SECURITY AND COUNTER TERRORISM POLICY

Executive Sponsor & Function:

Director of Workforce and Organisational Development

Document Author:

Jane Powell, Planning and Performance Business Partner

Approved by:

HEIW Executive Team

Approval Date:

8 May 2019

Date of Equality Impact Assessment:

May 2019

Equality Impact Assessment Outcome:

This Policy has been screened for relevance to equality. No potential negative impact has been identified.

Review Date:

May 2022

Version: v1

Table of Contents

Contents ..... Page

1. Policy Statement

1.1 The Health Education and Improvement Wales (HEIW) Board recognises its exemplar role both as an employer and as a service provider. HEIW is committed to creating, as far as reasonably practicable, a safe and secure environment for staff and visitors and also to protect people, property, equipment and assets against risk of injury, loss or damage whilst on HEIW controlled premises.

1.2 HEIW is committed to working in partnership with staff, trade unions and outside agencies, such as the police, to achieve the aims of this policy.

2. Purpose

2.1 The purpose of this security policy is to ensure that a safe and secure environment is provided for HEIW staff and visitors whilst working at their headquarters in Ty Dysgu or whilst undertaking work on behalf of HEIW. Its purpose is also to provide a secure environment for property, equipment and the assets of HEIW.

3. Scope

3.1 This security and counterterrorism policy and any arrangements made under it applies to:

- all persons employed or engaged by Health Education and Improvement Wales (HEIW) including part time workers, temporary and agency workers and those holding honorary contracts.

- visitors and volunteers.

Other NHS Health Boards and Trusts will have their own health and safety policies which will apply to HEIW staff working in NHS premises elsewhere across Wales.

4. Aims and Objectives

4.1 The aim of this security policy is to provide a safe and secure environment for staff and visitors within HEIW premises and to provide a secure environment for property, equipment and assets belonging to HEIW.

4.2 This Policy aims to be an overarching policy and all Directorates will implement procedures to support this policy. The policy is deemed to set the minimum requirements to:

- prevent/minimise the number of incidents relating to:
  - Violence and Aggression (physical or verbal);
  - Criminal Damage;
  - Theft (from HEIW premises or of HEIW property);
  - Arson.
- provide safe and secure working environment.
- fulfil the Board's legal duty of care to all its staff, visitors and contractors to provide a safe working environment.

5. Roles and Responsibilities

5.1 The Chief Executive is the Executive Lead and has overall responsibility and is accountable to HEIW Board for the management of Security within the organisation.

5.2 The responsibility for policy implementation rests with the Director of Workforce and Organisational Development.

5.3 The Director of Workforce and Organisational Development through delegated powers, shall ensure that all employees and others are aware of the policy and of their role in its implementation and monitoring. They shall also ensure that a responsible person is identified to manage security on a day-to-day basis and appropriate training given where necessary.

5.4 The Head of Planning, Performance and Corporate Services is the HEIW lead for the review of this document.

5.5 The Executive Team within HEIW are responsible for ensuring that the policy is implemented within their Directorates. They will:

- Ensure that employees within their team are aware of HEIW Security policy and any additional specific team security procedures.
- Undertake assessments of security risks present within their areas of responsibility.
- Ensure that training requirements of staff are fulfilled.
- Take reasonable precautions, through risk assessment and taking appropriate action, to protect HEIW's staff, visitors, contractors, property, equipment and assets.
- Empower their staff to raise any issues of security concerns or breaches of current security systems.

5.6 It is the responsibility of all Staff within HEIW to:

- Take responsibility to adhere to this policy and any local operational procedures to.
- Take responsibility to ensure security of the areas within which they work by closing windows and locking doors as necessary when the area is not in use.
- Have to take reasonable precautions to safeguard HEIW's staff, visitors, contractors, property, equipment and assets.
- Assist with any security investigation and engage and assist with any management security audits.
- Report any security concerns immediately to their line manager.
- No staff, unless trained to do so, should confront unauthorised persons on any premises. Personal safety is paramount.

