

**Information, communication**

**and technology (ICT) and Password Policy**

Approved by Board of Trustees on: May 23rd 2023

Lead Staff Member: Jackie Rosenberg

Lead Trustee: Grace Reid

# 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.

# 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

Staff will ensure that all personal passwords held remain strictly personal to that member of staff and are not disclosed in any form. They must not be relayed verbally, written down or otherwise revealed to any other individual, either within or outside the organisation.

If any person has to access information through the use of another person's password in exceptional circumstances, due to absence from work etc. then the password must be changed as soon as is practicable (e.g. upon return to work). In the event that this does not occur, both individuals may be subject to action in accordance with the Disciplinary policy.

## Password management – organisation

Any system capable of using passwords must have the facility enabled. An individual should not use the same password for multiple systems.

Length of password, character constraints and frequency of changes are system dependent and are therefore defined by each system, but as a minimum:

* Passwords should be at least eight characters long and must include a combination of alpha and numeric characters, in any order;
* Passwords should be changed at least every 60 days, and in the event of suspected or actual breaches of security;
* 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 should never be written down

## System access

Access to IT systems 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.

## 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.