Information Technology (IT) Use Policy

BRITISH ASSOCIATION FOR PERFORMING ARTS MEDICINE

CARING FOR PERFORMERS' HEALTH

Category	Policy
Summary	This policy outlines the requirements in relation to acceptable use of BAPAM's IT Systems to protect our organization, clients and employees against the risks associated with the improper use of IT Systems.
Valid from	May 2018
Version	1.1
Date of next review	May 2021
Approval date/ via	BAPAM Medical Committee
Distribution	BAPAM Trustee and clinicians e-mail & online forum Staff e-mail and meetings Public website
Related documents	Employee Handbook Clinical Governance Policy Clinician Agreement
Author	Dr Deborah Charnock, Chief Executive
Further information/contacts	

1. Background

The use of information technology, the Internet and other forms of electronic communications is an important part of everyone's work. While this technology provides essential tools to help us with our work, it also presents legal and business risks.

This policy outlines the requirements in relation to acceptable use of BAPAM's IT Systems to protect our organisation, clients and employees against the risks associated with the improper use of IT Systems.

2. Definitions

'IT Systems' include but are not limited to:

- all company owned or provided computer hardware, including desktop, laptop, and, handheld computers, telephones, mobile phones, voicemail, and other technology providing access to IT Systems, the Internet or third party information technology systems;
- all company owned, licensed and/or provided software, or any software accessed through the use of IT Systems, including computer programs, business applications, the Internet, company intranet; and
- all company owned electronic data or files, including individual computer files, electronic documents, application data, electronic mail/messaging and records of computer, Internet or company Intranet use.

3. Overall Policy Requirements

All BAPAM personnel (staff, clinicians, Trustees, volunteers) who use BAPAM's IT systems are required to:

- Ensure that IT Systems are used for proper business purposes and in a manner that does not compromise the confidentiality of sensitive or proprietary information;
- Know the rules and regulations that govern the use of technology in their jobs, particularly in communicating with clients and potential clients, and regarding the handling of confidential customer information;
- Act with dignity, integrity, competence, and in an ethical and professional manner in their communications with the public, clients, prospects, employers, and fellow employees;
- Maintain accurate company records in compliance with record retention policies applicable to such records.

4. Ownership of IT Systems

IT Systems and all information created, stored, sent or received on IT Systems are the property of BAPAM. BAPAM reserves the right to view, audit, intercept, change, monitor and delete any such information.

IT Systems are to be used primarily and predominantly for business purposes related to the individual's position.

Users are not permitted to retain BAPAM IT Systems, devices, applications or data when their employment or contractual relationship with BAPAM ends unless agreed otherwise and with reference to other specific policies (e.g. clinical research data).

5. Personal Use of IT Systems

BAPAM recognises the need for occasional, incidental personal use of IT Systems. However, BAPAM's IT Systems shall not be used:

- for any other business purpose outside of BAPAM's business purposes;
- when use will result in incremental cost to BAPAM
- in a way that impacts a user's ability to carry out their work duties effectively, or is disruptive to others in carrying out their work duties
- in any way that would violate the standards of this policy or other company policies relating to the use of IT Systems.

6. Unacceptable Use of IT Systems

The following activities are prohibited while utilising BAPAM's IT Systems:

- Publication, distribution, storage, requisition or transmission of chain letters or obscene, pornographic or otherwise offensive material, or other material prohibited by applicable law
- Publication, distribution, storage, requisition, or transmission of any data, information or material that may be reasonably perceived by another individual as harassing, abusive, or offensive whether through language, content, or the frequency or size of communication. Offensive materials include, but are not limited to, materials that might offend any reasonable person on the basis of their race, gender, age, national origin, sexual orientation, religious beliefs, disability or other status protected under law
- Transmission of confidential, sensitive or privileged material, and/or any material that should not be viewed by the public, without appropriate controls to ensure the confidentiality and integrity of such information, and to ensure the adherence to regulatory stipulations regarding transmission of such material (see *Confidentiality* and *Data Protection Policies*; *Data Transmission Procedures)*
- Unauthorised download, installation, distribution, use of, or access to unauthorised files, data or software
- Unauthorised modification, reconfiguration, upgrade or alteration of BAPAM's IT Systems or applications
- Unauthorised Internet statements that suggest the user is speaking on behalf of BAPAM or its affiliates
- Revealing your IT System's authentication information, such as network account password or application logon credentials, to unauthorised individuals or allowing an unauthorised individual access to or use of your assigned accounts
- Use of IT Systems to impersonate the identity of another individual or change any message or communication in any unauthorized way that misrepresents another individual
- Unauthorised deletion, modification, transfer or duplication of XXX data, files, software, applications, or documentation
- Use of non-BAPAM e-mail accounts to conduct BAPAM business or the use of 'auto-forward' rules to send electronic messages to any external non-BAPAM electronic mail or messaging address
- Use of any e-mail or messaging systems other than the company provided e-mail or messaging systems (e.g. use of Internet e-mail providers, including but not limited to Yahoo, Hotmail, and MSN)
- Engaging in criminal activity, or other illegal activity

7. Privacy and Confidentiality

Users of BAPAM's IT systems should be aware that their use of IT Systems can be viewed, monitored, intercepted or stored in accordance with company policy or relevant legislation.

By using IT Systems, employees and other users consent to monitoring and retrieval of, and waive any right to privacy in, such messages, data or information

8. Investigations

In certain circumstances, BAPAM may monitor and investigate usage of IT systems and retrieve any messages, data or information created, stored or transmitted using IT Systems. The circumstances for such investigations include, but are not limited to:

- Legal or criminal investigations
- Regulatory or statutory investigations
- Internal or external audit requirements
- Discovery or Subject Access Requests under applicable law
- Reports of suspicious, inappropriate or unauthorised activity
- Automated monitoring systems indicating patterns of suspicious, inappropriate or unauthorized activity by users of BAPAM's IT Systems

9. Data Protection

All data contained in IT Systems must be preserved, stored, protected, transmitted, and used in accordance with applicable laws governing data protection and privacy.

10. Enforcement and Breaches of Policy

It is the responsibility of all BAPAM IT System Users to ensure compliance with this policy.

Any individual who suspects a breach of this policy should notify the Director.

Disciplinary actions for violations of these policies will be in accordance with BAPAM's disciplinary procedures, and could be up to and including termination of employment.

Certain activity may amount to gross misconduct, such as but not limited to, transmission or downloading of any racist, sexist, pornographic, defamatory or libelous material, or other unlawful material, or disclosure of company confidential information or personally identifiable information.

Where appropriate, notice will be provided to regulatory and law enforcement officials. Users should be aware that criminal penalties exist for the use of electronic communication systems for the transmission or storage of unlawful content.

Version 1.0 March 2014. Version 1.1 March 2016 (updated by D Charnock)
Review due March 2017
Review due May 2021