pdt paddington development trust

Information, communication and technology (ICT) and Password Policy

Approved by Board of Trustees on: June 26th 2018

Lead Staff Member: Jackie Rosenberg
Lead Trustee: Craig Macdonald

ICT Policy

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".

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.

This policy is also designed to ensure the security of PDT's computer equipment and software and physical property including its premises. It also covers all aspects of the organisation's security or electronic equipment that it is designed to protect, including but not limited to, entry codes, electronic codes in security fobs, electronic keys and alarm systems as well as the organisation's computer equipment and networks.

PDT will afford access to its confidential information to enable employees to carry out their duties, but such confidential information is valuable and loss or misuse of it could cause substantial damage to the organisation.

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.

For the purposes of this policy, computer equipment shall mean any hardware and/or software that uses or comprises electronic or computer code or circuitry, including but not limited to telephones, televisions, CCTV systems, DVD's, video recorders or sound recording equipment where such equipment is capable of being connected to a computer by digital or other interface.

PDT will take steps to use password protection and/or other security means including monitoring to protect its property. Employees are given access to PDT information and property, including its computer equipment, for the purpose of carrying 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 and to report immediately the loss and/or failure of any electronic or other security measure or equipment to their line manager or other appropriate person immediately.

The policy sets out rules in relation to the use of the PDT property.

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 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 recording medium such as a CD, DVD or flash 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 adware of any kind;
- use the organisation's property to:
  - harass;
  - discriminate;
  - bully;
  - defame;
  - Or otherwise act offensively 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 that will be likely to give rise 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.

PASSWORDS AND ELECTRONIC SYSTEMS SECURITY

This policy will ensure the organisation has a consistent, comprehensive and systematic approach to the management of Password Control within the Information Technology systems used.

1. INTRODUCTION

The purpose of this Password Policy is to enable the maintenance of integrity across the Organisation’s Information Systems.

This document describes the rules about password maintenance and the standards for the management of access controls in computer based information systems.

2. PASSWORD DISCLOSURE

2.1 Staff will ensure that all personal passwords held remain strictly personal to that member of staff and are not disclosed in any form.

2.2 They must not be relayed verbally, written down or otherwise revealed to any other individual, either within or outside the Organisation

2.3 If any person has to access information through the use of another person's password, due to absence from work etc. then the password must be immediately changed. In the event that this does not occur both individuals may be subject to action in accordance with the Disciplinary policy

2.4 The wilful or negligent disclosure of confidential information whether written or computerised could be seen as a gross misconduct under the Disciplinary Policy and may lead to dismissal

3. PASSWORD MANAGEMENT

3.1 Any system capable of using passwords must have the facility enabled

3.2 Length of password and characteristics are system dependent and are therefore defined

3.3 Passwords should be at least eight characters long and must include a combination of alpha and numeric characters, in any order.

3.4 Passwords must be unique to the system i.e. not be used for access to other systems

3.5 Passwords must not be shared with or disclosed to anyone

3.6 Frequency of password change may be system dependent and passwords must be changed at the frequency defined by the system.

3.7 If password change is not system dependent the user should be aware that current advice is to select a strong password solely for this usage and then not alter on a regular basis. (see attached Microsoft Guidance).

3.8 Passwords must be changed if security is believed to have been, or actually has been, breached

3.9 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

3.10 Passwords must be something memorable so it doesn't need to be written down.

4. MANAGEMENT

4.1 Access to IT systems will only be given once adequate training has been received and competence levels have been reached, as determined by the trainer

4.2 Where systems are locally implemented and maintained and are not under the control of IT or another organisation, training must be carried out by local management

4.3 In the case of PDA's/laptops and other devices capable of storing or displaying organisational information, (by receiving an email for example) the devices must be protected in line with this policy.

5. REMOVAL OF SYSTEM ACCESS

Should there be any breach of this Policy the Organisation may restrict access to any/all systems

6. BREACH OF POLICY

All incidents or information pertaining to a potential breach of this policy should be reported in accordance with the appropriate incident reporting policy.

7. REVIEW OF THIS DOCUMENT

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

7.1 The adoption of the standards highlights errors and omissions in its content

7.2 When other standards/guidance are suggested which will improve password security and bring it in line with best practice

7.3 2 years elapse after approval of the current version.