean up anything)
- No information is given other than to the police

In all other incidents where a police non-emergency response is required, dial 101.



Threats and Risks

Today, we all face a range of potential threats – from criminals, fraudsters, antagonists and extremists.

The objective may be to cause embarrassment, inconvenience, fear or distress, but may include an intent to cause serious physical injury or worse.

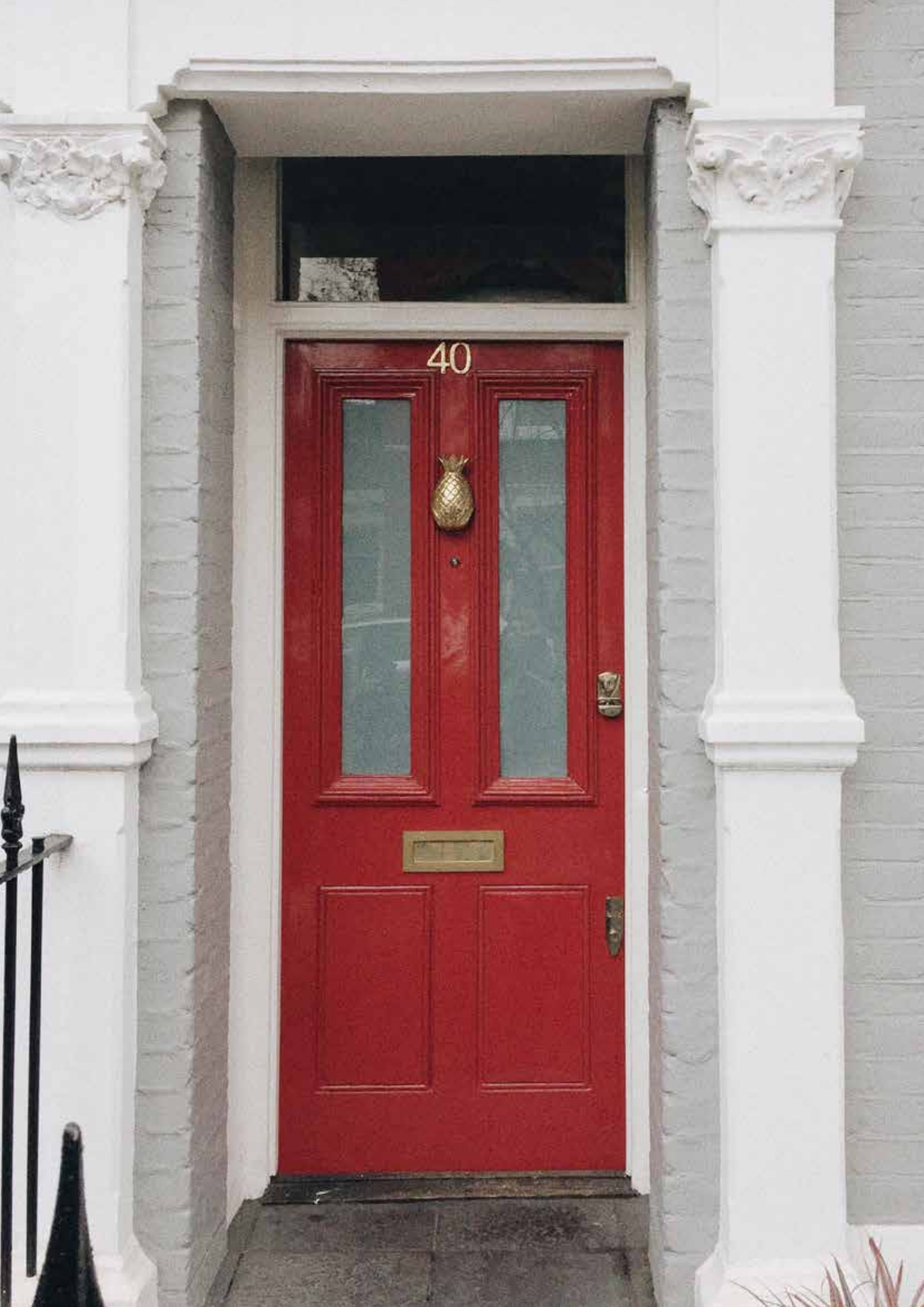
It is important to identify and recognise situations where you are at risk, so you can avoid them, or if this is not possible – reduce them.

For example, most people are relatively vulnerable when:

- Arriving/leaving home or place of work (particularly if alone or in the dark)
- Entering or leaving a vehicle
- When regular journeys can be predicted (i.e. - the same route, by the same method (bus/car), time and day)
- Answering the door at home or at work (to unknown persons)
- Working alone
- Being distracted when using an electronic device in a public place
- Unusual or new surroundings
- Whilst travelling (home or abroad)
- Interacting online
- Attending crowded places (with strangers such as nightclubs and sporting events)

The advice in this booklet is largely based on general crime prevention principles.

If these principles are integrated into your daily routine they could help to significantly reduce the risk to your personal security.


40

Security at Home

Encourage a security mind-set and apply sensible precautions to maximise security at home.

Routines

- Establish a routine for completing checks to confirm all doors and windows are secure before going to bed or leaving the premises
- Check for signs of break in before entering the property and for suspicious behaviour before departure
- Be aware of your surroundings and recognise situations where you may be more vulnerable

These precautions increase opportunities to spot unusual or suspicious behaviour.

Perimeter

To deter intruders, there are reasonable measures that can be taken to reduce vulnerabilities to the home and protect the perimeter of the property. Keep fences and walls in a good state of repair. It is important that boundaries clearly define the difference between public and private space.

- Front boundaries should be kept low, not exceeding 1.0 metre in height, to remove hiding places and provide good natural surveillance
- Side and rear boundaries should provide robust defensive barriers to a minimum height of 1.8 metres. An additional diamond style trellis topping (not exceeding 300mm) is difficult to climb and provides an ideal framework for spiky defensive planting, such as climbing roses

Any boundary structure at a height exceeding 1.8 metres which may be considered permanent, may require approval from the local authority planning department. Approval must be sought before the structure is constructed.

Gates

Side and rear gates should be in a good state of repair. They should be the same height as the side and rear boundaries (minimum 1.8 metres), be lockable and located at, or as close to the front building line as possible to avoid recessed areas.

Garages, outbuildings and sheds

These measures should be considered in order to reduce recognised vulnerabilities:

- Keep locked when not in use
- Metal up-and-over garage doors can be secured by fitting purpose made locks to either side, approximately 300mm up from the floor, or by fitting an external floor mounted locking ‘T’ bar with a closed shackle padlock
- Wooden garage double doors can be secured externally with two substantial hasps and staples with closed shackle padlocks, one towards the top and one towards the bottom to reduce leverage points
- Wooden side and rear doors can be secured with a BS 3621:2017 5-lever mortice deadlock or sash lock fitted half way up the leading edge of the door, with internal locking throw bolts or mortice rack bolts fitted one third from the top and bottom to reduce leverage points. The door will need to be at least 44mm thick to accommodate the lock

- Shed doors can be secured externally with two substantial hasps and staples with closed shackle padlocks, one towards the top and one towards the bottom to reduce leverage points. External hinge screws should be replaced with security screws to prevent them being removed and access gained this way
- Windows should have key operated locks and can be further secured with internal diamond mesh grilles
- Check garage doors and windows each morning for signs of forced entry
- Ensure tools and ladders, which could be used to access your home, are locked away or securely fixed (i.e. locked to a structure if space is at a premium)
- Keep the area around your home clear and tidy. This will assist you to identify unusual or suspicious objects and remove anything that could potentially be used to cause damage, e.g. loose bricks, large stones and garden ornaments
- If possible, keep your dustbin/recycling bins behind and away from secure gates or secured to a structure (until collection day) to prevent them being used as climbing aids

For further information:
www.soldsecure.com

Doors, windows and locks

A large proportion of newly built properties have been awarded 'Secured by Design (SBD)' certification, which means that they have had attack tested doors and windows installed under the SBD Scheme.

Some existing properties have had their doors and/or windows replaced with attack tested products that meet BS PAS 24:2016 or the equivalent, which includes the door and/or window, frame, locks, fittings and glazing. If there is documentation to confirm that this is the case, the measures detailed in this section will not be required.

Alternatively there may be documentation to prove that an existing building has had the doors and/or windows replaced to the above standard.