5.7 It is the responsibility of the Facilities and Compliance Manager for on-site security and he/she will be required to undertake the following:

- Risk assessments to ensure that staff, visitors, property, equipment and assets of HEIW are not put at risk during the normal operational activities of HEIW.
- Risk assessments to ensure that staff, visitors, property, equipment and assets of HEIW are not put at risk during exceptional circumstances of operational activities of HEIW.
- Risk assessments of all areas of HEIW in order to identify any security related risks. It is the responsibility of the Directorates to assess and review their local security procedures
- Installing notices, managing security procedures, advising on secure storage arrangements, the management of existing and the provision of new keys / access swipe cards
- Establish and maintain a panic alarm system for the receptionist

5.8 When completing a risk assessment, the following risks will be considered:

- Points of ingress and egress
- Keypads /Key Locked / Access controlled doors
- Identification and visitor badges
- Security procedure and protocol for incidents / breaches
- Intruder alarms
- Intercom
- Security lighting

- Closed circuit television (CCTV)
- Sound maintenance practices
- Maintaining security during normal operational hours
- Securing the site/department at the end of the day.

6. Notices

6.1 Notices to deter criminal activity and dissuade persons from intimidating, threatening or violent behaviour are recommended. Signs concerning security measures must be prominently displayed throughout the building and its grounds, in particular reference to when CCTV is in operation, all signage produced should be bi-lingual.

7. Security

7.1 If it is suspected that an intruder is on the premises or that a theft is being committed, staff should seek assistance or remove themselves to a safe area and inform the police immediately, contacting their manager where appropriate. Advice on any other or further action to be taken will be provided by the police.

7.2 Security of unoccupied offices and areas that are in use for only part of the day must have a visual check made that the building is secure before it is vacated and intruder systems correctly armed. The use of blinds will keep property out of obvious view to a prospective thief. Managers must encourage members of staff to use drawers and cupboards to place items out of site and temptation.

7.3 HEIW cannot accept responsibility for the security of personal belongings on the premises. Staff are advised that personal belongings of a valuable nature should not be brought onto HEIW premises. All offices should be locked when not in use and all personal items should be removed from surfaces and locked away in pedestals or lockers.

7.4 HEIW's property and equipment must only be removed from site for legitimate purposes e.g. for repair, transfer to another HEIW premises or to facilitate fulfilment of HEIW's business. Managers must ensure that any property or equipment removed from HEIW facilities or being used on other sites, must be handled and transported with reasonable care and must be kept and stored in a secure environment. All members of staff must take reasonable security measures to prevent theft and or damage to HEIW property, accidental or otherwise.

8. Storage

8.1 Departments that hold stores / stock must have procedures that effectively and actively manage the prevention of theft, damage or sabotage. There must be regular stock audits, as defined by the manager responsible for the area or as dictated to by current departmental procedures of stock, for high value or high risk items.

9. Possession of Illegal substances

9.1 HEIW has a duty under the Misuse of Drugs Act 1977 (and subsequent Amendments) to ensure that its premises are not used for the illegal supply, use or possession of any controlled or illicit substance. In relation to employees of HEIW please refer to HEIWs policy on Substance Misuse at Work.

10. Weapon Possession

10.1 There is no justification for any person on HEIW's premises to be in possession of a weapon. Safety is the first concern and no member of staff, unless trained to do so, should challenge or confront a person who is suspected of possessing a weapon. Members of staff must remove themselves to a safe area and contact the police immediately.

11. Key Handling / Access Systems

11.1 Managers are to ensure robust, recorded and auditable systems are in place in relation to the management of existing and the provision of new key / access swipe cards. Where digital or coded key pad door locks are fitted managers must ensure that the code entry is changed at regular risk assessed intervals.

12. Future Security Design

12.1 All new significant schemes shall be designed to comply with the relevant NHS Building Notes and the principals of "Secure by Design".

13. Identity Badges

13.1 The policy requires that:

- identity badges must at a minimum contain a photograph of the member of staff, their name and be integrated into a managed computer data base system.
- badges are to be worn at all times and be clearly visible.
- refusal or consistent failure to display identification badges whilst in the work place may result in the instigation of HEIW's disciplinary code.
- lost badges must be reported immediately to the Facilities and Compliance manager.
- when not being worn, identity badges must be securely stored.
- all personnel are provided with a badge and that all new starters are immediately issued with an identity badge.
- all non-wearers of identity badges should be challenged.
- managers will ensure that staff leaving HEIW will have their identity badge, swipe cards and keys returned.
- the compulsory completion of details within the visitor's book and the allocation of a temporary visitors' or contractors identification badge which should be worn at all times.
- contractors employed to work on HEIW premises must wear appropriate identification badges in line with local procedures and returned upon completion of works (daily or otherwise stated)

14. Arson

14.1 All cases of suspected arson must be reported immediately to:

- The Police and Fire Service who will investigate
- Director of Workforce and Organisational Development
- The Facilities and Compliance Manager

15. Assault

15.1 Acts of physical or verbal assault on members of staff, visitors and any other persons on HEIW controlled premises will not be permitted (HEIW's Violence and Aggression Policy). HEIW fully supports and endorses the involvement of the police. Employees accused of the above will be subject to investigation under HEIWs disciplinary code along with potential criminal investigations.

