Information, Communication, Technology (ICT) and Security Policy

Approved by Board of Trustees on:

Review Cycle: Every two years

Next Review Due: 2028

Lead Staff Member: Jackie Rosenberg

Purpose

This policy is designed to emphasise the importance that PDT places upon security of its property, confidential information and electronic systems including any computer and any accessory or peripheral device connected to or networked with any such computer, in this policy referred to as the organisation's "property". This policy is also designed to ensure the security of PDT's computer equipment, network, software and physical property including its premises and associated security measures.

PDT property should be used for the business interests of the organisation and must not be used in any way contrary to those interests. PDT will take active steps to protect its property, including taking legal action. Any copying, distribution or abuse of any organisation property other than for the organisation's legitimate business purposes is strictly prohibited. PDT information should not therefore be disclosed to any third party or be made use of in any other way without permission.

PDT reserves the right to change the terms of this policy from time to time and to introduce a replacement procedure as may be required.

Data Protection

PDT processes personal information in accordance with the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018 and associated legislation.

All staff, volunteers and contractors must ensure personal data is processed lawfully, fairly and securely.

Particular care must be taken when processing special category data, including health, safeguarding and equality information.

Definition and Scope

This policy applies to all employees, volunteers, agency workers, independent contractors or any other worker afforded access to PDT property, referred to in this policy as "employees". It should be read in conjunction with PDT's disciplinary, data protection and equal opportunities policies. The policy sets out rules in relation to the use of PDT computer equipment.

For the purposes of this policy, computer equipment shall mean any hardware or software that uses or comprises electronic or computer code or circuitry, including but not limited to PCs, laptops, fixed or mobile telephones, photocopiers and scanners, televisions, CCTV systems, electronic storage media, and video or sound recording equipment. It also covers all aspects of the organisation's security measures designed to protect such computer equipment, including but not limited to entry codes, passwords, electronic codes in security

fobs, electronic keys and alarm systems, as well as the organisation's computer equipment and networks.

Employees are given access to PDT information and property, including its computer equipment, to carry out their duties for the organisation and for that purpose only. Any loss sustained by PDT as a result of a breach of this protocol, whether intentional or unintentional, will give rise to disciplinary action and all employees are asked to take great care with electronic security systems. The loss and/or failure of any electronic or other security measure or equipment must be reported to the employee's line manager or other appropriate person immediately.

Principles

Employees must not, under any circumstances:

- use any device (including any flash drive, memory or mirroring device) in combination with PDT property unless specific authorisation has been given for that particular purpose;
- use any PDT computer, photocopier, scanner or any other copying device for the purpose of copying information onto any medium other than in PDT's business interests;
- download or upload any computer software, data, code or information belonging to PDT other than for business purposes;
- introduce any electronic storage media (e.g. CD, DVD or USB drive) to PDT computers unless it has been checked and approved by a person in authority within the organisation;
- use PDT property or any property in any way that will increase the likelihood of damage arising from the introduction of unscreened software or hardware that may expose that property to viruses, spyware or malware of any kind;
- use the organisation's property to harass, discriminate against, bully, defame or act offensively in any other way toward any person whether or not an employee of the PDT, directly or indirectly and inside or outside working hours.

Any breach of this policy or unlawful act carried out using PDT's computer equipment will give rise to an investigation which may to disciplinary proceedings and could, in serious cases, result in dismissal and/or entail disclosure of any facts or information to the police or other enforcing authority.

PDT also reserves the right to take legal action in the civil courts to recover losses sustained or about to be sustained as a result of any breach of this policy including any potential breach.

Password management – individuals

All users are responsible for maintaining the confidentiality of their passwords. Any system capable of using passwords must have the facility enabled. An individual should not use the same password for multiple systems.

Passwords must:

- Be unique to each system.
- Never be shared with another person.
- Never be written down in an insecure location.
- Never be transmitted by email or unsecured messaging.

Where systems permit, passwords should:

- Consist of a strong passphrase.
- Be at least 8 characters long.
- Passwords must not be a combination of characters that is likely to be guessed such as a family name, nickname, pet's name, DOB, car registration or consecutive characters e.g. ABC123

Passwords must be changed:

- If compromise is suspected.
- Following accidental disclosure.
- When instructed by IT support.

Following National Cyber Security Centre's recommendations, Routine password changes at fixed intervals is no longer regarded as good practice. Unique passphrases personal to the individual provides stronger protection.

Password management – organisation

To help Protect PDT systems from unauthorised access PDT will use:

- Login throttling or account lockouts after a number of failed attempts
- Geo location based restrictions to help limit access
- Security Monitoring, to log all failed attempts and notify unusual behaviour, or possible compromised accounts to IT staff
- Continuous adaptation of password trends and disallow passwords that have been frequently compromised or used.

Multi-Factor Authentication (MFA)

Multi-Factor Authentication must be enabled wherever technically available.

This includes:

- Microsoft 365 accounts
- Email systems
- Remote access services
- Cloud-based applications
- Administrative accounts

Users must not deliberately disable or bypass MFA controls.

