20. SECURITY

20.1.1 Contents:

Security staff based within Edinburgh bioQuarter may be contacted by dialling:

29289 or 29290 from any extension

(or by telephoning 0131 242 9289 or 9290 from outside Edinburgh bioQuarter)

20.2.1 Aim: To describe basic steps to be taken in the event of a malicious, criminal or terrorist act threatening the safety of University buildings, building users and activities in Edinburgh bioQuarter.

20.3.1 Introduction: The Management of Health & Safety at Work Regulations 1992 (as amended) impose a duty of care on employers and state that appropriate procedures should be in place to protect employees in the event of an imminent serious danger, and that employees should be notified of the hazards and the steps to be taken. A corresponding duty of care exists in respect of employees responsibilities to take steps to work safely and minimise hazards in the workplace.

20.3.2 As a globally prominent centre for scientific and medical research, the University has, in the past, albeit infrequently, experienced the undesirable attention of some extremist organisations, a few of which are known to attract individuals who are willing to resort to violence to further their aims. The risk is formally assessed by the security services as *low* at the time of preparation of this Manual, but there is no reason to believe that University buildings, and perhaps even some people directly, might not at some time in the future become targets of criminal assault and acts of terrorism.

20.3.3 There is present within some buildings, also, some material that could be misappropriated for criminal purposes, making the building vulnerable to the possibility of theft.

20.3.4 In a free society, and consistent with the University's public role, there is a limit to what obstacles can be put in the path of free movement within and around buildings, but there are reasonable steps that can be taken to reduce the likelihood of a criminal being successful in targeting our buildings and building users.

20.3.5 There is some potential also for University buildings and building users on the Edinburgh bioQuarter site to be affected collaterally by virtue of proximity to threats against the Royal Infirmary of Edinburgh.

20.4.1 General Crime Prevention: Although University buildings on the Edinburgh bioQuarter campus are patrolled by security staff, it is reasonable for building users to take steps to protect themselves and their property against criminality. The following are simple but useful measures that should be adopted by all buildings users:

- Lock away safely all personal possessions and valuables such as handbags, purses, wallets, and car and house keys when these are not immediately on your person. Lockers are available at various places around the building or items may be kept in a locked desk drawer or filing cabinet to which you have a key;
- Ensure that your car is locked before leaving it in an on-site car park or anywhere off-campus;
- Ensure that your bicycle is properly secured before leaving it unattended;
- Do not leave fire doors or delivery doors open and unattended;
- Do not allow people to follow you into secure areas unless they have a valid pass (authorised contractors and visitors must obtain passes from Reception in any of our buildings);
- Immediately report the loss of building keys and proximity pass cards to buildings security staff;
- Immediately report any theft or criminal damage to buildings security staff; and
- Immediately report any suspicious activity to buildings security staff, including people wandering around the building apparently looking lost.

20.5.1 General Security Guidance: The following guidance is adapted from a Home Office publication (referenced within Paragraph 20.21.1 *et seq*):

- Be alert and observant, and report any unusual or suspicious activity to buildings security;
- Take a regular good look around your own workplace and establish an awareness of what *should* and *should not* normally be there. This will be very important if you need to search your premises at any time (for example, if there were a bomb threat);
- Trust your instincts. If you feel that something is wrong, contact buildings security by dialling **29289** or **29290** from any extension;
- If you have information about possible bomb threats or other immediate threats, call **(9)999** and then inform buildings security staff; and
- If you have tip-offs or confidential information about possible terrorist activity, call the Police anti-terrorist hotline: **0800 789 321**.

20.6.1 Human Resources: The Home Office offers the following thoughts for consideration:

- Can you be reasonably certain that members of your staff *are* who they say they are?
- Have you checked references and employment records?
- Would you be aware of any behaviour or changes in behaviour that might give cause for concern?
- Are you, as a manager or supervisor, aware of how you should handle such instances?
- Are you confident that similar standards are applied to agency, contract or locum staff working within your organisation?

20.7.1 Contingency Plans: The Home Office also encourages the creation of contingency plans, which should address the following points:

- How you would aim to continue working if your usual place of work was not accessible or if a critically important item of equipment broke down, or if the supply chain failed?
- Is there a way for your colleagues to contact senior managers to check the current situation and for management to contact staff away from the workplace?
- Do you take steps to ensure that your standard emergency plans, such as fire evacuation drills, are up-to-date and regularly exercised?
- Do members of your staff know these procedures?