For further information:
www.securedbydesign.com

Security measures to be considered:

- Establish a routine for completing checks to confirm all doors and windows are secure before going to bed or leaving the house
- Ensure good quality locks are fitted to external doors and access windows
- Solid timber doors should be at least 44mm thick and supported with substantial hinges. Hinge bolts (metal pins that automatically engage or disengage as the door is opened or closed) can provide additional security, particularly for outward opening doors where the hinges are exposed
- A house with a solid timber front door should have a Kitemark (British standard or European Standard) BS 3621:2017 5-lever mortice deadlock (single point locking mechanism that can be opened or deadlocked with a key from both the inside and outside), fitted one third of the way up the leading edge
- A solid timber front door belonging to a flat or house that has been converted into flats or separate rooms should have a Kitemark BS 8621:2017 deadlock (all of the security benefits of a BS 3621:2017 lock, but has an internal thumb turn to enable quick exit without a key), fitted one third of the way up the leading edge of the door (see LACORS Housing - Fire Safety Guidance)*
- A surface mounted BS 3621:2017 automatic deadlocking rim latch lock for a house or BS 8621:2017 automatic deadlocking escape night latch lock for flats or separate rooms in converted houses should be fitted one third of the way down the leading edge
- Fit a 'Door and Hardware Federation Technical Specification (DHF TS) 003' fixed arm limiter to outer doors and make sure you use it
- Fit an internal shield/cowl (letter guard) to prevent car and house keys being fished through the opening. Alternatively, if the risk dictates, either blank off the letterbox slot and fit an external mailbox or fit an internal fire-proof letterbox

* LACORS is the body which co-ordinates local authority regulators and has published guidance on fire safety in residential accommodation including single dwellings, shared houses, bedsits, flats and flats of multiple occupation. The purpose of LACORS guidance is to provide a common set of guidance for each type of property, irrespective of which legislation applies.

- To protect thumb turn locks from being opened from outside, adjacent glass panels should be replaced with laminated glass which meets the minimum requirements of BS EN 356: 2000 class P1A. Alternatives are security film which meets the minimum requirements of BS EN 356: 2000 class P1, installed to the edge of the glass, under the beading or fixed internal grilles that meet one of the following:
  - LPS 1175 Issue 7.2:2014 SR1
  - LPS 1175 Issue 8:2018 SR 1/A1
  - STS 202 Issue 7:2016 Burglary Rating 1
  - LPS 2081 Issue 1.1:2016 SR A

If the door has a key operated multi-locking mechanism, make sure that you always lock it with a key. Simply closing the door and pushing the handle up will not prevent someone entering. You must push the handle up to engage the multi-locking mechanism and then use the thumb turn or key to lock it – LIFT, LOCK, REMOVE.

- Remember to keep the key out of sight but in a secure, accessible place in case of fire
- A UPVC, aluminum or composite doors, including external double/French or patio doors, will often have multi-point locking mechanisms. This should include either a DHF TS 007 Kitemarked 3-star cylinder or alternatively a DHF TS 007 1-star cylinder plus a pair of DHF TS 007 2-star handles. If not, these can usually be upgraded quickly and easily
- Solid timber side and rear doors should have a BS 3621: 2017 5-lever mortice deadlock or sash lock fitted half way up the leading edge of the door, with locking throw bolts or mortice rack bolts fitted one third from the top and bottom on the leading edge

- Lower hardwood panels can be reinforced internally with a 12mm overlapping plywood panel, glued and screwed into the door. The void created between the existing hardwood panel and the overlapping plywood panel should be infilled with chipboard of an appropriate thickness
- Patio doors should have a minimum of three locking points, with an anti-lift device to prevent the sliding door being lifted off its track. Surface mounted patio locks can be fitted to provide additional security
- Solid timber external glazed double doorsets should have a Kitemark BS 3621:2017 5-lever mortice sash lock fitted half way up the leading edge, with either mortice rack bolts or surface mounted locking throw bolts fitted to the top and bottom of each of the two doors, securing into the frame, not into the opposing leaf
- Double doors require two pairs of hinge bolts located as close as possible to the hinges. Alternatively, new hinges with integral bolts can be fitted
- A DHF TS 002 door viewer or audio/visual door entry system (video entry/intercom) will enable you to identify callers before you open the door. Even then, only open the door with the fixed arm limiter on
- All accessible windows should have key operated locks, unless they are designated fire escape routes. Ideally windows will have multi-point locking, but if not, additional surface mounted key operated locks can be fitted
- Easily accessible externally beaded windows should have the glazed panels secured with security clips, double sided security tape or silicone sealant which has been applied to the frame and the glazed panel bedded onto it
- Obscure the view into your home by fitting blinds, curtains or film including glazed exterior doors. Get into the habit of closing curtains or blinds when occupying a well-lit room

Replacement door and window standards

If you replace doors, windows and security products, ensure they have been tested to withstand attack and meet one of the following standards:

For doors, one of the following:

- PAS 24:2016
- STS 201 Issue 7:2015
- LPS 1175 Issue 7.2:2014 SR 2+

For windows, one of the following:

- PAS 24:2016
- STS 204 Issue 6:2016
- LPS 1175 Issue 7.2:2014 SR 1
- LPS 1175 Issue 8:2018 SR 1/A1
- STS 202 Issue 7:2016 BR1
- LPS 2081 Issue 1.1:2016 SR A

For further guidance:
www.securedbydesign.com
All security improvements should be made in consultation with your insurance company.

Key care

Improvements in keyless technology now allows the user to gain entry to a property or vehicle using a fob that emits a signal to release the locking device.

Criminals have identified that a 'relay' can replicate the signal to unlock the mechanism and gain entry illegally.

To reduce this risk of compromise for both (keyless and for conventional keys) the following should be applied:

- Keep keys (keyless fobs – in a signal blocking pouch or faraday bag) out of sight and away from doors and windows
- Do not leave keys under the doormat or in other obvious hiding places. It is better to give responsible members of the household their own keys
- Do not label your keys – if you need to identify keys, use a random colour-code
- Keep control of your keys, make sure you know who has copies and if you cannot account for all the keys, change the locks. Do not give keys to people you do not know, e.g. trades people
- Make sure the keys for doors and windows which could be used to exit the building in the event of a fire are readily accessible. They should not be visible or easily reached from outside

Alarms

Intruders do not want to be seen or heard, so setting off an alarm and attracting attention can be an effective deterrent.

It is recommended that a contractor who is affiliated to one of the recognised alarm inspectorate bodies, such as the National Security Inspectorate (NSI) or the Security Systems and Alarms Inspection Board (SSAIB) are contracted to undertake an installation.

For more information and advice, approach an insurance company and or an accredited trade body for the best alarm suitable for the situation/property.

Generally, there are four types of intruder alarm system:

1. Monitored: may provide a police response via the alarm company
2. Speech dialer: automatically calls pre-programmed key-holders (not police).
3. Audible only: relies on neighbours or passers-by to react
4. Smart Home Security: relies on an internet based app alert sent to a smartphone or tablet etc.

Additional options to consider:

- To maximise the deterrent, place external, active alarm bell boxes with flashing lights and sounders at the front and back of the property (burglar alarms)
- Consider fitting mains-operated smoke detectors or a fire alarm system in your home, if there is not already one installed. Have a fire extinguisher for example, available for emergencies
- Consider door alarms which announce when the door sensor contact is broken e.g "Front door open" designed to alert parents/carers but this can also be a good warning of intruders

NB: that DIY alarms will not necessarily receive a police response and that smart devices can be compromised by third parties.

Lighting

Good external lighting can help to deter intruders.

- Low wattage lighting is recommended to illuminate all external doors, car parking and garage areas and footpaths leading to your home
- External lighting should switch on using a photo electric cell (dusk to dawn) with a manual override
- Bollard lighting is not recommended as it does not project sufficient light at the right height to aid facial verification and reduce the fear of crime
- Consider fitting other forms of security lighting for use in emergencies, or if suspicion is roused. Floodlights, sited in strategic places, make it difficult for would-be assailants to hide from view
- Always have reserve lighting available such as a torch. Consider a torch with between 100-250 lumens

Any changes should be completed by a competent installer who is accredited and approved by The Institute of Lighting Professionals (ILP).

The installer should have the professional and technical competence to assess the levels of lighting required to improve the security.

CCTV

When considering the use of CCTV, the primary consideration must be for other people's privacy.

Seek further advice from a professional CCTV installer accredited to one of the recognised CCTV inspectorate bodies, such as the National Security Inspectorate (NSI) or the Security Systems and Alarms Inspection Board (SSAIB).

If the CCTV captures images within the boundary of the private domestic property (including the garden), then data protection laws will not apply.

However if the system captures images of people outside the boundary of the private domestic property; e.g. a neighbour's house or garden, shared spaces, or on a public footpath or street, then the following legislation will apply:

- Protection of Freedoms Act 2012
- Data Protection Act 1998 (DPA) and General Data Protection Regulations (GDPR)

Information Commissioner's Office (ICO)

It is the responsibility of the owner to protect the privacy of others, however since 2018, there is no longer a requirement for the owner to register with the ICO.

For more information about the legal requirements of CCTV:
https://ico.org.uk/your-data-matters/domestic-cctv-systems-guidance-for-people-using-cctv/

Subject Access Request (SAR)

Individuals have a right to access the personal data you hold about them, including imagery and audio where applicable. This request can be made to you verbally or in writing.

You must respond to a SAR within one month and provide the requesting individual with a copy of the data.

You should delete footage of people if they ask you to do so within one month of the request being made.

You can refuse to delete it if you specifically need to retain it for a genuine legal dispute. If this is the case, you should confirm this with the individual and tell them that your decision can be challenged in court or through a complaint to the ICO.

Visitors

The safest option is not to open the door to strangers in any circumstances. A door intercom system permits you to speak to a caller without opening the door.

