BAPAM Data Protection, Information Governance and Use of IT Systems Policy

Category	Policy
Summary	This policy provides an overview of BAPAM's Information Governance principles, and the procedures followed to meet the requirements of the Data Protection Act 1998 and GDPR 2018 for handling personal information. Key priorities relevant to BAPAM's work: • Personal data is relevant, accurate and good quality • Personal data is kept, processed and transmitted securely • Processes for collecting and using personal data are transparent and open • IT systems are used appropriately, protecting our organisation, clients and employees against the risks associated with the improper use of IT Systems The Policy applies to all BAPAM personnel
Valid From	November 2026
Last Revised	November 2026
Version	1.0
Date of next review	November 2028
Approval via	BAPAM Board & BAPAM Medical Committee
Distribution	BAPAM Trustees & clinicians e-mail & online forum Staff e-mail and meetings Public website
Related documents	*Access to Medical Records* *Confidentiality Policy* *Clinical Governance* *Clinician Agreement* *Employee Handbook* *Health Records Management* *Incidents* *Research*

References	Data Protection Act 2018 GDPR guidance, ICO SEQOHS standards and evidence guide
Author(s)	Claire Cordeaux, CEO Dan Hayhurst, Director of Communications and Information Dr Finola Ryan, Executive Medical Director

This policy is the property of BAPAM and is a controlled document. The only up-to-date version is maintained on SharePoint. As a controlled document, it should not be saved on local drives and must always be accessed through SharePoint.

Although this document may be printed or downloaded, please be aware that the electronic version on SharePoint is the controlled copy. Any printed or downloaded copies of this document are not controlled and are only valid on the day of printing or download.

The version number and status of this document are indicated on the first page and in the footer. Any amendments to this policy will be recorded in the Policy Amendment Log below. The policy may be fully revised and re-issued at the discretion of the CEO, Medical Director or Director of Communications and Information.

Amendment Log			
Amendment date	**Version**	**Additions or Alterations**	**Initials**
November - 2026	1.0	This policy combines the previous *Information Governance (last updated by F Ryan in Feb 2026), Data Protection (D Charnock (2013), last updated by C Cordeaux (2024), Data Transmission, IT, Handling Confidential Information When Working Remotely* policies. Appendices covering social media and AI use have been added. It has been compiled from updated information following comprehensive review and aligns with the SEQUOS standard for information and communication.	DH

1. Background & Purpose

This policy outlines how BAPAM meets its legal obligations concerning the collection and security of personal data as required by the Data Protection Act 2018 ('the Act') and UK GDPR, including the Schedules and updates in force at the time of ratification of this policy.

BAPAM also has a duty to comply with guidance issued by the Information Commissioner's Office, the Charity Commission, and the Fundraising Regulator, and any other relevant guidance relating to the collection and handling of personal data.

In relation to personal data, BAPAM must also comply with additional legislation including the common law duty of confidentiality, and any other relevant legislation and professional guidance governing the retention, security, and confidentiality of medical records.

This policy outlines our Information Governance principles, including how we handle confidential information when working remotely, and methods of data transmission.

This policy also outlines the requirements in relation to secure and acceptable use of IT Systems, including company IT systems, social media and AI.

2. Scope

This policy and its appendices apply to all personnel working for and contracted by BAPAM, including Trustees, employees, clinicians, and volunteers.

Personal data includes all information which is 'about' an identifiable, living individual that is held in any format including, but not exclusively, written and electronic information.

Data Protection legislation consists primarily of guidance which organisations must consider when handling personal data. Compliance requires applying the seven Principles of the Act in ways that are appropriate to the organisation's context, balancing statutory guidance with the organisation's mission and ethos.

Within the context of BAPAM's work and mission, our data protection policy and practices focus on the following key priorities:

- Collected information is relevant, accurate and good quality
- Information is held securely, appropriately maintained and processed
- Data is suitably protected when working remotely
- Transparent information is provided about the use of personal data, and how service users can access their personal information

Information covered by our **Information Governance**, **Data Transmission** and **Handling Confidential Information When Working Remotely** procedures includes:

- Corporate governance documents including records of Trustee appointments, Board minutes, and correspondence with the Charity Commission and with legal representatives

- Commercial/business information including funding agreements, banking, salaries and contracting
- Employment records for staff including performance management, sickness and disciplinary action
- Professional records and contracts for clinicians and professionals who deliver BAPAM services
- Information about practitioners listed in the BAPAM Directory
- Supporter and subscriber records
- Healthcare Records of patients accessing BAPAM's clinical assessment services
- Clinical governance records including patient feedback and complaints, incident reporting, whistleblowing, and safeguarding cases
- Other service user records arising from Helpline contact and participation in BAPAM education and training events
- Email and telephone communications, mass media information including website and social media
- Research data including data arising from collaborative research projects

IT Systems include but are not limited to:

- Company owned computer hardware, phones, voicemail, and other technology providing access to IT Systems
- Company owned, licensed or provided software, or any software or IT system used while working for or in association with BAPAM, including business applications, AI tools, online platforms, social media, e-marketing tools and the internet
- Company owned electronic data, including individual computer files, electronic documents, application data, electronic mail/messaging and records of computer or Internet use

3. Definitions

Data Subject (natural persons) is the living individual to whom personal data relates.

Personal Data. Under the DPA 2018, personal data refers to any information relating to an identified or identifiable living individual – that is, an individual who can be identified directly or indirectly by the data. This includes names, identification numbers, location data, online identifiers or one or more factors specific to them, such as physical, physiological, genetic, mental, economic, or cultural information, or their social identity. Effectively, anything that could be used to identify an individual in some way is considered personal data, which includes technical factors such as internet IP addresses.

At BAPAM, the types of personal data held relate to:

- Personnel - employees, Trustees, clinicians and volunteers

- Service users:

- Performing arts professionals contacting BAPAM's Helpline
- Performing arts professionals registered on BAPAM's CRM system for access to services
- Participants attending BAPAM education and training events
- Visitors to BAPAM's website

- Subscribers and supporters:

- Healthcare or education practitioners listed in the Directory of Practitioners and/or delivering services
- Supporters giving donations via online services such as JustGiving
- Members of any subscriber and supporter schemes, including e-marketing lists

Special Categories of Personal data is personal data that has the potential to be used in ways that are discriminatory or harmful to the data subject if shared inappropriately, and as such, require higher standards of security than some other forms of personal data.

