Security Policy

BRITISH ASSOCIATION FOR PERFORMING ARTS MEDICINE

CARING FOR PERFORMERS' HEALTH

Category	Policy
Summary	This policy outlines BAPAM's principles and procedures for protecting its staff, clinicians, and patients within BAPAM's working environments. It places particular emphasis on security of personnel, property and premises. More details of specific hazards are outlined in the *Health & Safety* and *Lone Working* Policies.
Valid from	15 March 2016
Version	2.1
Date of next review	March 2019
Approval date/ via	BAPAM Medical Committee
Distribution	BAPAM clinicians e-mail & online forum Staff e-mail and meetings Public website
Related documents	*Employees Handbook* *Health & Safety Policy* *Lone Working Policy* *Incidents Policy*
Author	Dr Deborah Charnock, CEO
Further information/contacts	*Southampton Row:* Security: Office hours – Reception: 020 3008 6015 Security: Out of hours - OPEM systems: 0203 008 7247 or 0843 2999 365. *South Camden Centre for Health:* Security :07412 009 537 or Ext 1705 (externally 0203 182 1705) Operational Manager = Ext 1710 (externally 0203 182 1710)

Context

This policy outlines BAPAM's principles and procedures for protecting its staff, clinicians, and patients within BAPAM's working environments. It places particular emphasis on security of personnel, property and premises.

The policy is primarily relevant to personnel working in BAPAM's London office and clinic premises, although general principles apply in all settings.

Clinicians working in regional locations must familiarise themselves with local security procedures, which may accessed with the support of the BAPAM Office and Clinics manager. The same applies to staff undertaking offsite educational work and running events in hosted facilities.

Specific guidance on workplace hazards (eg. Fire procedures, equipment safety) is provided in the *Health and Safety* Policy and personal security in the *Lone Working* policy.

1. BAPAM's administrative offices: 31 Southampton Row, London WC1B 5HJ

1.1 General Access and Security

The BAPAM office in Southampton Row is a serviced office. Most security procedures are determined and overseen by the landlord, Avanta. Details are outlined in Avanta's Directory of Services. All BAPAM admin staff will be provided with a copy of the Directory, and it will also be available on the BAPAM Staff file of the shared W drive.

The following are key points from the Avanta Directory, with additional guidance specific to BAPAM staff:

1.1.i Building - Office hours security

The Avanta offices have a manned reception between 8.30am and 6pm Monday to Friday. Security support is available by contacting OPEM systems on 0203 008 7247 or 0843 2999 365.

Only authorised personnel are allowed into the offices and facilities within the building. Entry is by electronic pass: all BAPAM staff will be issued with their own electronic pass, and should not share it with unauthorised personnel. Colleagues working with BAPAM for extended periods will be treated as staff and will be issued with a temporary pass.

Avanta and the BAPAM Office and Clinics Manager will maintain a log of all passholders. Any personnel leaving the BAPAM permanently must surrender their security pass on departure.

Visitors must report to Reception and sign the log. BAPAM staff must, as much as possible, let Reception know the names of expected visitors and of any special access needs (wheelchair, etc).

BAPAM staff should only allow a visitor for BAPAM into the building if they are expected or known to the staff member.

BAPAM staff should not provide any visitors (to BAPAM or to other resident organisations) with access to other parts of the building unless they have evidence that this has been authorised.

BAPAM staff are entitled to deny entry to any personnel they consider a security risk or unwanted visitor.

BAPAM staff will be held liable by Avanta if they allow entry to someone who goes on to commit a crime within the building.

Cleaners are security checked by Avanta and fulfill their duties as outlined in their Directory document.

1.1.ii Building - Out of hours security

BAPAM staff can access the premises any time outside office hours using their security pass with a unique pin number issued and monitored by Avanta. Again, these should not be shared at any time with non-BAPAM personnel.

If any security issues arise, staff should contact OPEM Systems on 0203 008 7247 or 0843 2999 365. Staff working outside office hours should also follow guidance outlined in the *Lone Working* policy.

1.2. BAPAM office access and security

BAPAM's office in Southampton Row office consists of one outer office room opening onto the corridor, and one inner room accessed through a door between these rooms.

All permanent BAPAM personnel will be issued with a key to the outer office door.
The inner office door key is kept in a code-protected wall box in the outer office. The Office and Clinics Manager is responsible for setting the code, and communicating the code to BAPAM staff by secure e-mail.

All valuables, including confidential documents and equipment (server, laptop, projector), are kept in the inner office room. This room should be kept locked when not in use. Visitors are not allowed unauthorised access to BAPAM records or property and should never be left unattended, particularly with access to the inner office. (Issues relating to data security, particularly patient records, are outlined further in *Information Governance* policies).

The outer office door should also be locked when the office empty. The last staff member to depart on any occasion is responsible for locking all office doors.

The Chief Executive and the Office and Clinics manager are responsible for approving keyholders .The Office and Clinics Manager is responsible for maintaining a record of keyholders and instructing staff in office security and safety procedures.