20.7.2 Means by which local arrangements have been designed and tested are described elsewhere in this Manual (see Section 34), but local rules for each centre, service and area should address these points too.

20.8.1 Access Control: All regular building users are each issued with a combined photographic identification and proximity card, allowing card-holders access to those parts of the buildings as have been considered appropriate for their duties. The effectiveness of this security measure depends on buildings security staff being prepared to challenge anyone *not* displaying a photographic identification, and authorised buildings users *not* allowing people who are unknown to them to follow them through a controlled access point.

20.8.2. Temporary cards may be issued to visitors, contractors *etc*, with appropriate levels of access, but it may be necessary in some cases for the hosts of such visitors to arrange for them to be escorted through the buildings.

20.8.3 Card-holders must report loss of access control cards, *as soon as possible after discovering their loss*, by telephoning the QMRI Security office on (0131) 242 9289 (internal extension 29289) or (0131) 242 9290 (internal extension 29290), or the University's main Security office on (0131) 650 2257; this is to help prevent unauthorised persons gaining access to the building. Security staff will immediately suspend access entitlement for the missing card(s), but can re-enable the cards if they are later discovered by the authorised card-holder (otherwise there may be a charge for issue of replacement cards).

20.8.4 It is a responsibility of Receptionists and Security Officers to monitor the arrival of people into our buildings, and to challenge anyone attempting to enter without proper authorisation.

20.8.5 It is important that building users do not enter or leave buildings through fire doors, except in a building emergency, and fire doors must not be propped open at any time. The door into the QMRI that is intended mainly for use by bicycle users must not be propped open, nor doors leading into any of our buildings from Stores loading bays.

20.8.6 All doors to outside are electronically monitored, and most are monitored also by CCTV cameras.

20.8.7 Staff entering any one of the buildings *outwith hours of expected building occupancy* (see definition at Paragraph 9.4.1 of this Manual), *must* sign themselves IN *and* OUT using one of the special log books provided for that purpose; these books are held in Reception at the main entrance to each of the buildings. It is unacceptable for staff entering or leaving the building using doors other than the main front doors to disregard this requirement. Local arrangements may exist for University staff working within the Infirmary.

20.8.8 See also Section 21 of this Manual, which describes arrangements for security cards and keys.

20.9.1 Unattended Suspicious Items: Only in a tiny minority of cases will an apparently abandoned package represent a genuine threat; mostly these will turn out to be packages that have simply been mislaid or forgotten by their owners. Of those that *are* associated with malign intent, the majority are likely to be hoax devices intended simply to cause disruption without any potential for actual physical damage. There is a small possibility, however, that an apparently abandoned package *might* represent an improvised explosive device with the potential to inflict injury to people in the proximity and/or damage to the building. All suspicious packages *must*, therefore, be reported to buildings security staff for investigation.

20.9.2 An unattended item may be characterised as something without a discernible owner (though it may be, in other respects, typical of what might be found legitimately at that location), but which may have been:

> **H**idden - Does it seem as though some attempt has been made to conceal the item?
>
> **O**bviously Suspicious - Does the item seem suspicious?
>
> **T**ypical – Is it typical, or more likely *not* typical, of other items in the place where it has been discovered?

20.9.3 Paradoxically, a package that has been constructed with the specific purpose of creating alarm, but with no intention of causing injury or physical damage, may look more "bomb-like" than an improvised explosive device specifically intended to cause injury and damage. Superficial investigation may reveal the presence of wires connected to a container with a timing device in relatively clear view. A terrorist might be expected to take greater pains to ensure that an improvised explosive device looks more innocent, inviting it to be handled and detonated. In *either* case, however:

- *Do* not touch any suspicious package;
- If it is feasible, cordon-off or otherwise restrict access to the area within which the package has been discovered;
- Ask people in the immediate area if they are aware of *who* has abandoned the package. If the owner can be identified, ask him or her to show the contents, and then stand-down the alert unless there are persisting concerns;
- Do *not* place the package in a bucket of water;
- Do not use a cellular telephone or radio transmitter in close proximity to the package (*i.e.* not within 15 metres of the package); and
- Report the discovery to buildings security staff, and leave the area. Buildings security personnel will control access to the area and report the discovery to the emergency services.