Other measures could include:

- Fit a door viewer with a privacy cover (DHF TS 002) or audio/visual electronic door entry device to positively identify callers before you open the door
- A fixed arm door limiter will allow you to open the door a little way to speak to a caller without opening the door
- Ask friends and relatives to inform you of intended visits
- Arrange fixed times for tradespeople to call; check their identity on arrival and never leave them alone in the house
- Be wary of late night callers to your home
- Instruct children never to answer the door or let strangers in to your home

Waste disposal

When discarding sensitive, confidential or personal material, ensure that you treat it as confidential waste and shred where possible. Packaging from expensive items should not be discarded in view of passers-by, as criminals could target your home.

Do:

- Shred correspondence, put it in a confidential waste bag and keep it safe (not in a public area) until it can be disposed of correctly
- Carefully dispose of CDs, DVDs, USBs, PCs, laptops, tablets and other devices that contain sensitive, confidential or personal data
- Ensure the packaging from expensive or high end purchases are discarded out of sight so not to alert others of these items being recently purchased or inside the property
- Separate it from normal waste

There are reputable companies that specialise in disposal of confidential waste and should be considered where applicable.

Neighbourhood Watch

A scheme for local residents who agree to keep an eye out for anything suspicious and tell one another or the police.

Neighbourhood Watch schemes can:

- Help to reduce crime and the opportunities for crime
- Be a good way to help people feel more secure in their neighbourhoods
- Encourage neighbourliness and closer communities

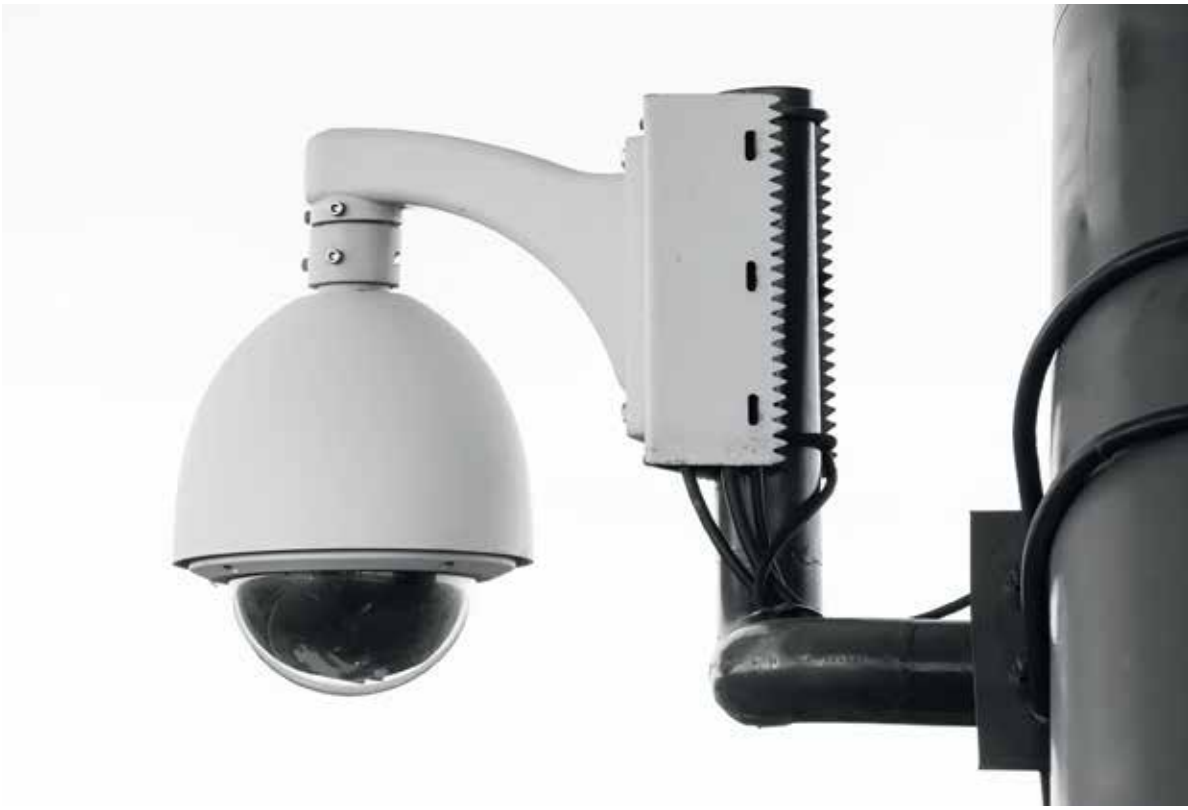
For further information:
www.ourwatch.org.uk

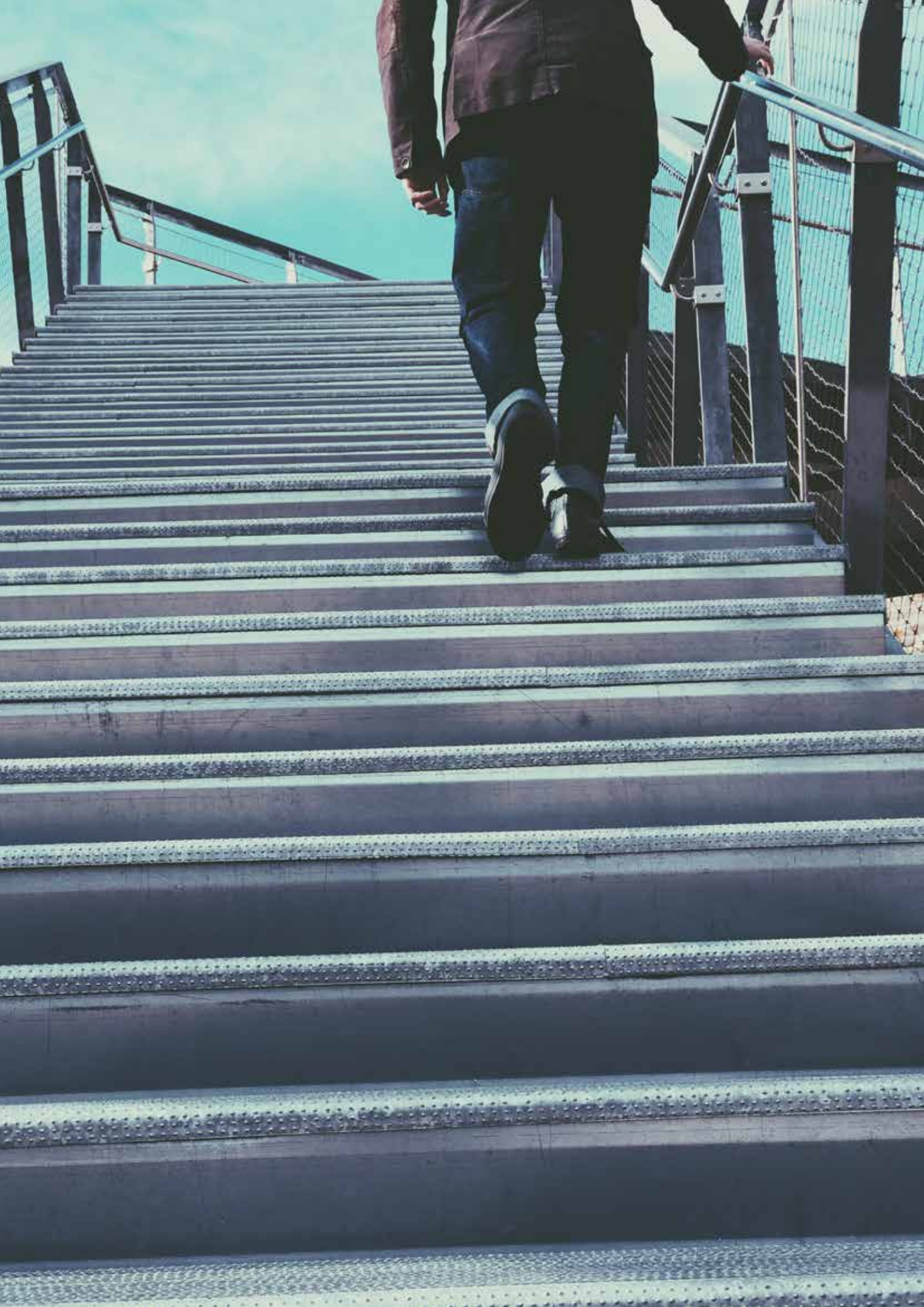
Fire safety

Ensure everyone in the household knows the evacuation plan and where the keys are located. Make sure that your home security improvements do not stop you from escaping quickly in the event of a fire.

Safety is important either when you're in, or away from the house. Fit approved smoke alarms with a British Standard Kitemark or Loss Prevention Certification Board (LPCB).

For further information:
www.gov.uk/government/publications/make-your-home-safe-from-fire





Security away from home

The chances of you or a member of your family becoming a victim of violent crime are low. Violent crimes by strangers in public places are rare and account for a very small percentage of recorded crime.

The principles of situational crime prevention theory state that three things must be present for a violent or aggressive incident to happen:

- a victim
- a perpetrator and
- an opportunity

By taking some suitable safety precautions, you can reduce the opportunities, and therefore the risk of experiencing violence or aggression.