Special Categories of personal data is information about a data subject's: racial or ethnic origin; physical or mental health or condition; sexual life; political opinions; religious or other beliefs of a similar nature; membership of a trade union; the commission or alleged commission by the data subject of any offence, or any proceedings for any offence committed or alleged to have been committed by them, the disposal of such proceedings or the sentence of any court in such proceedings.

A ***Data Controller or Controller*** is the person within an organisation who determines (either alone or jointly or in common with other persons) the purposes for which, and the manner in which, any personal data is processed. The Data Controller must exercise control and take responsibility for the data protection of the information belonging to that organisation. This includes any agreements and contracts with third parties accessing that data – i.e. *Data Processors* (see below). At BAPAM, the *Data Controller* is currently the CEO.

A ***Data Processor or Processor*** is any person(s), other than an employee of the Data Controller, who processes the data (notably personal data) on behalf of the *Data Controller*. At BAPAM, data *processors* are most commonly independent contractors providing IT services (management of computers and secure cloud-based systems, our CRM system, website, mailing lists etc), as well as accountancy and human resources support. It may also include independent organisations and professionals working with BAPAM on shared patient care or research initiatives.

Processing in relation to information or data means obtaining, recording or holding the information or data or carrying out any operation or set of operations on the information or data.

A ***Healthcare Record*** for the purposes of the Act is one which relates to the physical or mental health of an individual which has been made by or on behalf of a health professional in connection with the care of that individual.

4. Legal Compliance

Although BAPAM is not a statutory service provider, it has a duty to comply with the Act and guidance issued by the Information Commissioner's Office (ICO) (and maintains an up-to-date notification with the ICO), the Charity Commission (Charities Act 2022), and the UK GDPR and Data Protection Act 2018. BAPAM must also comply with the common law duty of confidentiality in relation to medical records and special category data, and consider relevant guidance issued by the Fundraising Regulator relating to personal data management. BAPAM's policies and procedures for management of personal data also take account of additional relevant legislation listed below:

- *Access to health records 1990*
- *Access to medical reports act 1998*
- *Safeguarding Vulnerable Groups Act 2006*
- *Health & Social Care Act 2008*
- *Human Rights Act 1998*
- *Privacy & Electronic Communications Regulations (PECR) 2003 (How do we comply with the PECR electronic mail marketing rules? | ICO)*
- *Serious Crime Act 2015*
- *Equality Act 2010*

5. Responsibilities

The BAPAM Board of Trustees has overall legal responsibility for information governance and Data Protection compliance.

Day to day responsibility for Data Protection and Information Governance is delegated to the **CEO** as the Data Controller. The main responsibilities are:

- Briefing the board on BAPAM's Data Protection responsibilities
- Policy development, implementation, monitoring and effective mitigation of risks, including preparation of breach (*Incident)* reports and action plans involving Data Protection breaches and 'near misses' for the BAPAM Board and Medical Committee
- Reporting relevant breaches to the ICO within 72 hours
- Advising staff and personnel on Data Protection and Information Governance issues
- Ensuring the delivery of Data Protection and Information Governance induction and regular training
- Approving unusual or controversial disclosures of personal data (in consultation with the Executive Medical Director or a nominated Trustee where appropriate)
- Approving contracts with Data Processors
- Maintaining up to date notification with the Information Commissioner's Office
- Handling requests from individuals for access to their personal data (personnel and service users)

The **BAPAM Director of Communications and Information** has the following responsibilities:

- Delegated authority from the CEO for responsibilities listed above as follows:

- Briefing the Data Controller in identifying aspects of their area of work which have Data Protection implications and advising on guidance if necessary
- Reviewing Data Protection and related policies and procedures, ensuring that all BAPAM activities take full account of Data Protection requirements, and filing *Incident reports* and advising on and implementing action plans where required
- Advising, training and inducting staff on data protection issues
- Monitoring contracts with Data Processors

The **Executive Medical Director** is responsible for supporting and advising the BAPAM CEO, Director of Communications and Information, Clinics Manager and staff on specific Data Protection issues as they relate to BAPAM's *Clinical Governance policy* and healthcare management procedures.

All **BAPAM personnel** (Trustees, staff, clinicians and volunteers) are responsible for understanding and complying with this policy and the procedures that BAPAM has adopted.

6. Openness

BAPAM is committed to maintaining an appropriate balance between openness and confidentiality in the management and use of information. We actively support the principles of good corporate governance, accountability, and transparency by ensuring our data practices are clear and accessible. We place equal importance on robust security arrangements to safeguard confidential information about our personnel, patients, service users, and supporters, as well as commercially sensitive data.

7. The Seven Data Protection Principles

The Act imposes obligations on anyone who processes personal information to do so in accordance with the Seven Data Protection Principles and Schedules under the Act. These set down a framework for the lawful processing of data. A fundamental element of the Act is that it gives an individual the right to consent to their data being collected and used, to access the data held about them, and to have the data corrected or deleted where appropriate.

The Seven Principles and notes on BAPAM's general procedures for dealing with them are outlined in the section below. Additional, detailed operational considerations are outlined throughout this policy and its appendices.

Principle 1: Personal data shall be processed fairly, and lawfully and transparently.

In brief, to comply with Principle 1, BAPAM will always ensure that:

- there are legitimate grounds for collecting and using the personal data
- the data subject is asked for informed consent in a clear and unambiguous way and consent for their data to be processed has been recorded, including recording where consent has been subsequently withdrawn

- the data is not used in ways that have unjustified adverse effects on the individuals concerned
- all the individuals about whom data is collected are made aware of the uses that BAPAM makes of information about them
- staff handle people's personal data only in ways it would be reasonable to expect
- BAPAM does not do anything unlawful with the data

There are additional considerations concerning the processing of **special categories personal data**. BAPAM processes information about a person's ***physical and mental health*** (including ***sexual life*** where relevant) as necessary for ***medical*** purposes. Processing is only undertaken by:

  - a health professional, or
  - a person who, in the circumstances, owes a duty of confidentiality equivalent to that which would arise if they were a health professional

Medical purposes includes the purposes of preventative medicine, medical diagnosis, medical research, the provision of care and treatment and the management of healthcare services.