20.9.4 Key information required by Police Scotland in respect of unattended items:

- **WHAT** has been found?
- **WHERE** was it found?
- **WHEN** was it found?
- **WHY** is it suspicious?
- **WHO** found the item?

20.9.5 Good housekeeping is important also as a means to reduce opportunities for a terrorist to conceal an improvised explosive device amongst accumulated refuse and discarded materials. Waste bins are common places for terrorists to plant improvised explosive devices, though other hiding places may be used.

20.9.6 The emergency services may request assistance from building users to plan a search of the building, area by area. Since no-one knows our buildings as well as we ourselves do, and no-one else would know what is unusually present or absent within the communal areas, offices and laboratories that we occupy, it makes sense for us to help in the planning of such searches. The priority areas for searching are most likely to be:

1. Crowded areas to which many people, including members of the public, have access;
2. Vulnerable/critical areas, within which the effects of damage would be most impactful; and
3. Areas to which, normally, only authorised personnel have access

20.9.7 Evacuation of a building in such circumstances should be done according to advice sought from and issued at the time by the emergency services. Sounding a building emergency alarm may not always be appropriate, and a mass evacuation may not always be the safest way of ensuring the safety of building occupiers. If evacuation is recommended by the emergency services, the Evacuation Assembly Points listed at Section 5 of this Manual will usually be appropriate, but Evacuation Assembly Point Controllers should marshal people to a suitable location, distant from that building, to protect against the potential for injuries to be caused flying debris.

20.9.8 By the same token, however, advice may be issued for occupants of premises <u>not</u> to evacuate, if there is reasonable concerns that a threat might exist to the safety of people actively evacuating or at the location to which they would normally be expected to assemble after evacuating. In such circumstances, refuge should be sought in protected spaces/locations within which they might more safety shelter from the threat, or a more distant evacuation assembly point may be considered.

20.9.9 Cordon distances normally to be established around suspicious items:

Backpack-sized package:	minimum 100 metres
Small vehicle:	minimum 200 metres
Large vehicle:	minimum 400 metres

20.9.10 Further information on this subject is available at http://www.cpni.gov.uk/

20.10.1 Suspicious Items Received in the Post: Much of our daily incoming mail arrives in padded envelopes and boxes, and there is a limit to what can reasonably be done in anticipation of the very low likelihood that one of these might one day contain an improvised explosive device or other device with the potential to cause injury or physical damage. Recipients should, nevertheless, be alert where packages appear unexpectedly to contain loose wiring, broken glass, other sharps, uncontained liquids or powdered solids, or where they appear to have been posted from an unexpected location, or in a form that attracts attention because of the way in which the address has been written or the package wrapped.

20.10.2 Counter-terrorism advisers have listed the following as possible indicators that items sent by mail may be suspicious:

- Restrictive markings, unusually indicating that the package is intended to be opened only by one specifically named person;

- Items addressed to the addressee’s job title only, not including the person’s name;
- Badly typed or poorly hand-written labels;
- Misspelled words on the address label, *etc*;
- Excessive postage for the weight and size of package received;
- Unexpectedly rigid or bulky items, particularly if the rigidity seems to be an uneven feature of the package;
- The absence of a return address, or an unusual or unexpected source address;
- Stains or smears on the package covering;
- Unexpected or unusual odours emanating from the package and/or
- Unusual methods of sealing, which may suggest the possibility of a trigger mechanism.

Whereas some of the above are not uncommonly associated with packages received in post rooms *etc*, the presence of several possible indicators together may be taken as suspicious and suggest the need for careful and cautious management (see Figure 1).