- Plan ahead. Before you go out, think about how you are going to get home. Can you travel home with a friend? What time does the last bus/train leave?
- Avoid danger points like quiet or poorly lit alleyways, subways or isolated car parks. Walk down the middle of the pavement if the street is deserted
- If you do have to pass danger points, think about what you would do if you felt threatened
- If you feel worried, consider heading to a public place and/or somewhere you know there will be other people, for example a garage or shop
- If you are at all worried, try and stay near a group of people
- Try to keep both hands free and do not walk with your hands in your pockets
- Try to use well-lit, busy streets and use the route you know best
- Whenever possible, walk facing oncoming traffic to avoid vehicles approaching from behind you
- Avoid passing stationary cars with their engines running and people sitting in them
- If you do have to walk in the same direction as the traffic and a vehicle pulls up suddenly alongside you, turn and walk or run in the other direction
- Never accept a lift from a stranger or someone you do not know well, even if there is poor weather or you are late. Consider calling a friend or licensed cab
- Keep your mind on your surroundings – remember if you are talking on your mobile phone or wearing audio/noise cancelling headphones, you will not be aware of potential problems near you
- Be particularly careful when using cashpoint machines. Make sure nobody is loitering nearby, shield the keypad whilst tapping in the PIN code, do not count your money in the middle of the street and report anything unusual
- If you think you are being followed, trust your instincts and take action. As confidently as you can, cross the road, turning to see who is behind you. If you are still being followed, keep moving. Make for a busy area and tell people what is happening. If necessary, call the police by dialing 999
- Spread your valuables around (bag, jacket, trousers etc.) It's a good idea to keep valuables such as wallets in an inside pocket
- Don't display your valuables such as a mobile phone, laptop, jewellery or watch. Keep such items covered in a pocket or bag whenever possible

- Consider carrying a personal safety alarm, or download a personal safety app on your mobile phone, which can be used to disorientate an attacker giving you vital seconds to get away or send a message to your emergency contacts
- Let a friend know of your movements, planned routes, location and return time

For further advice:
www.suzylamplugh.org

Lone working

A lone worker is a person who works in an environment by themselves or without direct supervision. They can find themselves working in an array of surroundings such as rural, residential streets, factories, large or small buildings or within a vehicle.
Lone working can last for prolonged or for short periods of time.

It's important to recognise the potential for a situation to quickly develop and increase your vulnerabilities; some useful points to consider when lone working are listed below:

Minimise risk:

- Consult your Employers Lone Working Risk Assessment and adhere to employer guidance and policy
- Make sure that your mobile, lone worker device (BS 8484:2016), or tracker is charged and with you
- Prior to setting out, ensure someone knows your whereabouts and when you're next expected to check in with them
- Do not publicise your routine outside your line management or on social media (such as on an office white board in an open plan office)
- If engaged with a threatening person, create distance, remain calm, and remove yourself; personal safety comes first
- Keep your work tools close to prevent them being used to threaten or cause harm
- If working alone, do not wear audio headphones
- Don't take unnecessary risks

- Report all incidents to your employer and, where appropriate, to the police. Have a clear escalation point if something isn't right, with clear guidance on what to report to who, and when. For instance, in an emergency, call 999, but if you notice suspicious behaviour (that doesn't create an immediate threat) note information (descriptions, vehicle make, model, colour and registration number) and report it to an appropriate person (line manager, security manager, site manager)

Maintain situational awareness:

- Take note of your surroundings and note alternative exits
- When lone working at a new or unfamiliar site, consider the exit routes and make note of local landmarks that could offer assistance in an emergency (such as local shops, libraries, police stations)
- Carry your ID, cash and contact numbers with you (in case of vehicle theft/need to make quick getaway)
- Trust your instincts

For further information:
www.hse.gov.uk
www.suzylamplugh.org

A lone worker device can come in a number of guises including: a small fob, handheld or app based on a smart phone. The sole purpose of the lone worker device is to summon immediate assistance when activated. These are designed to be carried discreetly and when activated can disorientate the aggressor, giving vital seconds to get away.

Meetings

When conducting public or private meetings, particularly where you may be alone in an office, you may encounter people who are confrontational or in different states of distress. They may display different emotions and be upset, angry or aggressive.

It is important to continually assess your surroundings, the person's behaviour and potential threats before and during meetings. You should take proportionate steps to reduce the risks and stay safe. Once a meeting plan is in place this should be regularly reviewed and tested involving staff.

The plan should include:

- A Standard Operating Plan (SOP) with an Emergency Plan

Outline what to do in an emergency. The plan should include if the person is displaying signs of irrational, aggressive, or confrontational behaviour. If unsafe terminate the meeting - create distance, disengage and call for assistance. Report incidents to your employer and/or police as appropriate.

Risk Assess
The following checklist is not exhaustive, but should form part of your initial and dynamic risk assessment. Consider additional training to ensure that you have the necessary skills to deal with a potentially volatile situation.

You will need to consider the following:

Location
Is the meeting room appropriate? i.e no items lying around that could be used as weapons?

Seating
Consider the seating positons.
Are you sat at their level? Are you using eye contact and open hand gestures to display a non-confrontational and receptive body language?

Consider using the chair nearest the door, so egress can be achieved quickly if required

Escape route
The route to be taken in an emergency.
Is there a safe area for those involved including staff?

Delaying Plan
Consider an excuse to remove yourself from the situation without causing further issues

Help and assistance In the event of an incident
Have an agreed phrase to alert staff in the event

Mobile Phone
Carry at all times. Check the battery is charged and has a signal

Lone Worker Device/Personal Safety Alarm
Carry at all times, check it is working.

Panic Button
Is this facility available in the room?

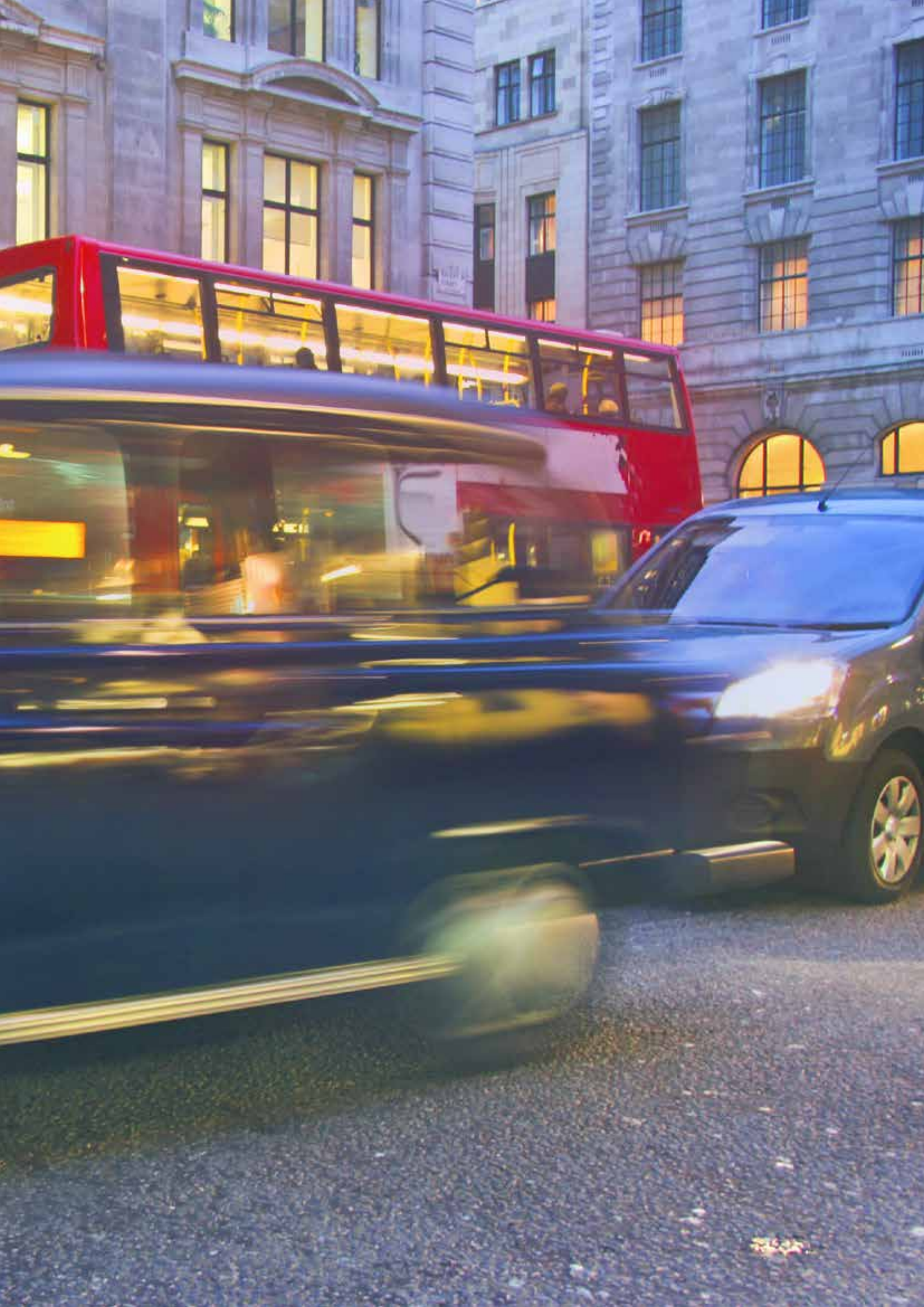
Booking System
Create an appointment system which identifies the visitor, room location, start and finishing times and ensure checks are conducted to reduce the risk. Ensure others are aware of the time and location of surgery/ meeting. Checks could include confirming the name, address and contact details.