BAPAM may process information about a data subject's racial or ethnic origin, gender, and sexual orientation as necessary for the purpose of identifying or keeping under review the existence or absence of equality of opportunity or treatment between persons of different protected characteristics, with a view to enabling such equality to be promoted or maintained in all BAPAM's services and operations.

BAPAM processes information about ***membership of a trade union*** as follows:

i) performers registered on BAPAM's service user database: for anonymised service activity reports to Trades Union organisations who are BAPAM funders
ii) employees: in cases relating to employment legislation.

Principle 2: Personal data shall be used only for specified, explicit purposes.

BAPAM will always:

- be clear from the outset about why it is collecting personal data and what it intends to do with it
- comply with the Act's fair processing requirements – including the duty to give privacy notices to individuals when collecting their personal data
- comply with what the Act and GDPR says about notifying the Information Commissioner
- ensure that if BAPAM wishes to use or disclose the personal data for any purpose that is additional to or different from the originally specified purpose, the new use or disclosure is fair

Principle 3: Personal data shall be adequate, relevant and limited to only what is necessary (data minimisation).

BAPAM ensures that:

- it holds personal data about an individual that is sufficient for the purpose we are holding it for in relation to that individual
- it does not hold more information than we need for that purpose

Principle 4: Personal data shall be accurate and, where necessary, kept up to date.

BAPAM ensures that:

- it takes reasonable steps to ensure the accuracy of any personal data it obtains
- the source of any personal data is clear
- it carefully considers any challenges to the accuracy of information
- it considers whether it is necessary to update the information

Principle 5: Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.

To comply, BAPAM:

- regularly reviews the length of time it keeps personal data
- considers the purpose or purposes it holds the information for in deciding whether (and for how long) to retain it
- securely deletes information that is no longer needed for this purpose or these purposes
- updates, archives or securely deletes information if it goes out of date

Specific operational details relating to BAPAM's personal records management in relation to Principles 3 to 5 are outlined in the *Access to Medical Records Policy, Healthcare Records Policy*, *Employee Handbook,* and *Clinician Agreement*.

As patient records – both electronic and hard copy – contain extensive s*pecial categories* personal information, BAPAM considers retention and destruction particularly important. Digital records and hard copies are destroyed after **eight years** except for patients under 18 – these records must be retained until 26 years of age (our insurer's requirement).

Principle 6: Appropriate technical and organisational measures shall be taken to ensure the integrity and confidentiality of data and to guard against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

In practice, Principle 6 requires BAPAM to have appropriate security to prevent the personal data we hold being accidentally or deliberately compromised. In particular, we:

- design and organise security to fit the nature of the personal data we hold and the harm that may result from a security breach
- are clear about who in BAPAM is responsible for ensuring information security
- make sure BAPAM has the right physical and technical security, backed up by robust policies and procedures, well-trained staff and expert contractors –See *Information Security Procedures* below
- are ready to respond to any breach of security swiftly and effectively

Principle 7: BAPAM will be able to demonstrate accountability to UK GDPR and the Data Protection Act 2018.

This principle ensures that BAPAM is responsible for complying with the UK GDPR and can demonstrate compliance through appropriate technical and organisational measures to meet the requirements of accountability.

This includes:

- adopting and implementing data protection policies
- taking a 'data protection by design and default' approach
- ensuring written contracts exist with organisations that process personal data on our behalf
- maintaining documentation of our processing activities
- implementing appropriate security measures
- recording and, where necessary, reporting personal data breaches
- carrying out data protection impact assessments for uses of personal data that are likely to result in high risk to individuals' interests
- adhering to relevant codes of conduct and signing up to appropriate certification schemes

Accountability obligations are ongoing, and measures must be regularly documented, reviewed, updated and reported to the Medical Committee and Board.

8. Data Breach Reporting

All personnel must follow BAPAM's relevant operational procedures and inform the CEO in the event of a data breach being discovered. The CEO is responsible for reporting data breaches to the ICO within 72 hours.

It is a legal requirement to report a personal data breach to the ICO under the GDPR if it is likely to result in a risk to people's rights and freedoms. If there is the likelihood of a *high* risk to people's rights and freedoms, the breach also needs to be reported to the individuals who have been affected.

High risk situations area likely to include:

- the potential of people suffering significant detrimental effect – for example, discrimination, damage to reputation, financial loss, or any other significant economic or social disadvantage.

Under the GDPR there is a requirement for organisations to report a personal data breach that affects people's rights and freedoms, without undue delay and, where feasible, not later than 72 hours after having become aware of it.

Organisations will have to provide certain details when reporting, but the GDPR says that where the organisation doesn't have all the details available, more can be provided later. The ICO will not expect to receive comprehensive reports at the outset of the discovery or detection of an incident – but we will want to know the potential scope and the cause of the breach, mitigation actions we plan to take, and how we plan to address the problem.

9. Information and Consent

The UK GDPR defines consent as follows:

"Consent of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her".

Implied consent is therefore insufficient.

BAPAM informs personnel about the processing of their personal data through contractual information (see *Employee Handbook* and *Clinicians Agreement)*.

Service users are given clear and appropriate information to support informed decision-making.

BAPAM informs service users about the processing of their personal data, and the secure data transmission methods we will use, through written and verbal communications including registration and appointment emails and telephone calls, and online patient information resources. All staff are trained in providing this information.

BAPAM's policy is to inform service users – i.e. performers registering with us and participants at BAPAM events – of our privacy policy BAPAM Legal Information | Performing Arts Medicine

Clinicians record patient consent in the clinical record if it is necessary for BAPAM to share information arising from the clinical consultation in direct communications with third parties.

We request consent from service users to subscribe to our newsletter and an online mailing list for notifications of events and activities including fundraising initiatives.

In compliance with the PECR electronic mail marketing rules we may use the charitable purposes soft opt-in to send electronic mail marketing without consent (but not to people who have previously unsubscribed) where the message furthers our charitable purposes.

Procedures for opt-out are provided in all marketing emails.

All BAPAM direct marketing is conducted via email: we do not undertake marketing via personal letters, SMS messages or telephone calls.

BAPAM never offers data subjects' contact details to third parties for independent marketing purposes.

Visitors to the BAPAM website are informed about the site's use of Cookies under the Legal and Privacy section of the website.