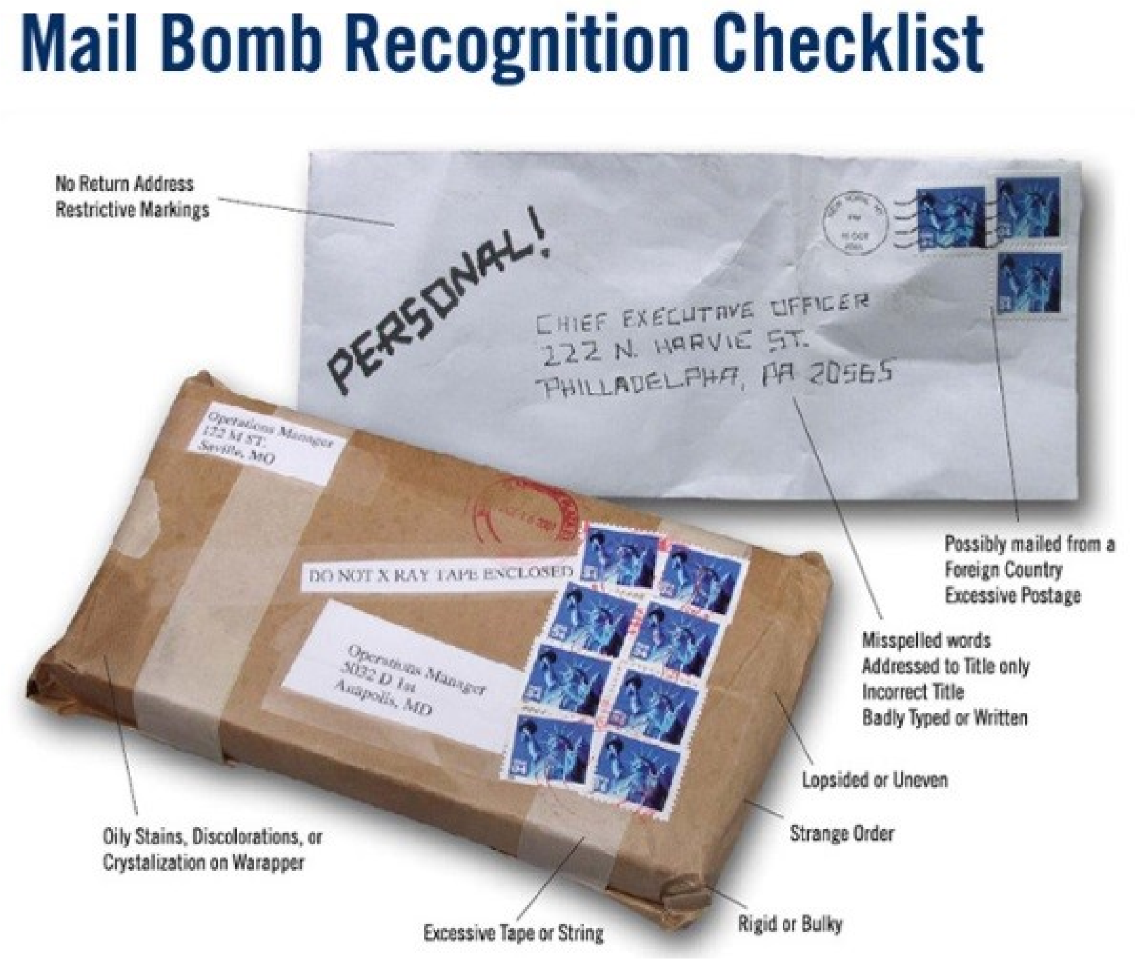

Figure 1: Mail Bomb Recognition Checklist

20.10.3 Where reasonable suspicion exists, the recipient of suspicious mail (which may contain an improvised explosive device, hazardous substances, *etc*) should:

- Cease handling the package, after laying it on a firm surface somewhere away from windows and doorways;
- Do not allow anyone to touch, prod, tamper with, smell or relocate the package;
- Do not discard any part of the package (all parts may prove to be of evidential value);
- Do *not* place the package in a bucket of water;
- Do not use a cellular telephone or radio transmitter in close proximity to the package (*i.e.* not within 15 metres of the package);
- Evacuate the immediate area, to a minimum distance of 100 metres, but do not close the door of the room within which the package has been left so that attending emergency services personnel will be able to observe without disturbing it;
- If possible, switch off ventilation systems in the area;
- Take steps to prevent anyone else entering the area or approaching the package;
- Report the circumstances to buildings security staff; and
- Wash hands thoroughly if they have come into contact with the contents of the package, particularly if the presence of chemicals is suspected.

20.11.1 Threats of Violence: A simple threat of violence is often sufficient to seriously disrupt an organisation, even if the terrorist has no intentions of following it up with an actual physical attack. Nevertheless, *all* threats of violence against a person or attack on property *must* be taken seriously and reported to the proper authorities. Threats may be made by telephone, in writing or directly by an individual or group of people presenting themselves within or close to one of our buildings.

20.12.1 Threats Made by Telephone: This is likely to be extremely stressful for the person receiving a threatening call, but it is critically important that the recipient gathers all possible information from the caller.