Meeting Room
Designate a room that's accessible to other members of staff who can provide assistance if required in the case of emergency.
If there's a risk of aggressive or unacceptable behaviour invite a colleague to join the meeting.

Incident Log
An incident log should be created to record all incidents and should be noted immediately after the incident, as anecdotal accounts can be unreliable. The log should be dated, timed and signed.

All completed incident logs must be regularly reviewed to identify individuals who have previously displayed aggressive or unacceptable behaviour.

This will allow those who have displayed unacceptable behaviour to be excluded from future meetings.



Travel

Security advice for travelling in either personal vehicles or using public transport

Motor vehicles

It is important to consider the security of any vehicles you use regularly; this includes personal and work use. You may wish to consider alternative routes and times for regular journeys to reduce the predictability of your travel routines. Always carry a fully charged mobile phone or a portable power bank/charger as a backup.

Before every journey you should:

- Lock the vehicle doors and boot during your journey. Open windows only enough for ventilation purposes, particularly in town. Keep your distance from the vehicle in front
- Always check you have the fuel required to complete your journey. Ensure you have adequate breakdown recovery cover
- If you break down, pull as far off the road as you can and put your hazard warning lights on. Call your breakdown organisation and let them know if you are travelling alone or if you have children with you
- If you break down on a motorway, it is usually safer to wait for assistance outside your vehicle, standing on the verge or behind the crash barrier. Take your keys with you and shut all doors except the one nearest to you, which you can leave wide open so that you can get in quickly if you need to
- Make a habit of checking the road before leaving your home or place of work. Note any suspicious or strange vehicles (make, model, colour and registration number) to police if appropriate
- If the driver of another vehicle forces you to stop and then gets out of their vehicle, stay in your vehicle, keep the engine running and, if you need to, manoeuvre around them to get away
- Do not give or accept lifts from people you don't know or from someone who is under the influence of alcohol and or/drugs

If you think you are being followed:

- Try to keep calm
- Keep the vehicle moving, even if only slowly
- Close all windows and ensure doors/boot are locked
- Contact the police immediately – if safe to do so
- Do not drive home, if you can, make your way towards the nearest open police station or a busy area. Continuously sound the horn or dial 999
- If possible, record the registration number of any suspicious vehicle

Vehicle security

When leaving your vehicle ensure that it is locked and consider the following:

- At home or in work, park your car in a locked garage or a secure parking area. If neither of these is an option, leave your vehicle where it can be seen by the general public. Try to park in a well-lit area, within view of a CCTV camera or in a staffed car park
- Ensure that the windows and sun roof are closed and it is fully locked and secure
- Remove satellite navigation devices where possible, including the support cradle/ suction pads. Wipe away any suction marks left on the windscreen or dashboard
- Be alert to any visual changes to your vehicle. If you notice a suspicious object on or near the vehicle, do not approach or enter it. Contact the police and give them the location and registration number of your vehicle
- Carry a torch so you can check your vehicle after dark
- Never leave laptops, documents, corporate clothing, jackets, parking permits or papers in unattended vehicles, as this may cause you and/or your employer to be identifiable
- Fold in wing mirrors to discourage vandalism
- On frosty mornings, don't leave your vehicle unattended with the engine running whilst it defrosts
- Do not leave your vehicle unlocked on garage forecourts

Regular journeys

- If possible, avoid setting patterns in your travel arrangement which could make it easy for someone to predict your whereabouts. Vary your routes and times of departure as much as possible
- Make sure a trusted confidant knows your route and the time you expect to arrive

Public transport

Taxis/Public Service Vehicles (PSV)

It is advisable to find out which licenced taxis operate in your area and plan your journey in advance. Avoid private-hire cars that tout for business and are unlicensed. Use taxis that display the public notices and licences required for regulated legal taxis.

- Call and book ahead, so there is a record of your booking and the vehicle is properly licensed. If possible, do not use waiting taxis
- Share information about your journey and the vehicle you're using with someone you trust
- Do not share a taxi with someone you do not know
- Consider alternative pick-up or drop-off points to your home or place of work
- Do not wear anything that would disclose your occupation
- Always sit behind the driver in the back seat
- If you feel uneasy, ask to be let out in a well-lit area where there are plenty of people
- Report any concerns to the licensing authority or police

For further advice and guidance:
www.suzylamplugh.org

Rail, sea and air

When travelling by any of these transport options consider the following:

- If travelling by train, enter a carriage that is already occupied. Keep luggage in view, if you have to store it on a rack
- Between packing your bags and check-in, maintain control of all items, both checked and carry-on luggage
- Never leave your luggage unattended
- If you have to surrender your luggage, make sure you get the correct bags back. Do not open them unless you are confident they have not been tampered with. Secure zip loops with a padlock or use a lockable luggage strap
- When travelling by ship, be cautious about walking on deck at night. Try to obtain a cabin and ensure that the door is kept locked at all times
- Do not take responsibility for the luggage of people you do not know
- Consider carrying a personal safety alarm with you

Further guidance on safety on, or near, the railway is available from British Transport Police (BTP):
www.btp.police.uk/safety

Report crime or incidents discreetly by texting 61016.

The text number is monitored 24/7 and, while it is not for reporting emergencies, BTP will send officers if required.

Buying vehicles

When buying a car you should also think about the security.

The New Vehicle Security Assessment (NVSA) and British Insurance Vehicle Security Awards should be considered as part of the decision making process.

For more information:
www.thatcham.org

Protect yourself by:

- Arranging to meet the person selling the car at their house, not at your house or another meeting place.
- Consider your method of payment; avoid carrying large amounts of cash.

Ask the seller for the vehicle:

- Registration number (on the number plate)
- MOT test number
- Mileage
- Make and model

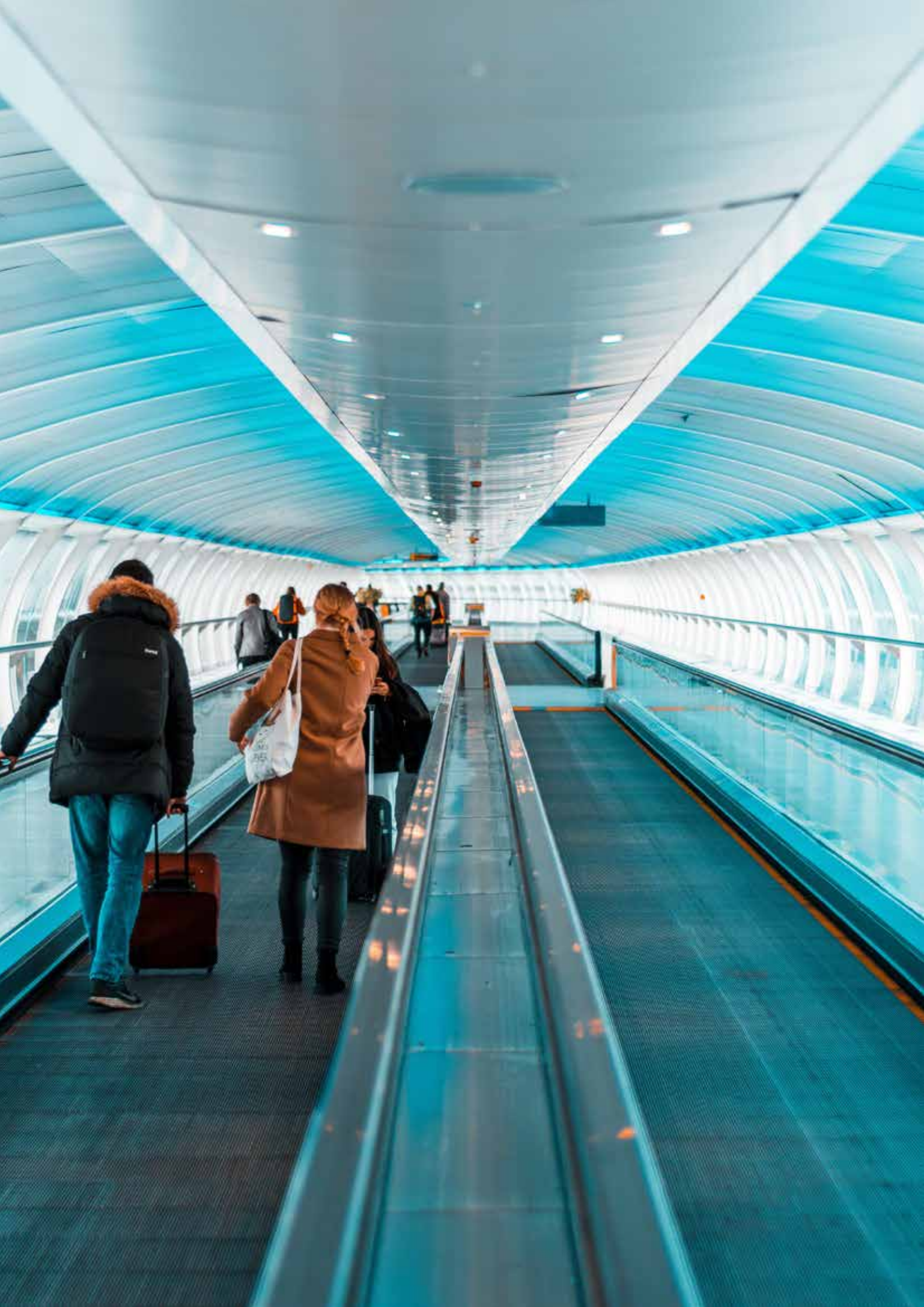
Use the DVLA's free vehicle checker to make sure what the seller tells you matches the DVLA's records.

