DAWAT E ISLAMI UK

SECURITY POLICY

Prepared by: Dr Zeerak Nasim, Health & safety Lead

Status of Policy: Final

Ratified by: Trustees

Implementation Date: Jul 2019

Review Date: Jul 2020

Dawat e Islami UK treats the security of our staff/visitors/pupils as a top priority. Security arrangements are monitored and reviewed regularly by Dawat e Islami Security lead, and following a security related incident or feedback from an interested party.

The security plan covers the following areas:

1. Education and training
2. Perimeter security
3. CCTV security
4. Doors/windows security
5. Funding available from The Government
6. Entrance protocols
7. Good house keeping
8. Emergency plans
9. Post Incident plan
10. Senior management involvement

1. Education and training

1.1. Security advice leaflet to be read by all staff/volunteers
1.2. ACT E-Learning module to be completed by all staff/volunteers
1.3. To attend Project Argus (workshop-based training delivered by local police). This will be organized by the Security Majlis in the near future.
1.4. Compliance with the above three tasks will be monitored by Kabina Level Security Lead
1.5. Bulletin service to keep everyone up to date with current situation and potential risks

2. Perimeter security

2.1. All buildings to have perimeter wall/fencing
2.2. Any damaged walls/fencing should be repaired
2.3. Appropriate lighting arrangements on all external areas within the perimeter to deter intruders
2.4. Apply for Government funding for this if needed
2.5. Good housekeeping externally to reduce risk of arson (see section 7 for further details)
2.6. When building is not in use, the gates should be locked. However, this needs a careful planning as each site is different in its use. There should be a close liaison with Faizan-e-Madina Majlis, Madani qaafila majlis and division nigraan in finalizing this Madani pearl.

3. CCTV security

3.1. CCTV surveillance in all internal and external areas of the building
3.2. Tap into Government funding if needed to install new or update existing system
3.3. Daily monitoring of CCTV system by designated people, especially around namaz and Madrasa times (aim should be to monitor people entering and any other security hazards).

3.4. Regular servicing of the CCTV equipment
3.5. More than one person to have access to the CCTV data
3.6. Check the DVR capacity and it should have at least 4 weeks of recorded data
3.7. Sisters must monitor their own side of the CCTV system independently (maintenance tasks to be completed by Islamic brothers)

4. Doors/windows security

4.1. All doors and windows locks should comply with British Standard 3621
4.2. All fire doors and final exit doors should comply with Fire regulations
4.3. Fix any damage or other issues with Fire Exit doors
4.4. All people who use the building should be made familiar with available fire exits
4.5. All corridors must remain free of obstruction at all times

5. Funding available from The Government

5.1. One islamic brother will be appointed at UK Level who will coordinate and apply for security funding available from the Government
5.2. This islamic brother must get sharayi guidance from Mufti Saajid sahib before the application
5.3. Detailed records must be maintained on how the money was spent
5.4. For any work that needs to be done in this regard, this must be carried out by a professional builder with registered company. Guidance for this is available in The Health & Safety Folder Section 15

6. Entrance protocols

6.1. This is our weakest point due to the nature of our work i.e. full public access without any checks
6.2. Kabina Level Security Zimmadaar will liaise with building level Security zimmadaar and make sure named individuals are appointed to carry out tasks suggested below
6.3. During operational hours we need to make sure:
  6.3.1. Designated staff, who are appointed for daily checks (as per Health & Safety Folder), should include checking the building for any suspicious packages or items and make sure it is safe before the building is opened.
  6.3.2. Staff are appointed to observe who is coming and going, via CCTV and periodically through physical presence around the entrance area.
  6.3.3. If designated staff notice any suspicious behaviour, challenge the person as explained in the Safety Advice Leaflet page 2 (How can I Help?)
  6.3.4. If designated staff notice any suspicious packages, follow the HOT protocol (See Appendix 1)
  6.3.5. Designated staff should do random patrols of the building in pairs, with high vis jackets, and observe for any suspicious vehicles or people on foot/in cars and challenge them as per situation
6.4. Make sure everyone leaves the building after the religious activity
6.5. Doors should be locked and only opened for the next religious activity, as per 2.6.

6.6. If it is felt that a particular centre needs additional paid staff to fulfill security duties, then security lead from that centre shall prepare a business case for this (i.e. the need, level of threat, any particular incidents that have happened, why can existing staff not fulfill this role etc.). This business plan will then be sent to Board of Trustees for approval. It is only after Board of Trustees approval, and all the HR procedures, a new employee will be taken on board.