10. Data Protection Impact Assessments (DPIA)

The GDPR includes an obligation to conduct a DPIA for types of processing likely to result in a high risk to individuals' interests. The Information Commission Office (ICO) guidance is that DPIAs are required for projects using data which:

- uses systematic and extensive profiling with significant effects;
- processes special category or criminal offence data on a large scale
- systematically monitors publicly accessible places on a large scale.

The ICO also requires a DPIA if there are plans to:

- use new technologies
- use profiling or special category data to decide on access to services
- profile individuals on a large scale
- process biometric data
- process genetic data
- match data or combine datasets from different sources
- collect personal data from a source other than the individual without providing them with a privacy notice ('invisible processing')
- track individuals' location or behavior
- profile children or target marketing or online services at them
- process data that might endanger the individual's physical health or safety in the event of a security breach

BAPAM will consider a DPIA for any major new data projects which involve the use of personal data, these are likely to include:

- migrating to a different CRM system
- providing access to researchers
- introducing new technologies

11. Right of access (data subject access requests)

Personal data is processed in accordance with the rights of data subjects under this Act

To comply, BAPAM has procedures in place which ensure data subjects have:

- a right of access to a copy of the information comprised in their personal data, in electronic format if this is how the information is stored
- a right to object to processing that is likely to cause or is causing damage or distress
- a right to prevent processing for direct marketing
- a right to object to decisions being taken by automated means
- a right to have inaccurate personal data corrected
- a right to have data erased, unless there is good reason not to do so
- a right to have their data transferred directly to another provider
- a right to claim compensation for damages caused by a breach of the Act

Additional relevant policies include *Healthcare Records Policy, Access to Medical Records policy* and *Employee Handbook*.

Individuals have the right to access their personal data and supplementary information so that they are aware of and can verify the lawfulness of the processing. This includes:

- confirmation that their data is being processed
- access to their personal data
- other supplementary information – mainly the information that should be provided in a privacy notice

BAPAM will provide a copy of the information free of charge unless the request is manifestly unfounded or excessive, particularly if it is repetitive, in which case the CEO will decide whether a fee should be levied on the administrative cost of providing the information. The information will be provided within one month, although can be extended to a further two months where requests are complex or numerous. If this is the case, the individual will be informed within one month of the receipt of the request as to why the extension is necessary.

BAPAM will verify the identity of the person making the request, using 'reasonable means', and if the request is made electronically, the information will be provided in a commonly used electronic format.

12. Sharing information

BAPAM's policy is that personal data should only be shared if explicit consent from the data subject has been given. Further details regarding the circumstances and process for sharing are outlined in the *Confidentiality Policy* and *Data Transmission Appendix*.

Occasionally, data relating to BAPAM personnel or patients may need to be shared without consent – for example, *Incidents* where there are criminal or *Safeguarding* concerns. In these circumstances, the BAPAM CEO and Executive Medical Director will act in accordance with relevant BAPAM policies and national guidelines (including Schedules relating to the Data Protection Act, as well as the Serious Crime Act 2015 and Safeguarding Vulnerable Groups Act 2016) and in consultation with a nominated Trustee where appropriate.

Note that personal data contained in routine *Incidents Reports* to BAPAM's Medical Committee is pseudonymised through use of CRM ID numbers: the identity of the patients and personnel described in these reports can only be decoded by authorised BAPAM staff, and some items may be excluded or circulation restricted to further protect a data subject's identity.

13. Information Security Procedures

BAPAM treats all personal data as confidential and keeps it secure and accessible only to authorised personnel. The following security measures are in place:

- All hard copy personal data is permanently stored in BAPAM's administrative offices, which are always self-contained and accessible only to authorised BAPAM personnel. Confidential medical records are held in a locked cupboard
- All hard copy restricted personnel records are stored in locked filing cabinets, which are only accessible to the CEO or nominated Trustee (see Employee Handbook)
- BAPAM operates a clear desk policy: staff keep all information out of sight of unauthorised personnel by keeping desks clear of confidential information
- All staff PCs are protected by passwords and screen-time outs
- All staff user accounts require MFA
- All access to our online systems is monitored and audited
- Power users who can access online patient records and core file libraries are enrolled in Microsoft Intune, enabling securely managed user access and the central control of devices, applications, and data. Only authorised users with compliant devices can access our core systems. Access from locations outside of the UK is restricted
- Intune prevents malware and viruses by centrally managing and enforcing Microsoft Defender Antivirus policies, and all software installation across all company devices

- All telephone conversations are kept confidential and held in a confidential space using headphones. The voicemail system is restricted to power users and accessed via secure mailbox on registered devices only

- BAPAM uses anonymised online survey forms to gather feedback from service users. No personal identifiable information (including IP addresses) is collected via these forms unless users choose to provide this

- All data security arrangements are under constant review and are discussed as a standing item either at the Board or Medical Committee

- BAPAM takes particularly seriously the storage and transmission of *Special categories* personal information in electronic format. Personal medical information is shared using secure file sharing methods. When necessitated, hard copy information may be sent by post

- When transmitting data, all BAPAM personnel follow the procedures outlined in the *Data Transmission Appendix*

- Procedures for processing personal information remotely (e.g. by Clinicians working at clinic locations other than BAPAM's London clinic, staff working remotely) are outlined in the *Guidance for Handling Confidential Information When Working Remotely Appendix*. A central requirement is that sensitive personal information should not be stored on personal devices

- BAPAM monitors data security issues through Data Controller/Processor contracts, staff training and centrally managed online systems. All access is logged. Any breaches, including 'near misses', are logged as Incidents (see *Incidents Policy*) and are discussed in detail at BAPAM staff and Medical Committee meetings, as well as in regular summary reports to the Board. Action plans arising from *Incident* reports may include updates to policies and procedures

- The Microsoft data center for our cloud-based systems is GDPR and HIPPA compliant, based in Dublin with backup in Berlin which meets with the EU adequacy decision, and we have checked that we are compliant with the ICO. Contracts with Data Processors all meet this requirement

14. Ownership and use of IT Systems

- Company IT Systems and all information created, stored, sent or received on these IT Systems are the property of BAPAM

- Users of BAPAM's IT systems are informed that their use of IT Systems can be viewed, monitored, intercepted, stored or deleted in accordance with company policy and relevant legislation

- 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)

- BAPAM permits the reasonable and appropriate personal use of IT Systems while at work, including personal social media during breaks

The following examples are **unacceptable uses of BAPAM's IT Systems:**

- 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

- 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

- 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

- Impersonating the identity of another individual or changing any message or communication in any unauthorised way that misrepresents another individual

- Unauthorised deletion, modification, transfer or duplication of company data, files, software, applications, or documentation

- Use of non-BAPAM email 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 email or messaging systems other than the company provided email 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

15. IT Systems Investigations

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 or indications of suspicious, inappropriate or unauthorised activity

16. Training

BAPAM staff receive Data Protection training on induction, and all personnel complete Data Security Awareness training at least once per three years. Additional mandatory Information Governance and Data Security training is undertaken at least once per three years by staff as required. All personnel receive regular notifications and updates from the CEO and Director of Communications and Information about Data Protection issues.