For more information:
www.gov.uk/get-vehicle-information-from-dvla

Selling vehicles

When selling a vehicle, think about the security:

- Arrange to meet the buyer at an open public location; you are comfortable with in daylight
- Disconnect your electronic devices from the vehicles pairing (Bluetooth) system and delete any information that may be left
- Delete map and address from the in car navigation system



Working away from home (UK or Overseas)

Before travelling ensure that you make time to research where you're going, even if the country appears to be safe.

Make sure co-travellers understand how to behave and know their responsibilities whilst travelling and representing their organisation. Refrain from posting information about the trip on social media.

Before travelling, make sure that someone at home knows:

- The itinerary and any deviation from the scheduled itinerary
- An emergency point of contact telephone number
- Who you are going to see
- How you will travel
- When you expect to arrive and when you expect to return
- What to do in the event of undue delay

Make sure you know the local equivalent of 999 and memorise your location.

Hotels

Ensure that the hotel has been booked through your organisation's approved process or through a reputable travel provider.

- Where possible, avoid regularly using the same hotel
- At reception, try to avoid other people hearing your name and room number
- Never see visitors in your hotel room. Meet visitors in a recognised place of business, in a public space or a meeting room (where venue staff will be aware of the arrangement)
- Be wary of hotel paging or public address systems. It is advisable to prearrange with the hotel for callers to leave their name and contact details with reception. This will reduce the risk of identification and possible attack
- If travelling you could take a door wedge. It can be placed under the door to prevent the door being opened from the outside
- Know the fire and escape route options

Hotel safes can be useful for securing valuable items such as currency and jewellery. It should not be used for securing sensitive or personal information as they can be opened with a master key or override code.

Further information before you travel:
www.gov.uk/foreign-travel-advice

www.cpni.gov.uk

Physical Threats

Firearms and weapons attack: Whilst Marauding Terrorist Attacks (MTA) attacks are rare, in the event of such an attack, it helps to be prepared. Should such an attack occur, remember the words: Run. Hide. Tell.

RUN

- Escape if you can
- Consider the safest options
- Is there a safe route? Run, if not Hide
- Can you get there without exposing yourself to greater danger?
- Insist others leave with you, but don't let their indecision slow you down.
- Leave belongings behind.
- Do not attempt to film the incident. Run

HIDE

- If you cannot Run, Hide
- Find cover from gunfire
- If you can see the attacker, they may be able to see you. Cover from view does not mean you are safe. Bullets go through glass, brick, wood and metal. You must still hide, even If you are behind a locked door
- Find cover from gunfire e.g. substantial brickwork/heavy reinforced walls
- Be aware of your exits
- Try not to get trapped
- Be quiet, silence your phone and turn off vibrate
- Lock/barricade yourself in
- Move away from the door

TELL

Call 999 – What do the police need to know? If you cannot speak or make a noise, listen to the instructions given to you by the call taker:

- Nature of the Incident: What is happening?
- Location: Where is the incident taking place? Give an address or general location
- Suspects: Where are the suspects?
- Direction: Where did you last see the suspects?
- Descriptions: Describe the attacker, numbers, features, clothing, weapons etc.
- Further information: Casualties, type of injury, building information, entrances, exits, hostages etc.
- Stop other people entering the building if it is safe to do so

Armed police response:

- Follow police officers instructions
- Remain calm
- Avoid sudden movements that may be considered a threat
- Keep your hands in view

Officers may:

- Point guns at you
- Treat you firmly
- Question you
- Be unable to distinguish you from the attacker
- Officers will evacuate you when it is safe to do so

Plan and prepare now. You must stay safe:

- What are your plans if there was an incident?
- What are the local plans? (personal emergency evacuation plan, first aid training etc.)
- Consider first aid when it is safe to do so

A short film about staying safe in the event of a marauding terrorist attack can be seen here:
www.gov.uk/government/publications/stay-safe-film

Hazardous substances

A hazardous substance can be any substance, whether solid, liquid or gas, that may cause harm. Hazardous substances are classified on the basis of their potential health effects, whether acute (immediate) or chronic (long term)

If you think someone has been exposed to a hazardous substance, use caution and keep a safe distance to avoid exposure yourself.

Tell those affected to:

Remove themselves

- From the immediate area to avoid further exposure to the substance
- Fresh air is important
- If skin is itching or in pain, find a water source
- REPORT to the emergency services 999

Remove outer clothing

- Try to avoid pulling clothing over the head, if possible
- Do not smoke, eat or drink
- Do not pull off clothing stuck to skin

Remove the substance

- From skin using a dry absorbent material to either soak it up or brush it off
- Rinse continually with water if skin is itching or in pain

Remember: Exposure is not always obvious.

Signs can include:

- The presence of hazardous or unusual materials
- A change in environment such as unexplained vapour, odd smells or tastes
- Unexpected signs of skin, eye or airway irritation, nausea, vomiting, twitching, sweating, disorientation, breathing difficulties

Be aware of your surroundings and move away from suspicious items.

Act quickly. These actions could save lives.

For further information:
www.gov.uk/government/publications/remove-guidance-on-removing-hazardous-substances

Demonstrations

It is possible that your profession or association with an organisation could lead to protesters gathering at your home or work.

If this happens:

- Stay calm – Such protests may intimidate but will not necessarily lead to a physical threat
- Remain inside
- Close and lock doors and windows and draw the curtains/blinds
- If this happens inform the police using 999
- Inform your workplace/colleagues/family members
- Do not, in any way, respond to or antagonise the protesters
- Remain indoors, out of sight and avoid confrontation
- If possible, note descriptions of individuals, vehicles present and location of protestors (including numbers)
- If you have a CCTV system fitted that has recorded images of protesters, you should hand any footage obtained over to the police; it may assist with identification and provide evidence in cases where offences have been committed
- Postpone any expected visitors
- Await the arrival of the police

Other Threats

Unattended Items

Does the item look lost or suspicious?

Consider the HOT protocols:

Hidden?

- Has it been concealed or hidden from view?

Obviously suspicious?

- Does it have wires, circuit boards, batteries, tape or putty- like substances? Do you think the item poses an immediate threat to life?

Typical?

- Is the item typical of what you would expect to find in this location?
- Most lost property is found in locations where people congregate

If after applying the HOT protocols you still believe the item to be suspicious, call 999.

Delivered items

Letters, parcels, packages and other items delivered by post or courier have been used on occasions to disguise harmful devices and substances.

Delivered items may be explosive, incendiary, include sharps or blades, or contain chemical, biological or radiological material.

Other hazardous or offensive material such as faeces, have also been used in delivered items. Anyone receiving a suspicious delivery is unlikely to know what type it is, so procedures and precautions should cater for every eventuality.

A delivered item will probably have received fairly rough handling in the post, so is unlikely to detonate because it is moved. Any attempt to open such an item may activate it.

Threat items come in a wide range of shapes and sizes. A well-made device will look innocuous but may still have tell-tale signs.

Indicators of a suspicious delivered item:

General indicators that a delivered item may be of concern include:

- An unexpected item, especially if hand delivered
- A padded envelope (Jiffy Bag) or other bulky package
- An 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
- An envelope flap stuck down completely (normally gummed envelope flaps leave slight gaps at edges)
- Marked 'to be opened only by...' 'personal' or 'confidential'
- An item addressed to the organisation or a title (rather than a specific individual)
- Unexpected or unusual origin (postmark and/or return address)
- No return address or return address that cannot be verified
- 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 package
- Odours emanating from package

Explosive or incendiary indicators

Additional explosive or incendiary indicators include:

- Unusually heavy or uneven weight distribution
- Small hole(s) in envelope or wrapping
- The presence of wiring

White powder (CBR) indicators

Additional chemical, biological or radiological (CBR) indicators include:

- Powders or liquids emanating from package
- Wrapping stained by liquid leakage
- Marked with written warning(s)
- Unexpected items or materials found in package upon opening or x-raying (loose or in a container) such as powdered, crystalline or granular solids, liquids, sticky substances or residues
- Unexpected odours upon opening
- Sudden onset of illness or irritation of skin, eyes and nose

If in doubt call 999 and ask for the police. Clear the area immediately.

Do not attempt to open the letter or package. Avoid unnecessary handling.

Keep it separate so it is easily identifiable.

For further information:
www.cpni.gov.uk

www.gov.uk/government/organisations/national-counter-terrorism-security-office

Bomb Threats

If you receive a telephone threat you should:

- stay calm and listen carefully
- note the callers number, otherwise, dial BT 1471 to obtain the number once the call has ended
- record the call if you're able to do so
- if practical, keep the caller talking and alert a colleague to dial 999
- if the threat is a recorded message, write down as much detail as possible
- if the threat is received via text message do not reply to, forward or delete the message. Note the number of the sender and follow police advice

If the threat is received via email or social media application:

- do not reply to, forward or delete the message
- note the sender's email address or user name/user ID for social media application
- preserve all web log files to help the police investigation

Remember: Dial 999 and follow police advice.