20.12.2 Recipients of threatening or abusive telephone calls should take careful note of several potentially useful factors that might later help the emergency services to trace and prosecute those who have such calls and which, in the more immediate short-term, will help buildings security staff take steps to protect building users and others nearby:

- If possible, invite a colleague to monitor the call (this adds to the amount of information that can reliably be gathered from the call, and adds weight to a potential prosecution);
- If the facility exists (using an answering machine, for example), attempt to record the call;
- If it is feasible, and the circumstances seem to so warrant (the threat having been perceived to be genuine and sufficiently serious) a third colleague might usefully be dispatched to inform the emergency services immediately by making a (9)999 call (It is not very likely, but it might just be possible for the emergency services and telephone service provider to monitor and trace the call);

- Note the date, time and duration of the call;
- Record in writing as much as possible of the precise message being communicated by the caller;
- Is there is any indication that the call is being made from a call box or cellular telephone?
- Note the gender and, if possible, estimate the likely age of the caller (*e.g.* child-like or adult);
- Record any name (individual or organisation) mentioned by the caller as he or she introduces himself or herself;
- Does the caller use any code words?
- Record also any names mentioned by the caller as people they may wish to speak with, and any comments made by the caller in that context;
- Does the caller have a regional dialect or national accent?
- Does the caller sound well-spoken, foul-mouthed, calm, angry, irrational, intoxicated *etc*?
- Does it sound as if the caller is attempting to disguise his or her voice?
- Does the caller have a stutter or lisp?
- Does the caller speak slowly, normally or rapidly?
- Is the caller's voice deep or high-pitched?
- Does the caller's voice sound familiar?
- Does it sound as if the warning is being read from a script?
- Does it sound as if the caller is alone, or are there were other people present (and what does it sound like the other people are saying or doing)?
- Note any background noises, such as street noises, motor vehicles, machinery, animals, television/radio *etc*;
- Record also any reference to the purpose of the action being threatened;
- Note any specific threats made;
- If the caller makes any threat of planting a device within the building, note carefully whether reference is made to locations, types of device, potential scale of damage, and time before the device is expected to detonate;
- Record any other points that the caller makes or which occur to you during or immediately after the call; and
- If the facility exists, attempt to perform a 1471 dial-back to trace the origin of the call.

20.12.3 The recipient of a threatening or abusive telephone call should take care if encouraging the caller to communicate additional information, not to inflame his or her emotions, but may attempt to prolong the conversation if the caller seems calm and prepared to talk freely.

20.12.4 Where the warning pertains to a bomb or similar device, unless they have already volunteered the information, the caller should certainly be asked:

- Where is the bomb right now?
- When is it going to explode?
- What does it look like?
- What kind of bomb is it?
- What will cause it to explode?

- Did *you* place the bomb?
- (If not, who did?)
- Why was the bomb placed?
- How can I contact you again?
- What is your name?
- What is your address?
- What is your telephone number?

20.12.5 While it is unlikely that a genuine terrorist would actually answer the last four questions … if he or she does so, it might suggest something about the credibility and seriousness of the threat. In any event, even if the caller *does* provide that information, buildings security staff and the emergency services will *always* investigate, treating the threat as perfectly serious until it is found to be otherwise.

20.12.6 The above information might usefully be displayed alongside telephones capable of receiving incoming calls (particularly if there is a heightened state of alert) and, in particular, at Reception and security desks in each building.

Please refer to Annex A to this Section for a suitable bomb threat checklist.

20.13.1 Threats Made in Writing, eMail, Social Media, *etc*: Written communications that could in any way be interpreted by the recipient(s) as threatening against individuals, groups or property, in whatever form received, *must* be reported immediately to the emergency services, copied as soon as possible to buildings security staff and College management. Immediately after ascertaining the threatening nature of a document received in hard copy, the recipient should lay the document down and not allow it (and the package within which it was delivered) to be touched until the emergency services take charge of it, in order to preserve evidence such as fingerprints. Documents received by email or intercepted on social media *etc*, should be retained for inspection.

20.13.2 Packages containing also suspicious objects should be treated as described in Paragraph 20.9.1 *et seq*.

20.14.1 Threats Made in Person: The presence of any individual behaving in a threatening manner within or close to a University building should be reported *immediately* to buildings security. Reception staff and others who may be approached by such a person should *not* put themselves at risk by attempting to confront them.