17. Breach of policy

All BAPAM personnel receive a copy of this policy and are required to comply as a condition of working at BAPAM. Any individual who suspects a breach of this policy should notify the CEO. In certain instances, breaches of the policy may constitute professional misconduct and could lead to disciplinary action. Certain activity may amount to gross misconduct, such as but not limited to, transmission or downloading of 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.

The policy will also be given to third-party contractors and data processors.

18. Clinical Audit and Research

BAPAM may conduct clinical audits and work with academic institutions to collaborate on research. The use of data is outlined in our *Research Governance Policy*.

Appendix 1: Data Transmission

This appendix sets out the security issues that BAPAM personnel should consider when transmitting patient data. The appendix is an integral part of this policy and breaches must be reported to the CEO as set out in Section 17: *Breach of policy*.

All BAPAM personnel are responsible for:

- getting patient agreement that the method of transmission is secure and acceptable.
- ensuring transmission is to an authorised and appropriate recipient
- assessing the risks in specific instances and proposing a method of transmission
- agreeing with the recipient that the method of transmission is adequately secure
- ensuring that the transmission reaches the intended recipient.

No security measures can achieve perfect security. BAPAM is committed, however, to taking security measures appropriate to the potential risk of harm to a patient that would be posed by information falling into the wrong hands (e.g. distress and breach of confidentiality). The types of patient information, level of risk and appropriate methods for transmission are outlined below.

Types of patient data and risk:

- **Patient names**

  Names on their own may not be especially confidential, unless there is other data associated with them or the individual is well known. Generally, sending such information is regarded as **low risk**.

  However, BAPAM undertakes not to identify any individual as a BAPAM patient, and some protection when transmitting names should be considered.

- **Patient contact details**

  Contact details (especially residential address and mobile phone numbers) must be treated as confidential, since they may pose a risk in the wrong hands.

  Sending these details should be considered **medium risk.**

- **Medical details and records**

  Medical details, patient and clinic records, clinician letters, test results etc, are highly confidential and potentially harmful to patients in the wrong hands.

  Sending these details should be considered **high risk.**

Key security principles & technical options

BAPAM has identified a range of options for transmitting confidential information as

appropriate to level of risk, whilst also aiming to avoid an unnecessary administrative burden or delay to patient care.

Electronic Transmission

a) File sharing

BAPAM's preferred method for transmitting confidential data (including patient information) is to send a secure SharePoint link to the recipient by email. The link only works for the specified recipient. All files remain in BAPAM's secure online file storage, and the recipient may read the file online and download a local copy if they wish. All access to online files is logged and can be audited.

To access the file, recipients need to either be logged into a Microsoft account with the email address used to share the file, or they will be sent a one-time passcode.

Patients sometimes find the passcode hard to access so an alternative method of electronic transmission is to:

b) A*ttach documents to an encrypted email*

Confidential information may be sent by encrypted email using Outlook encryption options. Before sending, check the intended recipient has been correctly identified and that their email address is correct. Recipients will need to use a one-time passcode or authenticate with the specified email address to read the message and access attachments.

c) Standard email

As a last resort where secure electronic transmission methods are not practical, the patient provides consent *in writing* that their correspondence can be sent by standard email. This can be in an email that should be tracked to the patient record in the CRM system.

Hard copies

Surprisingly few postal items go missing and standard post is considered a relatively secure method for transmission of patient data. BAPAM personnel may send hard copies in the post when necessary, including for accessibility reasons when electronic communications are not practical.

However, a consideration is that if hard copy information goes missing, it is instantly accessible to anyone who gets hold of it.

Note that premium postal services add little extra protection: e.g. 'Special Delivery' is tracked and receives some special handling, but its main benefit is compensation for lost items, not security.

Courier services are not necessarily more secure than ordinary post, and the same safeguards apply.

To maximise security, a hard copy item for post or courier should always be prepared as follows:

- placed in a well-sealed envelope

- addressed to a named person
- address should be checked as accurate and up to date
- BAPAM's return address must be included on the outside of the envelope
- correct postage must be paid
- if hand delivered, the identity of the receiver must be verified

BAPAM does not use or transport hard copy patient information for clinics. All information is transmitted electronically.

Appendix 2: Handling Confidential Information when Working Remotely

BAPAM's procedures for handling confidential information when working remotely (i.e. away from a BAPAM administration office) apply to all personnel (staff, clinicians, volunteers). This appendix is an integral part of this policy and breaches must be reported to the CEO as set out in Section 17: *Breach of policy*.

Enabling personnel to work remotely is key to BAPAM's operations as a national organisation providing services in a variety of locations and with a diverse workforce including part-time, sessional and volunteer personnel. Facilitating access to information through company, personal and mobile electronic devices and online systems is an essential for our work. However, these practices present special risks to the security and integrity of BAPAM information.

From confidential patient, personnel or organisational information accessed in the cloud, stored on laptops or printed, to contact details on a mobile phone, the inherent risks to information used in remote working environments should be apparent to all personnel. This Appendix provides practical advice and guidance to enable appropriate management of these risks.

Remote working heightens risks relating to information governance:

- Loss of information (through error or theft, including hacking)
- Damage to information (including computer viruses)
- Unauthorised disclosure

In turn, this can lead to risk of:

- Breach of confidentiality/data protection
- Compromised data quality
- Reputational damage
- Financial costs (including ICO fines due for breaches; compensation claims)
- Disciplinary action

BAPAM personnel are required to follow the working practices contained within this document and any related documents to ensure they:

- follow the correct processes and guidelines to facilitate safe remote access to confidential information
- understand their responsibilities in terms of the safe and effective use of company, personal and mobile devices
- understand their responsibility in relation to information protection, including Data Protection standards and the principles of confidentiality

Definitions:

Personal device: any electronic device or system which is not owned and controlled by BAPAM, that enables access to and processing of BAPAM information. This covers devices that operate within systems belonging to other organisations, as well as domestic-use devices (e.g. a family PC) and mobile devices (see below). Personal devices used to access BAPAM information pose special risks if they are also used by non-BAPAM personnel.