1.3 Items for security

The Chief Executive and Clinics Manager hold keys to the filing cabinet in the inner office. The following items must be stored in the cabinet:

Petty Cash
Cheque books
Collection boxes

Only the Chief Executive has access to online banking details which are locked in the Chief Executive's desk and the Chief Executive is the only keyholder.

The Chief Executive and Clinics Manager are the only holders of ALTO cards which can be used for purchases, petty cash withdrawals and online payments (see Alto Card and Petty Cash procedures). These are kept on their persons. Records relating to the cards are held with the finance documents.

Trust Deed, Board and Medical Committee minutes are kept in the locked filing cabinet in the inner office.

Hard copies of staff records and other confidential BAPAM personnel information are kept in the Chief Executive's locked desk cabinet in the inner office. Summary electronic records are kept on the Shared Drive. Clinicians' records are kept in hard copy in the Office and Clinics Manager's locked desk and/or filing cabinet, and summary records are kept on the CRM database.

BAPAM maintains all electronic data on the secure server installed in the outer office. All passwords for general office admin and IT should be recorded on the Passwords file on the W drive.

BAPAM staff are responsible for the safety of their personal belongings.

1.4 Health and Safety: workplace hazards

BAPAM staff safety is the responsibility of the Office and Clinics Manager, who is also the Fire Safety and First Aid officer. BAPAM has an overarching Health and Safety policy provides and procedures for workplace hazards and safety.

The Avanta Directory of Services also outlines local procedures for fire safety, use of electrical items and cleaning/maintenance issues.

Staff will receive training at induction and regular updates on all aspects of workplace safety and security.

2. London Clinic premises: South Camden Centre for Health, 146 – 162 Drummond Street London NW1 2PL

BAPAM's London clinic operates from a rented clinic room in South Camden Centre for Health (SCCH) in Drummond Street near Euston. SCCH is a busy NHS outpatients facility (which also hosts several independent service providers) and has a comprehensive range of policies and procedures, including Personal Security.

2.1 General Access and Security

All BAPAM personnel, including clinicians, need to complete SCCH's induction programme prior to working at the Centre, and will have access to SCCH policy documents on the SCCH

shared computer drive. Copies will also be available through the BAPAM office. The Office and Clinics manager is responsible for scheduling SCCH inductions and highlighting local procedures (including full a list of full emergency contact details for BAPAM and SCCH). Key procedures are:

SCCH is open to patients between 8am and 6pm (staff can enter from 7.45am), Monday to Friday and has a manned clinics reception, *Operational Manager* (0203 182 1710 or 0203 182 1745 , or ext 1710 internally) and onsite *Security* (07412 009 537 or ext 1705 internally). As BAPAM uses the Centre as a part-time tenant, all BAPAM personnel must sign in at each visit and will be issued with temporary ID which must be worn at all times whilst on the premises. Staff will also be issued with temporary security passes for authorised entry to clinic areas.

BAPAM has a designated desk and computer within the main Reception space. Staff must not allow patients or unauthorised personnel into this area or other restricted access areas of the Centre. If staff need to discuss issues with patients after their consultation, they should either go back to the consulting room or meet in the Waiting Area or SCCH small meeting room near the main entrance.

Onsite security issues must be reported immediately to the SCCH Security officer and the SCCH Operational manager. The BAPAM Office and Clinics Manager must also be informed for Incident reporting and for implementing any staff support or training issues arising.

All personnel working at the Centre are responsible for their personal belongings. Cases of fraud or theft must be reported to the police, and to the BAPAM Office and Clinics Manager. The Office and Clinics Manager is responsible for reporting on to the Operations manager at SCCH (If the Office & Clinics manager is unavailable, or the incident poses an immediate security concern, staff should go directly to the Security officer and SCCH Operations Manager). The Office and Clinics manager is also responsible for reporting these events to the BAPAM Chief Executive as outlined in BAPAM's Incidents policy.

Personal panic alarms are available from SCCH Reception – they must be signed in and signed out (see Lone Working below).

Physical restraint should never be used.

3. Personnel-related security issues

Any issues arising from the behaviour of BAPAM personnel (staff, clinicians, volunteers) in any setting should be handled according to the Incidents or Whistle-blowing policies.

4. Reporting & Communication

All security incidents must be reported to the Office and Clinics Manager as outlined in the Incidents Policy. Additional reporting to personnel responsible for the host premises as outlined in their local policies and procedures must also be implemented.

Security issues for policy development, communication and shared learning will be the responsibility Chief Executive as outlined in the Incidents Policy.

5. Training & Support

All personnel will be offered appropriate training in Security, including dealing with difficult patients and in conflict resolution. The Chief Executive will be responsible for providing appropriate support to staff and clinicians involved in security incidents, in consultation with the Honorary Medical Director where appropriate.

6. Breach of Policy

All BAPAM personnel (staff, clinicians, trainers) will receive a copy of this policy as well as detailed operational guidance and will be required to comply as a condition of working at BAPAM. Breaches may constitute professional misconduct and could lead to a termination of contract and disciplinary action.

First edition January 2013
Revised October 2014
Second edition March 2016
Next review March 2019