



Title	Data Protection Policy	Document No.	HP 013
Author	Jim Murphy	Revision No.	03
Approval	Jim Murphy	Issue Date	April-21

PAM Group Data Protection Policy

This is a public policy produced by PAM Group and intended for our stakeholders. These include our clients, their employee's our colleagues, job applicants, suppliers and any regulatory authority.

PAM Group looks after the information it holds about you and respects your privacy. We will always take appropriate security precautions to prevent your information being lost or falling into the wrong hands or not processed for its intended purpose.

The data that we hold is both personal data and sensitive personal data. We make sure that the information we hold is as accurate as possible; we do not hold more information than we need; and we do not hold it longer than we need to.

We do not share your data with anyone else without your permission, except when we believe it is the only way to prevent harm to you or other people. If we do disclose information without your permission, this is authorised by our Data Controller who is also the Managing Director.

Other policies to be referred to:

- Privacy Policy see our website www.pamgroup.co.uk
- Our Consultation Policy see our website www.pamgroup.co.uk

Introduction and Principles

This policy applies to the whole of PAM Group, People Asset Management Limited, PAM Wellbeing Limited, Premier Occupational Health Ltd and PAM Recruitment. PAM Group processes data for the purposes of providing occupational health services, rehabilitation services and our own administration including employment, finance and administration.

PAM Group is committed to good practice in the handling of personal data and careful compliance with the legal requirements of the Data Protection Act 2018. PAM Group aims above all to protect people from harm through data being misused, mismanaged or not being held securely.

PAM Group also ensures that it takes account of the legitimate concerns of individuals about the ways in which their data may be used. In particular, PAM Group aims to be open and transparent in the way it uses personal data and, where relevant, to give individuals a choice over what data is held and how it is used.

PAM Group has policies and procedures in place to ensure that it complies with the eight Data Protection Principles set out in the Data Protection Act. These specify, in brief, that personal data must be:

1. Processed fairly and lawfully;



Title	Data Protection Policy	Document No.	HP 013
Author	Jim Murphy	Revision No.	03
Approval	Jim Murphy	Issue Date	April-21

PAM Group Data Protection Policy

2. Obtained for specified purposes and then only used for those purposes;
3. Adequate, relevant and not excessive;
4. Accurate and up to date;
5. Not kept any longer than necessary;
6. Processed in accordance with the data subject's rights;
7. Securely kept; and
8. Transferred outside the UK only in certain circumstances.

The most important risks which this policy addresses are:

- Inappropriate disclosure of personal data about service users that puts an individual at personal risk or contravenes a duty of confidentiality;
- Negligent loss of data that would cause concern to people whose data was lost and would seriously affect PAM Group's reputation;
- Failure of our colleagues to follow good practice in the processing of data
- The management and security of our premises and computer systems that securely store data.

Responsibilities

The Board of Directors of PAM Group recognises its overall legal responsibility for Data Protection compliance. Day to day responsibility for Data Protection is delegated to the Managing Director as the nominated Data Protection Officer. The main responsibilities of the Data Protection Officer are:

- Briefing the Board on their and PAM Group's Data Protection responsibilities;
- Reviewing Data Protection and related policies;
- Advising our colleagues on Data Protection issues;
- Ensuring that Data Protection induction and regular training takes place;
- Approving unusual or controversial disclosures of personal data;
- Approving contracts with Data Processors (external contractors and suppliers of outsourced services);
- Notification (i.e. registration with the Information Commissioner); and
- Management of subject access requests from individuals for access to their personal data.

Our operational Directors and Senior Management Team have responsibility for data protection within their own area of operation. However, all of our Colleagues are responsible for ensuring information and data is maintained securely in accordance with this policy and procedures that apply to their area of work. All of our Colleagues have the following responsibilities:



Title	Data Protection Policy	Document No.	HP 013
Author	Jim Murphy	Revision No.	03
Approval	Jim Murphy	Issue Date	April-21

PAM Group Data Protection Policy

- Assisting the Data Protection Officer in identifying aspects of their area of work which have Data Protection implications so that guidance can be provided as necessary;
- Ensuring that their activities take full account of Data Protection requirements; and
- Engaging fully in Data Protection and confidentiality training.

Confidentiality and Security

PAM Group recognises that a clear policy on confidentiality of personal data – in particular that of service users – underpins security. It maintains a policy that sets out how our colleagues are authorised to access which data and for which purposes.

All colleagues are required to abide by any security measures designed to protect personal data from loss, misuse or inappropriate disclosure or processing data for any other reason other than the delivery of services that the Company has accepted.

Principles underlying operational procedures

Good Data Protection practice is, wherever relevant, incorporated into everyday operational procedures. PAM Group holds ISO 27001 Accreditation for Information Security Management. Our principles include:

- Transparency, so that all the individuals about whom data is collected are made aware of the uses that PAM Group makes of information about them, and in particular to whom it may be disclose. See our Privacy Policy and Consultation Policy
- Informed consent, where necessary, especially in the case of service delivery;
- Good quality data, so that all the data held about individuals is accurate and can be justified as adequate, relevant and not excessive;
- Clear archiving and retention periods; and
- Security, proportionate to the risk of information being lost or falling into the wrong hands.

Specific legal provisions

PAM Group maintains an up to date Notification with the Information Commissioner as required by law.

All contracts between PAM Group and external data processors are reviewed by the Data Protection Officer for compliance with Data Protection Act requirements.