Mobile device: any device which renders BAPAM information portable. This may include (but is not limited to): laptops, tablets, mobile phones, storage devices such as USB sticks and portable drives. Mobile devices may belong to BAPAM or may fall within the 'personal devices' category.

Hard copy information: any information arising from BAPAM work that is held in a print format.

Responsibilities:

The CEO has overall responsibility for Information Governance, data protection and information management systems at BAPAM.

The Chief Executive in conjunction with the Director of Communications and Information, and line managers are responsible for ensuring that BAPAM personnel are made aware of and comply with the policy and related documents.

BAPAM personnel are bound by the same rules of confidentiality whilst working remotely as they are when working within the central BAPAM administration office. Individual personnel are responsible for the security of any electronic or hard copy information in their care which relates to BAPAM.

Operational Guidance:

Hard Copy information

- Secure electronic documentation, storage and transmission of all sensitive information is preferred over hard copy. If hard copy information is required for a specific purpose, we hold it only as long as necessary. Once the requirement is fulfilled, hard copies are destroyed, and digital records are kept online

- BAPAM does not store hard copy information for current patients. If we receive information in hard copy, it is digitised and added to the online patient record. If we create hard copy documents such as patient letters (e.g. for accessibility purposes), copies are retained in digital format only

- Historical hard copy patient records that are within the required data retention period are stored securely at BAPAM's London office and can only be accessed by authorised BAPAM personnel. If they require transmission, they are digitised, added to the online patient record, and transmitted electronically. Hard copy originals may then be destroyed

- BAPAM personnel whose main base is away from the London office do not access hard copy patient information. No BAPAM personnel take or store hard copy patient information offsite. Patient information is always accessed online using our secure SharePoint site

- All BAPAM personnel must follow a 'clean desk' policy, even if working from home

- Personnel should make every effort to ensure that sensitive and confidential information in any format is not misplaced, lost or stolen. They should be especially vigilant in public settings. The information should be carried as hand luggage when using public transport. BAPAM personnel must not leave notes, paperwork or mobile devices in a car overnight or for any extended period

- All information arising from work for BAPAM is the responsibility of BAPAM, and BAPAM may ask for it to be returned at any time

Electronic Information:

Electronic information is accessed directly via BAPAM's secure Email, SharePoint and CRM system, by authorised users only. Additional security measures are detailed in Section *13: Information Security Procedures*.

- Electronic information should not be downloaded onto local devices unless strictly necessary and must be permanently deleted from the local device as soon as it is no longer required

- Personnel must never access sensitive data or confidential information relating to their BAPAM work through online systems that are easily accessible to other, non-BAPAM users e.g. an email account that is accessible to family members on a home computer or to work colleagues on another organisation's device or system (e.g. a shared 'admin@...' email address)

- Personnel must ensure that passwords and authentication methods for accessing BAPAM information electronically are kept secure

- Personal and mobile devices must be locked whenever they are left unattended.

Incident reporting

Any adverse incident involving remote working must be reported in accordance with BAPAM's incident reporting procedures. Lost and stolen devices must be reported immediately upon discovery of the loss, to the Chief Executive and Director of Communications and Information.

Appendix 3: Social Media Use

This appendix sets out BAPAM's policies for use of social media. BAPAM's company social media accounts and all software used to manage them are included within the definition of 'IT Systems' in this policy. The appendix is an integral part of this policy, applies to all personnel including Trustees, employees, clinicians and volunteers, and breaches must be reported to the CEO as set out in Section 17: *Breach of policy*.

Our social media policies relate to:

1. Managing BAPAM's social media accounts
2. Representing BAPAM through social media
3. Using personal social media

What is social media?

Social media is the collective term given to web-based tools and applications which enable users to create, share and interact with content (words, images, graphics and video content), as well as network with each other through the sharing of information, opinions, knowledge and common interests.

In using the term "social media", we include platforms like Instagram, Facebook, Bluesky and LinkedIn, as well as online communities like blogs, social networks, chat rooms and forums, and messaging apps such as WhatsApp.

Why do we use social media and what can we use it for?

Social media is essential to the success of communicating BAPAM's work. It is important for designated staff and volunteers to participate in social media to engage with our audiences and stakeholders, contribute to relevant conversations, and raise awareness of our work, using the charity's corporate accounts. Some staff and volunteers may also support the charity's work using their personal accounts, and many will have social media accounts for personal use.

Building an engaged online community can lead to more significant long-term support and involvement from supporters. Social media guidance from the Charity Commission (September 2023) conveys how social media can be a highly effective way for a charity to engage its audiences and communicate about its work.

Social media helps us to:

- Promote our campaigns
- Share our news and updates with our audiences
- Celebrate our successes
- Raise awareness of important issues and challenges
- Support our fundraising activities
- Build an online supportive community
- Raise our public profile and strengthen our reputation

Why do we need a social media policy?

While social media brings the charity to a wide audience, it can also present risks. We want to ensure that all staff and volunteers using social media represent and reflect BAPAM in the best way possible. It is also important to mitigate risks (such as reputational or legal issues) associated with the use of social media to protect our supporters, personnel, work and reputation.

Point of contact for social media and authority to post on BAPAM's social media accounts

The Director of Communications and Information has overall responsibility for the management of our social media channels. Day-to-day publishing and monitoring is delegated to specified Comms Team members. No other staff member or volunteer is permitted to post content on BAPAM's official channels without the permission of the Director of Communications and Information or CEO.

Security

We uphold best practices for channel security with secure passwords, MFA and email notification of new logins in place. Never give out the passwords for our channels without express permission from the Director of Communications and Information.