Security Awareness

All staff, volunteers and contractors shall receive information security and data protection training appropriate to their role.

Refresher training will be provided periodically and following significant changes in systems, threats or legal requirements.

System access

Access to IT systems shall be granted according to business need and the principle of least privilege. Users will only be granted access appropriate to their role and responsibilities.

Access will only be given once adequate training has been received and competence demonstrated to the trainer.

Where systems are implemented and maintained by a third party and are not under the control of PDT's IT, training must be carried out by that third party

In the case of mobile devices including laptops and other devices capable of storing or displaying organisational information, e.g. email access, the devices must be protected in line with this policy.

Should there be an actual or suspected breach of security or of this policy, the organisation may restrict an individual's or group of individuals' access to any or all systems.

Device Security and Compliance

All PDT devices must be enrolled into the PDT device management system (Microsoft Intune) where the devices security compliance level can be enforced and monitored. This includes:

- Passwords or biometric authentication must be used to gain access
- Anti-malware software is kept up to date

- Security patches are applied within recommended time frames based on severity
- Device encryption is enforced and cannot be disabled.
- Devices will be automatically restricted access to PDT systems if the device falls out of compliance

Users must:

- Lock devices when unattended.
- Report lost or stolen devices immediately.
- Allow security updates to install when required.

Encryption Requirements

All laptops, mobile devices and removable media storing PDT information must use approved encryption wherever technically possible.

Confidential and personal information must be protected:

- At rest on devices.
- During electronic transmission.
- During backup and recovery processes.

Unencrypted storage of confidential information on portable devices is prohibited unless formally authorised.

Remote and Mobile Working

When working remotely, users must:

- Maintain physical security of devices.
- Prevent unauthorised viewing of information.
- Lock screens when away from devices.
- Use only approved access methods.
- Exercise caution when using public Wi-Fi.

Confidential information must not be left visible in public places or unattended locations.

Artificial Intelligence and External Services

Employees must not enter confidential PDT information into publicly available artificial intelligence tools unless explicitly authorised.

This includes:

- Personal data

- Health information
- Safeguarding information
- Financial information
- Board papers
- Commercially sensitive information

Any proposed use of AI systems must comply with:

- Data protection legislation
- Confidentiality obligations
- PDT information security requirements

Third-Party Suppliers and Service Providers

Third-party suppliers with access to PDT systems or information must be subject to appropriate risk assessment and due diligence.

Where personal data is processed on behalf of PDT:

- Appropriate contractual arrangements must be in place.
- Data Processing Agreements must be maintained where required.
- Security responsibilities must be clearly defined.

Suppliers must promptly notify PDT of any incident that could affect PDT information or services.

Security Incident and Data Breach Reporting

Any actual or suspected information security incident must be reported immediately.

Examples include:

- Phishing attacks
- Malware infections
- Password compromise
- Unauthorised access
- Loss or theft of equipment
- Accidental disclosure of information
- Data breaches

Reports should be made immediately to:

- The Chief Executive
- The IT Support Provider
- Any designated Data Protection Lead

Certain personal data breaches must be reported to the Information Commissioner's Office within 72 hours of becoming aware of the breach. Employees must therefore report incidents immediately.

Where the Chief Executive is implicated in the incident, the matter should be reported directly to the Chair of Trustees.

Personnel must not attempt to conceal security incidents

Data Breach Management

All suspected data breaches shall be investigated promptly.

PDT will assess:

- The impact of the breach.
- The risks to affected individuals.
- Whether notification is required to the Information Commissioner's Office (ICO).
- Whether affected individuals must be informed.

Employees must report incidents immediately to ensure statutory reporting deadlines can be met.

Joiners, Movers and Leavers

Managers must notify ICT support promptly when:

- Staff join the organisation.
- Roles change.
- Individuals leave the organisation.
- Contractors cease engagement.

Access rights must be:

- Created promptly for authorised users.
- Modified when duties change.
- Removed promptly on departure.

All PDT equipment, access devices and credentials must be returned when employment, volunteering or contractual arrangements end.

Data Retention and Secure Disposal

Information shall only be retained for as long as necessary to satisfy:

- Legal or Regulatory requirements

- Funding requirements
- Operational needs

Information that is no longer required must be securely destroyed or deleted.
Equipment containing organisational information must be securely wiped prior to disposal, transfer or re-use.

Monitoring

PDT reserves the right to monitor the use of its systems, equipment and networks where lawful and proportionate to do so.

Monitoring may be undertaken:

- To investigate suspected misconduct.
- To protect organisational assets.
- To identify security threats.
- To meet legal or regulatory obligations.

Users should have no expectation of privacy when using organisational systems beyond applicable legal protections.

Breaches of Policy

All incidents or information pertaining to a potential breach of this policy should be reported to the CEO.

Review of this Policy

This document will be subject to review when any of the following occur:

- Business practices change rendering any aspect of this policy outdated or no longer in line with best practice
- 2 years elapse after approval of the current version.