20.14.2 An angry, aggressive or otherwise threatening individual may be inflamed by confrontation. It is not often as easy to "talk down" a person in an agitated state as it may appear from popular television programmes. If it is possible and safe to withdraw from direct contact with the individual, do so immediately. Otherwise:

- If it is possible, put yourself in a position where you are close to an exit from the area, ideally with a solid item of furniture between you and the agitated individual;
- Speak calmly and in a quiet voice;

- Do not make sudden movements;
- Do not hold eye contact with the person for long periods of time, but *do* appear to be listening to what they are saying by nodding occasionally;
- Do not attempt to rationalise with the person or justify a contrary argument;
- Suggest that tea (or something similar) could be brought to where the confrontation is taking place and, if the offer is accepted, covertly request security back-up when ordering the refreshments; and
- As soon as it is feasible and safe to do so, withdraw from the room and report the incident to buildings security staff.

Please refer to Annex A to this Section for a suitable bomb threat checklist.

20.15.1 Firearms and Weapons Attacks: The general advice issued by the UK government *etc* is to:

- **Run** – If, clearly, there a safe route away from the situation;
- **Hide** – In a suitably securable location if there is a means to do so that would not result in you becoming trapped, seek cover from view and shelter from ballistic fire; and
- **Tell** – Inform the emergency service of the circumstances.

20.15.2 After surveying and assessing the situation, and if it is safe to do so, inform the Police, reporting:

- What has happened, reporting also all persisting hazards, such as the continued presence and location of people with weapons;
- The precise location of people with weapons, and also those sheltering from them;
- What restrictions there may be to safe access for attending emergency services personnel into and around the area;
- The number and condition of casualties;
- The presence already of other emergency services personnel and their circumstances; and
- Any other information that seems relevant and likely to be of interest to the Police *etc*.

20.16.1 Suspicious Behaviour: Those who are normally based within premises are often best placed to note things that are out of the ordinary and, by reporting these, may be in the best position to prevent a situation developing into an emergency. Behaviour that is “out of the ordinary” in some way may be as relevant to potential criminality as to terrorist interest, and the Police will not be unhappy about receiving reports that may help prevent a crime from taking place. People showing an unusual interest in our premises, perhaps asking unexpected questions about the location of specific laboratories and the nature of work being done within these *etc* (sometimes known as “hostile reconnaissance”), or being seen taking photographs of the location of CCTV cameras for example, should be reported to buildings security as promptly as possible.

20.17.1 Threats Made to Staff *etc* at Home: In addition to informing the Police (as soon as possible) of any threat made in connection with your employment, regardless of the form it takes, please inform also University Security.

20.18.1 Security of Hazardous Substances for Transport: Those consigning hazardous chemical, radioactive and/or biological materials for transport must take steps to minimise the possibility of packages being mislaid, misappropriated, misused or stolen, particularly when these are properly labelled as containing high consequence dangerous goods. Wherever possible, packages should be handed over directly to properly identified persons representing transport companies contracted by the University to manage the delivery. Until the courier arrives to collect the package, it should be kept where it cannot be accessed by any unauthorised person. Further information regarding security of biological materials being consigned for transport is contained at:

https://www.ed.ac.uk/health-safety/biosafety/policy/guidance/transport

and

https://www.ed.ac.uk/health-safety/biosafety/policy/guidance/biological-security

20.19.1 Protection Against Electronic Attack ("Hacking"): Edinburgh University IT specialists are available to give expert advice on aspects of IT security. However, as a mater of routine:

- Consider if changes in your business circumstances or relationships might increase the threat of electronic attack to your organisation;
- Check that protective security measures are properly implemented and up-to-date;
- Anti-virus software should be updated regularly;
- Patches should be applied to eliminate known vulnerabilities;
- Internal security policies should provide appropriate protection from inside attack.

20.19.2 More information about how to protect against electronic attack, and details on the latest vulnerabilities and patches, can be found on the National Infrastructure Security Co-ordination Centre web site:

http://www.cpni.gov.uk/advice/cyber/

20.20.1 Security of Confidential Information: Most if not all building users will have some contact with personal and confidential information, including clinical patient data. It is particularly important that patient confidentiality is maintained at all times. Guidance will be given on this matter during induction training, but security will be increased by taking a few simply steps:

- Lock hard-copy confidential information into desk drawers or filing cabinets when not in use;