Representing BAPAM through social media

Code of conduct headlines

• I will not insult, harass, bully or intimidate individuals or organisations
• I will respond to others' opinions respectfully and professionally
• I will not do anything that breaches my terms of employment/voluntary role
• I will acknowledge and correct mistakes promptly
• I will disclose conflicts of interest where I am able
• I will not knowingly post inaccurate information
• I will link to online references and original source materials directly
• I will be considerate, kind and fair
• I will always ensure my activity does no harm to the organisation or to others
• I will champion BAPAM and its services

- Staff and volunteers must ensure they reflect BAPAM's values in what they post and use our tone of voice. Only the Comms Team is permitted to respond to comments on our social media posts on behalf of the organisation. All posts and comments should be attributed to the charity and not an individual. In special cases it may be appropriate for a staff member or volunteer to make an individual comment as themselves, but this should be under the supervision, and with the approval, of the Director of Communications and Information

- When posting from BAPAM's social media accounts, you must respond to comments in the voice of our charity and not allow your own personal opinions to influence responses. Personnel must not reveal their personal opinions via our accounts

- Collaborative posts, 'liking', 'sharing' or 'reposting' as BAPAM, are means of highlighting information helpful to our service users, including sources of health advice. Care must be taken, however, to ensure that only appropriate content is shared or highlighted in this way. Examples of appropriate content include initiatives from partner organisations and trusted information provided by known health professionals such as practitioners listed in our Directory. All shared content must be approved by the Director of Communications and Information or specified Comms Team members

- Staff and volunteers must make sure that all social media content has a purpose and a benefit for BAPAM to further our charitable purposes (either directly or indirectly, by engaging stakeholders and building our brand using our strategy). All content must accurately reflect BAPAM's agreed position

- Those responsible for the management of our social media accounts should answer questions as swiftly as possible to help and engage with our service users and supporters. This will include signposting to appropriate services including the BAPAM helpline

- Clinical advice must never be provided via social media. All clinical enquiries must be signposted to the BAPAM helpline team

- **Protection, intervention and safeguarding:** If, during a social media interaction, personnel consider that a person/people is/are at risk of harm, they should follow BAPAM's safeguarding policy and report the safeguarding concern to the Executive Medical Director. As direct messages are not always monitored, automatic responses are in place which make this clear and provide contact details for the BAPAM helpline. More generally, the responsibility for measures of protection from harm for users of a particular platform lies first with the social networking site itself

- Personnel could be subject to unpleasant or abusive comments directed at the charity, our work or people. We encourage everyone who is on social media to be aware of our safeguarding, wellbeing and Incident raising procedures, and consult with a member of the Senior Management Team

- BAPAM does not encourage others to risk their personal safety or that of others, to gather materials in pursuit of social media engagement or for fundraising or awareness raising purposes. For example, promoting an unsafe challenge or visiting an unsafe location

- Staff and volunteers must not encourage people to break the law to supply material for social media, such as using unauthorised video footage

- BAPAM is not associated or affiliated with any political organisation. We can express views where appropriate on policies that impact our work and service users, but it is essential that BAPAM remains, and is seen to be, politically neutral. We cannot endorse a political party or candidate. We must carefully manage the risk that we are perceived to have any party-political bias and should carefully consider any posts which might be perceived as such, for example, posts which talk about individual politicians or parties rather than policies. Be aware that some partner organisations such as trade unions may be affiliated with a political party and exercise discretion if interacting with content that may be perceived as having any party-political bias

- Check facts and be honest. Personnel should not automatically assume that material that's shared or included in any post is accurate and should take reasonable steps where necessary to seek verification – for example, by checking data/statistics and being wary of photo manipulation. If you've made a mistake, don't be afraid to admit it. But think first about how to manage any risk to the charity and its brand in doing so by consulting with the Comms Team to craft the response

- Seek advice for complaints. If a complaint is made on BAPAM's social media channels, staff and volunteers should seek advice from the Director of Communications and Information, CEO or Medical Director before responding

- Know what to do in a crisis. Sometimes issues can arise on social media which can escalate into a crisis because they are sensitive or risk serious damage to the charity's reputation. Examples might include: a complaint about BAPAM personnel, registered practitioner, or a clinical service delivered, or a claim that information we have published is incorrect or has led to harm. The nature of social media means that complaints are visible and can escalate quickly. Not acting can be detrimental to the charity or our people. If there is an issue that could develop or has already developed into a crisis situation, the Director of Communications and Information and CEO must be informed, and they will take action as outlined in BAPAM's Risk Register and Crisis Response Plan. All personnel should report complaints or comments that could escalate into a crisis or have serious implications for the charity. Only the Directory of Communications and Information is permitted to amend or delete content in a crisis

- Personnel who monitor BAPAM's social media channels may be working part time and be carrying out other tasks in addition. All direct messages trigger an automatic response which makes it clear that important or urgent messages should be sent using alternative contact methods

- Use AI appropriately. AI can be a valuable tool that can support our communications activities. However, staff and volunteers must ensure AI created content adheres to our AI policy as outlined in Appendix 4

- **Confidentiality:** Communications must not breach confidentiality. Information about patients and service users must never be disclosed unless consent has been given. For example, service users may wish to share their story for fundraising or awareness campaigns. Other information may also be confidential, such as business data meant for internal use only or information that BAPAM is not ready to disclose yet. For

example, a news story that is embargoed for a particular date, or information from people who the charity has worked with which is private

- It is critical that all staff or volunteers abide by the laws governing copyright, under the Copyright, Designs and Patents Act 1988, when representing the charity. Never use or adapt someone else's images or written content without permission. Failing to acknowledge the source/author/resource citation, where permission has been given to reproduce content, is also considered a breach of copyright. Ensure images are licensed, or that we have documented permission to use them, and they are correctly attributed

- **Accessibility:** We endeavour to ensure our social media is as accessible as possible. This includes:

    - Using plain English, accessible fonts and avoiding small text sizes
    - Using contrasting colours
    - Using subtitles where appropriate
    - Using alt text for videos and images
    - Explaining text contained in an image in the copy that accompanies it

- **Use of social media in the recruitment process:** Any advertising of vacancies should be coordinated by the Senior Management Team and promoted through approved channels. There should be no systematic or routine checking of candidates' online social media activities during the recruitment process, as conducting these searches might lead to a presumption that an applicant's protected characteristics, such as religious beliefs or sexual orientation, played a part in a recruitment decision. This is in line with BAPAM's Equality and Diversity Policy