Telephone threats and anonymous calls

Anonymous calls and telephone threats are usually intended to lower your morale or cause fear, alarm and distress.

These calls can be extremely distressing, but if it is bearable, keeping the caller talking can reveal important information. If possible keep a note pad and pen to hand.

If the call is not too upsetting, consider the following actions:

- Write down the details immediately, including date, time, length of call and exact words spoken
- Note details about the caller; e.g. gender, accent, a speech impediment
- Listen for any clues as to the intention of the caller or the specific threat
- Listen for background noise, which may provide valuable information about the location or circumstances of the caller (traffic, trains, children etc.).
- On termination of the call, operate any trace facility, such as BT 1471 service, and write down the number if registered
- Inform the police immediately if threats have been made
- Tell your children to hang up without responding, if they received such a call. You may decide that your children should not answer the telephone if there is a risk of a malicious call
- If you are persistently receiving silent calls, do not say anything when you answer. Legitimate callers will identify themselves and if it is the malicious caller you can hang up.

Preventative action you can take:

- Ensure you home phone number is ex-directory
- Use a caller display function, so that the call can be screened before being answered.
- Amend the outgoing message on your answer machine or voicemail. You should not provide any personal information or indicate that you are away from your property for any length of time
- The use of social media, smartphones and tablets has increased the potential for theft of information that could be used to target you. Get Safe Online provides practical advice on how to protect yourself, your computers, mobile devices and your business against fraud, identity theft, viruses and many other problems encountered online
- Consider registering with the Telephone Preference Service (TPS). TPS is the UK's only official 'Do Not Call' register for landline and mobile numbers. It allows individuals and businesses to opt out of unsolicited live sales and marketing calls. It's free to register a telephone number

For further information:
www.getsafeonline.org

www.tpsonline.org.uk

Mobile devices

You need to be aware of the security risks and take steps to protect your devices. Think about the activities you use your device for, such as online banking, personal emails, social media and photographs.

Could these be made public or used against you?

- Use all of the security facilities available, e.g. device tracking, screen and SIM passcodes
- Disable your Wi-Fi and Bluetooth connection when not in use
- Record the IMEI numbers for your phone and tablet. An IMEI is 15 numbers long and uniquely identifies your phone. It can be found on the phone box package, under the phone battery or by typing *#06# into your phone
- Change the default PIN for voicemail access
- Avoid using public Wi-Fi hotspots. These may not be secure
- Disable location services where possible and review privacy settings to prevent someone tracking your movements and identifying your home address or place of work
- Geotagging marks a video, photo or other media with a location, this can reveal private information to a third party*
- Remove metadata from pictures, especially ones taken from mobile phones before you post them online**

* Geotagging captures the image's location through latitude, longitude, altitude and compass bearing.

** Metadata can be the basic data such as author, date created, date modified and file size. Metadata can be created manually or through automation. www.cpni.gov.uk/system/files/documents/d3/e8/28-February-2017-Edited-In-house-My-Digital-Footprint-booklet.pdf

IT security and online communications

IT security helps to protect the internet enabled devices (smartphone, laptops, PCs) we all use and the services that we access both online and at work from theft or damage.

- Use a firewall and anti-virus software and keep them up to date. Run system scans regularly
- Be cautious when using third party applications. Malicious codes known as 'malware' can spread rapidly around social networks or via email
- Do not open emails from unknown or suspicious senders
- Treat all email attachments and links with caution. Where it exists, turn off the option to automatically download attachments to emails
- Use software controls that ensure only reputable websites can be accessed, reducing the risk of malicious software being installed onto your system
- Make sure that the latest updates to your device's operating system are promptly installed
- Check the security protection of your home and business Wi-Fi networks. Change the default (manufacturer) passcode
- Do not rename Wi-Fi using identifying details such as your family name
- Use a hard-to-guess password and never write it down. Do not tell anyone your password
- Do not use the same password for all security log-on purposes
- Shred CDs/DVDs before disposal if they contain sensitive information

For further information:
www.ncsc.gov.uk/section/about-ncsc/what-is-cyber-security

Online Social Networking (OSN)

The internet can be a valuable source of information, education and entertainment for all the family. However, you need to take precautions when using it, especially for social networking purposes.

Internet-based social networking sites such as Facebook, Twitter, LinkedIn and Instagram are popular applications that allow individuals to create a profile containing personal information and interact with other users. Review your privacy settings to prevent some or all of your OSN profiles being seen by a large audience.

Business networking sites such as LinkedIn also require personal profiles to be created, which normally include an individual's work history.

Whilst these applications are useful tools to communicate with others or advertise professional skills, publishing personal information on your OSN profiles presents potential risks:

- You may be susceptible to identity theft, as dates of birth, full names, home addresses and email details are key pieces of information for identity fraudsters. Some sites 'own' any data posted on them and may reserve the right to sell your details to third parties
- Posting information can put your personal safety at risk. If you provide too much information and do not have the appropriate privacy settings applied, your business or social network accounts can be a veritable 'gold mine' for those intent on building up a picture of your relationships, opinions, places of interest and any other subject that they may seek to exploit in the future

- Location-based information can be posted on social networks, especially from GPS-enabled mobile devices, which tells others exactly where you are or have been. This information is not secure and could be viewed by anyone, including those who may want to harm you or your family, friends and colleagues. The responsibility rests with you to ensure that no-one is put at risk due to what is disclosed
- Regularly check what information you can find out about yourself, your family or your business on-line and edit where able

You should not include personal details such as:

- Mobile phone numbers
- Personal or work addresses
- Employment details
- Level of security clearance
- Family members
- Hobbies and places frequented
- Vehicle details
- Work information on personal accounts

To avoid putting other people at risk, photographs of family, friends and colleagues should only be published with your consent and theirs.

If applicable, published photographs should not reveal your occupation, home or place of work. Review your account settings.

Disable photo and location tagging, so you have to approve another user identifying you in a photograph or being at a specific location. Ensure your privacy settings are adequate and your account is as locked down as it can be.

It is equally important that family and friends are made aware of any risk, in order for them to take suitable precautions with their online presence. This is especially relevant if they are used to posting content about the person 'at risk'.

For further information

ACT (Action Counters Terrorism) awareness E-learning app

The publically available ACT awareness app is designed to help the public spot the signs of suspicious behaviour and understand what to do in the event of a major event.

The app contains live-time information from Counter Terrorism Policing and protect security advice.

Powered by Urim, the ACT app is free for members of the public and businesses and has been developed in partnership with industry specialists from Marks and Spencer and Highfield e-Learning. Available from Google Play or App Store, the app will provide access to:

- Practical advice and guidance to help you protect your business, plus information on how to respond in the event of an attack
- Information on Counter Terrorism Policing's suite of ACT training products, plus access to the online e-Learning package
- Suite of National Counter Terrorism Security Office guidance videos
- Latest reference documents and publications
- ACT online reporting and anti-terrorist hotline
- Emergency Response and post incident guidance
- Live-time news updates from UK Protect