- Be extremely careful if sending sensitive information using facsimile machines that the correct number is dialled and that there is someone appropriate waiting immediately to receive it;
- Shut-down computers or log-off to a password protected status when you are not actually working on confidential information using a computer;
- Ensure that passwords are safeguarded to individual users, and are complex constructions, so that they cannot be second-guessed or easily de-encrypted by password hacking programs;
- Do not write or display passwords and lock codes on desks, fixtures, equipment or notice-boards where they can be easily read, and their meaning be clearly understood, by unauthorised people;
- Lock filing cabinets, desk drawers and office doors where confidential information is stored and used when the material is not actively being used and the room is not occupied; and
- Take care to dispose of redundant hard-copy by committal to confidential waste disposal routes and/or shred the papers first, particularly if identifiable personal information is attached or included (further information on aspects of disposal of confidential waste is available at Sections 18 and 30 of this Manual)

20.21.1 Training: Training related to aspects of security are available upon request to the H&S Manager for University buildings on the Edinburgh bioQuarter campus **(**Email: Lindsay.Murray@ed.ac.uk); it is recommended that this be attended at least by Reception and servitor personnel.

20.22.1 Further Information: Security staff based within Edinburgh bioQuarter may be contacted on:

Telephone: 29289 or 29290 from any extension
(or phone 0131 242 9289 or 9290 from outside Edinburgh bioQuarter)

Email: QMRISecurity@ed.ac.uk

20.22.2 The Security department for the University may be contacted on:

Non-emergency number: (0131) 650 2257
(or 774 50 2257 from any extension within Edinburgh bioQuarter

Email: Security@ed.ac.uk

Web: www.security.ed.ac.uk

20.21.3 General information from the UK government on measures to be taken to prevent or limit the damage caused by terrorism in the workplace:

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

20.22.4 The University's policies regarding data security are set out in the Records Management Section's web site at:

https://www.ed.ac.uk/records-management

20.21.5 Further information is also available at:

http://www.cpni.gov.uk/

ANNEX A

ACTIONS TO BE TAKEN ON RECEIPT OF A BOMB THREAT

1 Remain calm and talk to the caller
2 Note the caller's number if displayed on your phone
3 If the threat has been sent via email or social media, see appropriate section below
4 If you are able to, record the call
5 Write down the exact wording of the threat:

When Where What How Who Why Time

ASK THESE QUESTIONS & RECORD ANSWERS AS ACCURATELY AS POSSIBLE:

1. **Where exactly is the bomb right now?**
2. **When is it going to explode?**
3. **What does it look like?**
4. **What does the bomb contain?**
5. **How will it be detonated?**
6. **Did you place the bomb? If not you, who did?**
7. **What is your name?**
8. **What is your address?**
9. **What is your telephone number?**
10. **Do you represent a group or are you acting alone?**
11. **Why have you placed the bomb?**

Record time call completed:

INFORM BUILDING SECURITY / COORDINATING MANAGER

Name and telephone number of person informed:

DIAL 999 AND INFORM POLICE

Time informed:

This part should be completed once the caller has hung up and police / building security / coordinating manager have all been informed

Date and Time of call:

Duration of call:

The telephone number that received the call:

ABOUT THE CALLER: Male □ Female □ Nationality Age

THREAT LANGUAGE: Well-spoken □ Irrational □ Taped □ Foul □ Incoherent □

CALLER'S VOICE: Calm □ Crying □ Clearing Throat □ Angry □ Nasal □

Slurred □ Excited □ Stutter □ Disguised □ Slow □ Lisp □ Accent* □

Rapid □ Deep □ Familiar** □ Laughter □ Hoarse □ Other (Please specify)

* What Accent?

** If the voice sounded familiar, who did it sound like?

Street Noises □ House Noises □ Animal Noises □ Crockery □ Motor □

Clear □ Voice □ Static □ PA System □ Booth □ Music □

Factory Machinery □ Office Machinery □ Other (Please Specify)

REMARKS:

ADDITIONAL NOTES:

Signature ______________ Print Name ______________ Date ______

ACTIONS TO BE TAKEN ON RECEIPT OF A BOMB THREAT SENT VIA EMAIL OR SOCIAL MEDIA

1 DO NOT reply to, forward or delete the message

2 If Sent via email, note the address

3 If sent via social media, what application has been used and what is the username / ID

4 Dial 999 and follow police guidance

5 Preserve all web log files for your organisations to help the police investigation (as a guide, 7 days prior to the threat message and 48 hours after)

Signature ______________ Print Name ______________ Date ______