- **Use of social media to support fundraising activities:** Our social media platforms play a key role in our fundraising efforts and engaging with our donors. Personnel should adhere to The Code of Fundraising Practices

- **Public Interest Disclosure:** Under the Public Interest Disclosure Act 1998, if a staff member releases information through BAPAM's social media channels that is considered to be in the interest of the public, BAPAM's Whistleblowing Policy must be initiated before any further action is taken

Use of personal social media accounts — appropriate conduct

This policy does not intend to inhibit personal use of social media but flags up those areas in which risks or conflicts might arise. All BAPAM personnel (for the purposes of our social media policies, 'personnel' includes independent practitioners listed in our Directory), are expected to use all forms of communication appropriately and responsibly, in ways that are considerate of BAPAM's values and policies, both online and in real life

- Personnel should not state or imply that personal opinions and content are authorised or endorsed by BAPAM

- Personnel must not use the BAPAM logo in social media profiles or posts in any way that may indicate that a personal profile or post is managed or authorised by BAPAM

- Personnel, including practitioners listed in BAPAM's Directory must ensure that they make it clear that their own social media content is not endorsed or produced by BAPAM. When content is agreed in advance with the Director of Communications and Information or specified Comms Team members, collaborative posting may be used for purposes such as sharing health information and marketing events

- Those in senior management including trustees and public-facing or specialist roles where they are well known in their field of expertise, must take particular care as personal views published may be misunderstood as expressing BAPAM's view

- Personnel should express opinions and deal with differences of opinion respectfully. Don't insult people or treat them badly

- Posting or sharing defamatory, offensive or derogatory content on personal social media accounts is not acceptable, may be considered a breach of BAPAM's Equality and Diversity policy, and could lead to disciplinary action

- Use your common sense and good judgement. Be aware of your association with BAPAM and ensure your profile and related content is consistent with how you wish to present yourself

- Don't approach VIPs directly. Don't approach high profile people or organisations from your personal social media accounts to ask them to support the charity, as this could hinder any potential relationships that are being managed by BAPAM. This includes asking for reposts about the charity. If you have any information about high profile people or organisations that have a connection to our cause, or if there is someone who you would like to support the charity, please speak to the CEO or Director of Communications and Information to coordinate an approach

- Refer press enquiries. If personnel are contacted by the press about their social media posts that relate to BAPAM, they should talk to the Director of Communications and Information or CEO immediately and under no circumstances respond directly

- Keep political activity separate from the charity. Personnel are expected to uphold BAPAM's positioning. Staff and volunteers who are politically active in their spare time need to be clear in separating their personal political identity from BAPAM and understand and avoid potential risks and conflicts of interest. Staff should also inform their line manager and the Director of Communications and Information or CEO about any such political activity, and trustees should inform the Chair. Senior staff and trustees should take particular care

- Personnel could be subject to unpleasant or abusive comments directed at the charity, our work or people. We encourage everyone who is on social media to be aware of our safeguarding, wellbeing and Incident raising procedures, and consult with a

member of the Senior Management Team

- Everyone should be vigilant regarding suspicious content or links and must not reveal personal, confidential or sensitive information about themselves, other staff members, service users, volunteers or supporters of BAPAM. Be wary of fake accounts that may claim to be BAPAM and immediately notify the Director of Communications and Information and CEO

- Care must also be taken to ensure that any links to external sites from our social media accounts are appropriate and safe

Appendix 4: Artificial Intelligence

Aims and Context

Artificial Intelligence (AI) provides new opportunities to improve BAPAM's work but must only be used to support our charitable objectives and use must be transparent and ensure we stay within our data protection, confidentiality and clinical governance policy framework. We are also mindful of the environmental impact of AI. This policy aims to set out some principles to guide our work as we better understand how best to harness the potential benefits of AI.

What is AI?

AI refers to a machine's ability to carry out tasks that normally require human intelligence, such as understanding language, generating content, recognising patterns or making decisions. Common tools include ChatGPT, Claude, Microsoft Copilot, and DALL·E. BAPAM is currently using AI to support research on policy and best practice, for transcribing notes, creating graphics and in search engines.

Core Principles for Using AI Responsibly

The following principles are to guide BAPAM in responsible use of AI. Staff should always be clear about the purpose of using AI for BAPAM's work. Purposes are likely to be:

- To improve efficiency
- To deliver services
- To promote innovation
- To increase fundraising.

Principles

- AI should only be used to support BAPAM's charitable objectives.

- BAPAM should disclose when AI has been used to create or assist content – especially in public communications.

- Human oversight and judgement must be applied at all times. All AI information should be fact-checked. Trustees and staff remain accountable for decisions and outputs, even when using AI.

- No personal, confidential or sensitive data should ever be entered into AI tools – especially if
cloud-based or publicly hosted (like ChatGPT). Always comply with UK GDPR and Data Protection policies.

- AI tools can unintentionally reflect and amplify social biases. Staff should be aware of this and
actively look for unintended bias in outputs.

• AI outputs will not necessarily be original or legally safe to publish and copyright laws must be
followed and all references published.

• Using AI in tools for users may increase cyber security risks and should always be approved by the Director of Communications and Information.

Development and Training

AI is a new technology to us, and further risks as well as helpful AI solutions may emerge. Staff will be required to work with in the purposes and principles above when using AI and to respond to an annual audit on how they are using AI in their work to help BAPAM to evolve policy and practice in this area. BAPAM will be guided by charity resources in this area (e.g. Charity Digital - Topics - How to create an AI policy; Charity Digital - Topics - How to train staff in the age of AI) in order to navigate our way through the risks and benefits of using this technology.

Staff should not use AI if they do not feel sufficiently competent to do so, and if they do not understand the likely impact of using AI. BAPAM will offer training and support to staff interested in developing their use of AI to improve and sustain the work of BAPAM. Our work is very people focused and we are not looking to replace staff with AI but to scale our offer by improving efficiency. Any member of staff wishing to use AI for work should attend the following course Introduction to AI (1 hour), unless they have prior learning. This is free to access.

Senior staff should review Charity Excellence resources Charity Excellence - AI Ready for Charities

The development and training programme, and annual audit will be overseen by the Director of
Communications and Information, and staff engagement is welcomed, but will also be supported subject to capacity.

Version Control

Version control		
Version	**Date**	**Author Initials**
1.0	November 2026	DH

Date of next review: November 2028