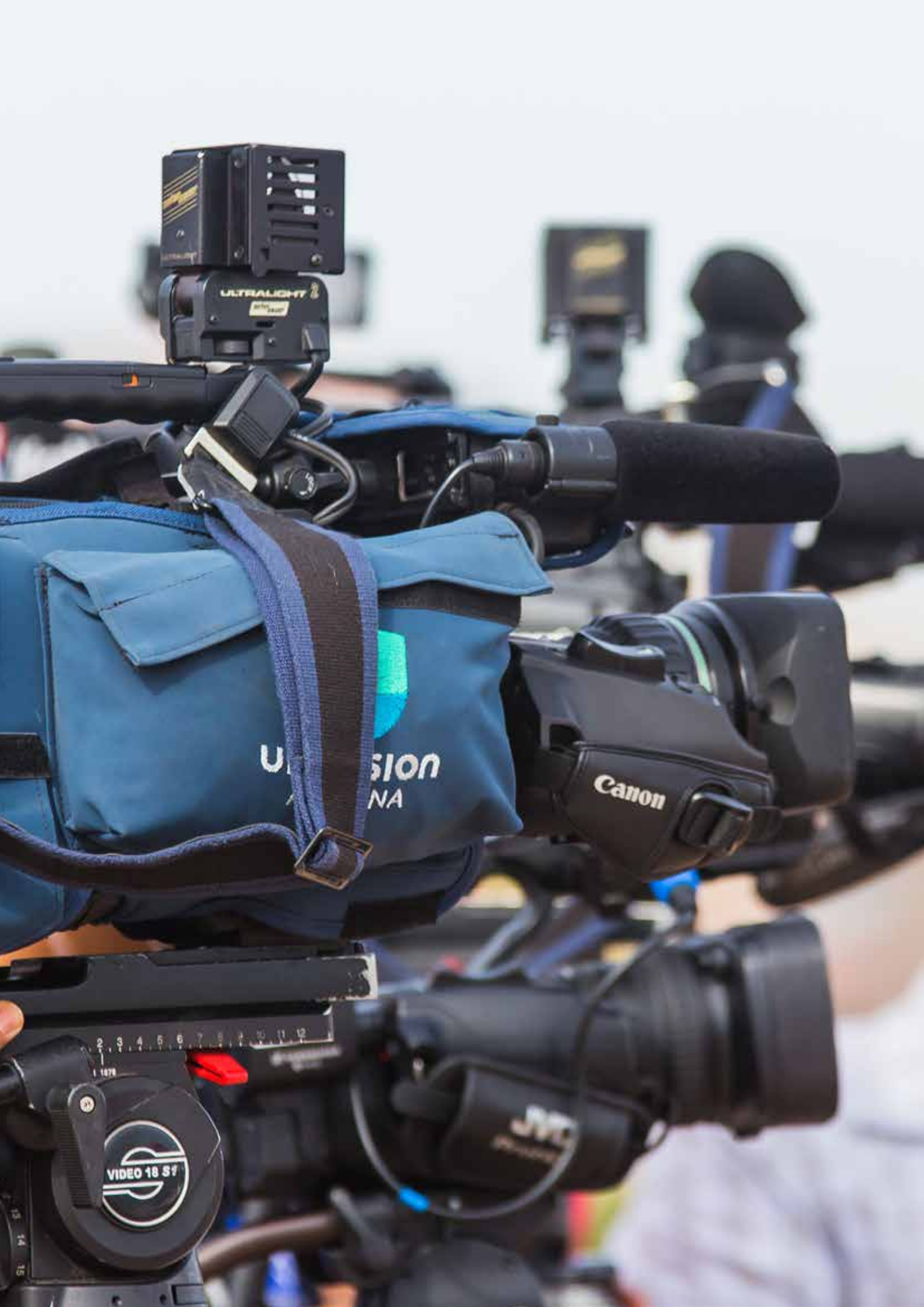
www.cpni.gov.uk/system/files/documents/d3/e8/28-February-2017-Edited-In-house-My-Digital-Footprint-booklet.pdf

www.ncsc.gov.uk/section/information-for/individuals-families

CHILDREN'S PERSONAL SAFETY ONLINE

Information and support for young people/parents and professionals is available at: www.thinkuknow.co.uk

Child Exploitation and Online Protection Centre (CEOP): www.ceop.police.uk


ULTRALIGHT
Canon
VIDEO 18 S1

Publicity and the media

Leafleting campaigns

Your neighbours may receive letters or leaflets describing in extreme terms the work that you do. Most people, whatever their personal view on the subject at issue, will be sympathetic towards anyone who is being victimised.

- You may want to talk to your neighbours
- All incidents should be logged and reported to police and to your employer
- Do not remove any posters or offensive notices found on your property without prior, careful examination
- Leaflets or other materials should be passed to police

Avoid revealing details about personal circumstances which might be of use to a person planning to target you or your business interests.

This includes interactions with the media, be it for work or social purposes.

It is impossible to provide advice to cater for every eventuality but the following are some examples of the kind of publicity which should be avoided or controlled:

- Home addresses and other identifying details should be excluded from business publications and online networks
- Work related press releases, publicity materials and website content should be reviewed to see if any information can be removed or amended to protect individuals
- Television camera crews and press photographers should not generally be allowed to enter private homes. However, where agreement is reached to grant interviews to the press on private premises or to the publication of articles about the private lives of interviewees or their families, the media should be asked not to publish details which would help to identify a home address or regular way of life
- The electoral roll is a source for commercial companies to obtain your personal information. You can seek advice on how to protect this information from your local authority
- If you have professional membership of any business-related organisation, ask them not to publish your full details or, if they do, to put them on a password-protected area of the site

Useful websites

Security advice

National Counter Terrorism Security Office:
www.gov.uk/government/organisations/national-counter-terrorism-security-office

Working with Counter Terrorism Security Advisors (CTSA):
www.gov.uk/government/publications/counter-terrorism-support-for-businesses-and-communities/working-with-counter-terrorism-security-advisers

Crowded Places Guidance:
https://www.gov.uk/government/publications/crowded-places-guidance

Marauding Terrorist Attack Guidance:
https://www.gov.uk/government/publications/marauding-terrorist-attacks

Centre for Protection of the National Infrastructure:
www.cpni.gov.uk

Foreign Travel advice:
www.gov.uk/foreign-travel-advice

General crime prevention advice

Secured By Design:
www.securedbydesign.com

Anti-fraud advice:
www.actionfraud.police.uk

Sold Secure:
www.soldsecure.com

Master Locksmith Association (MLA):
www.locksmiths.co.uk

Personal safety advice

Crimestoppers:
www.crimestoppers-uk.org

Suzy Lamplugh Trust:
www.suzylamplugh.org

Victim Support:
www.victimsupport.org.uk

Cyber/Information security advice

Get Safe Online:
www.getsafeonline.org

Cyber Aware:
www.ncsc.gov.uk/cyberaware/home

Internet Security & Safety Advice:
www.theukdomain.uk/cyber-security/

Advice on how to help children use the internet safely:
www.internetmatters.org

Child Exploitation and Online Protection Centre (CEOP):
www.ceop.police.uk

Direct marketing removal

Mail Preference Service:
www.mpsonline.org.uk

Telephone Preference Service:
www.tpsonline.org.uk

Notes

Local Police Station:

Local Counter Terrorism Security Adviser:

Local Hospital:

Local GP Surgery:

Report suspicious activity:
https://act.campaign.gov.uk

Further notes:

Further notes:

Further notes:

Further notes:

Further notes:

IN THE EVENT OF
a firearms or weapons attack

RUN HIDE TELL

RUN to a place of safety. This is a far better option than to surrender or negotiate. If there's nowhere to go, then...

HIDE It's better to hide than to confront. Remember to turn your phone to silent and turn off vibrate. Barricade yourself in if you can. Then finally and only when it is safe to do so...

TELL the police by calling 999.

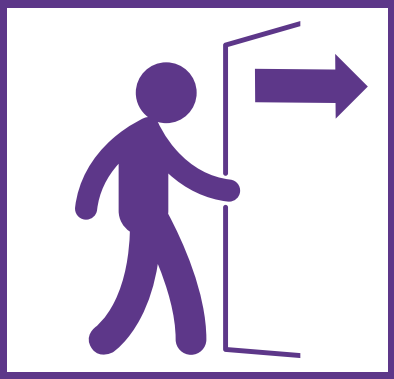
COUNTER TERRORISM POLICING

ACT ACTION COUNTERS TERRORISM

If you think someone has been exposed to a **HAZARDOUS SUBSTANCE**

Use caution and keep a safe distance to avoid exposure yourself.

TELL THOSE AFFECTED TO:



REMOVE
THEMSELVES...

...from the immediate area to avoid further exposure to the substance. Fresh air is important.

If the skin is itchy or painful, find a water source.

REPORT... to the emergency services.

REMOVE
OUTER CLOTHING...

...if affected by the substance.

Try to avoid pulling clothing over the head if possible.

Do not smoke, eat or drink.

Do not pull off clothing stuck to skin.

REMOVE
THE SUBSTANCE...

...from skin using a dry absorbent material to either soak it up or brush it off.

RINSE continually with water if the skin is itchy or painful.

ACT QUICKLY.

These actions can **SAVE LIVES**

Disclaimer

The material and information contained in this guidance is for general advice and information purposes only.

Whilst we have made every attempt to ensure that the information contained in this guidance has been obtained from reliable sources, NaCTSO (and its staff, officers and employees) are not responsible for any errors or omissions, or for the results obtained from the use of this information.

The information in this guidance has been prepared without guarantee of completeness or accuracy of the results obtained from the use of this information, and without warranty of any kind, express or implied.

This guidance (including any enclosures and attachments) has been prepared for the exclusive use and benefit of the addressee(s) and solely for the purpose for which it is provided. We do not accept any liability if this report is used for an alternative purpose from which it is intended, nor to any third party in respect of this report.

Reference to any specific commercial product, process or service by trade name, trademark, manufacturer or otherwise, does not constitute or imply its endorsement, recommendation or favouring by NaCTSO. The views and opinions of authors expressed within this document shall not be used for advertising or product endorsement purposes.

In no event will NaCTSO, or the partners, agents of employees thereof be liable to you or anyone else for any decision made or action taken in reliance on the information in this guidance, or for any consequential, special or similar damage.

To the fullest extent permitted by law, NaCTSO accepts no liability for any loss or damage (whether direct, indirect or consequential and including, but not limited to, loss of profits or anticipated profits, loss of data, business goodwill) incurred by any person and howsoever caused arising from or connected with any error or omission in this document or from any person acting, omitting to act or refraining from acting upon, or otherwise using, the information contained in this document or its references.

You should make your own judgement as regards use of this document and seek independent professional advice on your particular circumstances. Standards are current for the time of printing.

Report suspicious activity in confidence on the anti-terrorist reporting hotline

0800 789 321

In an emergency call police on 999
Non emergency calls dial 101

Report suspicious activity in confidence on the anti-terrorist reporting hotline

0800 789 321

In an emergency call police on 999
Non emergency calls dial 101