16. Criminal Damage

16.1 HEIW maintains the right to actively pursue those individuals that inflict criminal damage to their property or equipment where the offender can be identified.

17. Counter Terrorism

17.1 Terrorism can take many forms from physical attack on life and limb to interference with vital information or communications. and there is a possibility (although highly unlikely) that HEIW could be the target of a terrorist attack. HEIW therefore needs to put in place plans to strengthen our protection against the threat of terrorism e.g. protection from flying glass, vehicle access controls, management of crowded areas, car parking controls and business continuity plans. It also needs to put in place competent staff to implement relevant procedures to deal with imminent and serious danger that may result in an evacuation and/or lockdown of HEIW and any relevant training, information and equipment for staff as well as the supply and installation of security equipment.

18. Out of Hours Incidents

18.1 The procedure for dealing with out of hours incidents relating to the HEIW headquarters, staff, equipment and key holding functionality is listed below.

18.2 Ty Dysgu will be open from 7am to 7pm Monday to Friday with the exception of bank holidays. The security firm (Kingdom Security) will unlock the car park barrier, unlock the building and deactivate the alarm system at 7am. They will unlock the outer front doors and set the outer front door to automatic to enable the staff to enter the main entrance. However, staff can access the rear entrance using their ID cards.

18.3 All staff need to leave Ty Dysgu by 7pm. The last person in each of the offices on the ground floor should close the blinds in their office and shut the door. They also need to check that all doors are firmly closed including the kitchen doors, the door and that lights in the meeting rooms have been switched off. The lights in the open plan areas will automatically switch off. When existing the building via the rear entrance through the shower room, press the green button to open the door and ensure that the door is fully closed.

18.4 The security staff will arrive at 7pm and will check that all doors are locked, set the intruder alarm, lock the building and the barrier to the car park. They will make random checks to the site during the night.

18.5 In the event that the alarm is triggered, the following individuals will be contacted by Chubb and advised of the situation. *First nominated Key Holder is David Price; second nominated Key Holder is Jane Powell.*

18.6 Any staff accidentally locked in Ty Dysgu should make contact with the security firm direct (Kingdom Security) details will be available on the noticeboard in reception.

20. Training

20.1 Whilst there are no formal training programmes in place to ensure implementation of this policy, each Executive Director, Senior Leader and operational lead must ensure that managers and all staff, clinical and non-clinical, are made aware of the policy provisions and that they are adhered to at all times.

20.2 Training must include equality and diversity training for managers, to highlight the risk of stereotyping in the workplace and service provision.

21. Resources

21.1 The implementation and management arrangements associated with this policy do not present any significant resource implications to HEIW.

22. Implementation

22.1 This policy will be maintained by the Planning, Performance and Corporate Services.

22.2 Please refer to the responsibilities section for further information in relation to the responsibilities in connection with this policy.

23. Audit and Monitoring

23.1 The Planning, Performance and Corporate Services team will review the operation of the policy as necessary and at least every 3 years.

24. Policy Conformance / Non Compliance

24.1 If any HEIW employee fails to comply with this policy, the matter may be dealt with in accordance with HEIWs Disciplinary Policy. The action taken will depend on the individual circumstances and will be in accordance with the appropriate disciplinary procedures. Under some circumstances failure to follow this policy could be considered to be gross misconduct.

25. Distribution

25.1 The policy will be available via HEIW Intranet Site. Where staff do not have access to the intranet their line manager must ensure that they have access to a copy of this policy.

26. Review

26.1 The Head of Planning, Performance and Corporate Services will review the operation of the policy as necessary and at least every 3 years.

27. Further Information

Further information and support is available from the Facilities and Compliance Manager on (01443) 824171.