6.7. Any large crowds standing outside the premises should be dispersed as they are an easy target for an attack

6.8. Jamia-tul-Madina residential blocks should have strict enforcement of security.

6.8.1. No individual should leave the building after 11pm, unless prior approval of site naazim is sought.

6.8.2. Site Naazim will have to liaise with security majlis before permission is granted to leave the premises.

6.8.3. During an emergency, this rule should be ignored.

7. Good housekeeping

7.1. Any material that burns and is kept outside, is a target for an Arson Attack

7.2. Good housekeeping rules should be followed as per Fire Risk Assessment carried out and kept in Section 1 of The Health & Safety Folder (speak to Health & Safety representative of your building)

7.3. All external bins should be at least 2 meters away from building walls and chain locked to perimeter wall/fence in a secure manner

7.4. Clear undergrowth, foliage and any overhanging branches around the immediate area of the building, as they can be used to place explosive devices

7.5. Develop a protocol for checking incoming mail. If you come across a suspicious package, kindly follow HOT protocol (See Appendix 1)

8. Emergency plans

In the case of a potential or actual terrorist attack, the Government's advice focuses on "Run", "Hide", and "Tell" (See Appendix 2). This may sound like obvious instructions, but very quick and vital decisions need to be taken. There should be carefully planned drills, in liaison with Police, for all of these Emergency procedures, as soon as possible. The drills should be conducted at a time which is most practical i.e. reflecting the nature of congregation.

8.1. Evacuation

8.1.1. Full site evacuation should take place, if safe to do so and directed by trained staff or Police

8.1.2. Two people should be designated, for leading the evacuation, each time building is occupied

8.1.3. These designated individuals must familiarize themselves with this Evacuation Plan

8.1.4. The evacuation should move people towards a place of relative safety

8.1.5. A directional evacuation should be used if a specific area is currently dangerous. This type of evacuation should be via specific directed exit routes

8.1.6. Evacuation should be very calm, quiet, orderly and in one direction. Otherwise there would be increased risk of slips, trips and falls causing further delay or even trampling or crowd crush

8.1.7. Particular emphasis should be given to disable individuals and their PEEP's (Personal Emergency Evacuation Plan)

8.1.8. At least one evacuation drill is advised at peak times (i.e. weekly Ijtimah) to assess effectiveness of evacuation plan and review any weak areas

8.2. Invacuation

8.2.1. If the threat is outside or location of threat is unknown, people may be exposed to greater danger by evacuating the building

8.2.2. Moving people away from the threat while remaining inside the venue is called Invacuation

8.2.3. The designated people should be fully aware of these areas suitable for invacuation in advance. However, the choice of place would depend on location of the threat

8.2.4. Invacuation should be:

8.2.4.1. Away from windows and external walls

8.2.4.2. In areas surrounded by full-height masonry walls

8.2.4.3. Away from stairwells and lift shafts as blast can travel up

8.3. Dynamic Lock Down

Dynamic lockdown is the ability to quickly restrict access and egress to a site or building (or part of) through physical measures in response to a threat, either external or internal. The aim of lockdown is to prevent people moving into danger areas and preventing or frustrating the attackers accessing a site (or part of). It is recognised that due to their nature some sites may not be able to physically achieve lockdown. Guidance notes are provided below for each site to prepare bespoke Dynamic Lock Down Procedures.

How to achieve dynamic lockdown

8.3.1. In your planning you should identify all access and egress points in both public and private areas of the site. Remember, access points may be more than just doors and gates. Identify how to quickly and physically secure access/egress points

8.3.2. Identify how your site can be sectored to allow specific areas to be locked down

8.3.3. Staff roles and responsibilities should be identified in advance

8.3.4. Staff must be trained to act effectively and made aware of their responsibilities

8.3.5. Stopping people leaving or entering the site – direct people away from danger
8.3.6. Ability to disable lifts without returning them to the ground floor should be considered
8.3.7. Processes need to be flexible enough to cope with and compliment invacuation and evacuation

How to let people know what's happening

Various options exist depending on the nature and occupancy of the site, these include;

8.3.7.1. Public Address (PA) System
8.3.7.2. Existing internal messaging systems; text, email, staff phones etc.
8.3.7.3. "Pop up" on employees computers / internal messaging systems
8.3.7.4. Dedicated "Lockdown" alarm tone
8.3.7.5. Word of mouth
8.3.7.6. Using predefined signs

Note: Use of fire alarms should be avoided to reduce incorrect response to an incident.

9. Post incident plan

9.1. Provision of Emergency First Aid to all the casualties – Only when safe and instructed by The Police.
9.2. Specific First Aid information has already been provided to all trained first aiders
9.3. Accounting for all individuals through headcount
9.4. Supporting the psychological needs of the individuals at the scene and offering appropriate support
9.5. Contacting and notifying families of individuals affected by the incident
9.6. Recording all important actions that were taken during the attack
9.7. Identifying any critical personnel or operational gaps left in the organisation as a result of the incident
9.8. When appropriate, identifying "lessons learned" and incorporated into training and rehearsal

10. Senior management involvement

10.1. CEO of Dawat e Islami will directly oversee all of the above plan
10.2. CEO will ensure swift response from the Board of Trustees on certain decision making i.e. approval for additional Dawat e Islami funds for security
10.3. Security should be discussed in Board of Trustees meetings and minutes produced to evidence this

APPENDIX 1

UNATTENDED ITEMS:
LOST... or SUSPICIOUS?

H

Hidden?

- Has it been concealed or hidden from view?
- Bombs are unlikely to be left in locations such as this – where any unattended item will be noticed quickly.

O

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?

T

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 protocol you still believe the item is suspicious, notify your line manager immediately and using the railway telephone network call 999.

!

If you do not have access to the railway telephone network call 0300 123 9102

BRITISH TRANSPORT POLICE

APPENDIX 2

NPCC
National Police Chiefs' Council

IN THE RARE 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.