IT AND CYBER SECURITY POLICIES AND PROCEDURES FOR

PURBECK YOUTH & COMMUNITY FOUNDATION

Introduction

Purbeck Youth and Community Foundation's (pycf) IT infrastructure consists of several resident laptops and computers, and some portable devices comprising laptops, tablets and smart phones.

The resident computers are housed in one or more small offices within pycf main premises. A wireless router provides 2 independent networks, PYCF Admin and PYCF User Each of which provides internet access.

A paid-for subscription to Microsoft 365 provides each device with email services, data storage facilities "in the cloud", and access to the individual apps which make up the Microsoft Office product (Word, Excel, Powerpoint, Teams etc). Cloud storage may be restricted to the owner of the data, or sharable between designated users so that collaborative working is facilitated.

The cyber security policies and procedures defined in this document are intended to protect the integrity, safety and security of this infrastructure. They have been developed as a result of a detailed risk analysis carried out by pycf staff (including an IT consultant), and with recourse to the advice and recommendations in the document **Cyber Security- Small Business Guide Actions** published by the National Cyber Security Centre (see www.ncsc.gov.uk).

Specifically, pycf cyber security needs to protect and mitigate against the following 3 risks:-

- The risk that pycf's IT infrastructure is rendered dysfunctional to the point that it can no longer be effectively used for its normal working purpose;
- The risk that critical client personal data and records are irretrievably lost or corrupted;
- The risk that such data inadvertently falls into the hands of unscrupulous third-parties.

These risks may materialise because of any of the following hazards:

- pycf equipment (computers, routers etc) develops a hardware fault or fails to operate at all.
- Computer passwords are forgotten;
- Computer passwords are compromised (ie become available to other people who may use them for illicit access). Such "bad actors" may be external to pycf, temporary or occasional visitors to pycf premises, or disgruntled pycf staff.
- WIFI snooper devices are used to capture sensitive data while it is being transmitted over an unencrypted WIFI link.
- Pycf staff inadvertently (without malice) destroy or corrupt client personal data.
- Portable devices are lost or stolen
- Officer-resident computers are stolen.
- Viruses, ransomware or other malware is introduced to one or more pycf computers.

Malware may be introduced by several mechanisms as follows:

- use of an external USB device (flash drive, SD card, USB disk) which has been infected with malware whist being used on other systems;
- opening an email received from an external source which releases malware;
- accessing a suspicious website which releases malware.

Policies and Procedures

Policy

User Access Policy

Pycf policy is to restrict staff access to only those facilities which they need to carry out their role by assigning each staff member or pycf volunteer their own login identity which is password protected. Each user thus has their own email account, and is unable to access emails for other users. Similarly, each user has access to their own area of cloud storage and cannot access other users' storage.

Pycf uses Microsoft Sharepoint to provide shared access to a defined set of cloud-storage data to enable collaborative working. Our policy is to restrict shared access appropriately according to a user's role; for example, trustees and staff.

Pycf also maintains 2 separate LANs, (pycf admin and pycf user) to enforce isolation between staff access and access for other users.

Backup policy

Pycf policy is to store files in the cloud storage provided by Microsoft 365 and for this reason scheduled backup to external Devices (such as an external USB drive) is not required.

Password Policy

In general, users will need to use two passwords – one to login to the laptop or desktop PC or tablet which they intend to use, and a second password to login to Microsoft Office 365.

Our password policy manages each type of password differently.as follows:

Device passwords – Passwords for staff and volunteers give access to the device as ordinary users (ie without admin privileges) so that users cannot install third-party applications or modify the configuration of the device. Staff may change their password as they wish and are encouraged, but not mandated, to do so regularly.

In addition, each device has an admin loginid whose password is known only to authorised personnel (the IT manager and the Office Manager. If a user forgets his password, the admin login can be used to reset it. The admin password is recorded in a book kept under lock and key under the control of the Office Manager. This guards against forgetting the admin password.

Microsoft 365 passwords – These are allocated centrally using the Admin@pycf.org.uk Microsoft 365 login for which only the IT Manager and our support organisation Newburgh Networks have access. This password is recorded in a book kept under lock and key under the control of the Office Manager. This guards against forgetting the password. Some user logins provide access to more crucial facilities than others. It is pycf policy that the password for each of the following logins are changed every month. These crucial logins are:

office@pycf.org.uk

marklapper@pycf.org.uk

joycespiller@pycf.org.uk

miamurray@pycf.org.uk

hollymaygladwin@pycf.org.uk.

Policy for External USB Devices

Use of staff members' or visitors' personal external USB devices for the purposes of transferring data to pycf equipment is strictly forbidden. One USB stick, owned by pycf and kept under lock and key under the control of the Office Manager, is available for use and can be booked for use by staff.

Physical Security

Pycf's premises are hired by other organisations and many types of visitor attend. It is pycf policy that the pycf office is locked whenever it is unattended.

IT Support

First line support is provided by a (retired) volunteer with many years' experience in the software industry. We also employ a commercial firm, Newburgh Networks, to provide second-line support on a case-by-case basis.

Phishing Awareness and Reporting

Pycf has undertaken the NCSC (National Cyber Security Centre) free cyber security check - https://checkcybersecurity.service.ncsc.gov.uk/. This checks the security of our email, IP address and website and web browser. Actions have been taken to make everything compliant.

Pycf has signed up to receive scam alerts from the police via its actionfraud website www.actionfraudalert.co.uk and has registered with them to report any suspicious activity.

Staff awareness of phishing forms part of our staff cyber training (see below).

Internet Access "on the Road"

Pycf has an outreach vehicle and regularly needs online access "on the road". WIFI hot-spots (of which there are many) do allow this, but transmission over WIFI is not encrypted and can be "snooped" to access data in transmission. It is pycf policy to avoid using external WIFI hot-spots where possible by either ensuring necessary files are stored temporarily on the portable device or by using the tethering facility on a smartphone.

Technical

Security Configuration of all devices

Pycf policy is that all pycf computers and tablets are configured in a standard way by the IT Manager and that ordinary users do not have administration rights to alter this configuration in any significant way.

For example, for a Windows laptop, this means that apart from the applications which are loaded with Windows, only a defined set of extra applications are installed when the device is configured, and users do not have the ability to install other applications.

All devices are configured to require the use of a password.

Google Chrome is configured as the default browser.

The firewall is switched on and Windows Defender (delivered with the OS) is pycf's chosen anti-virus software. The configuration ensures that Windows Defender is switched on.

Similar actions, with slight differences, apply to the configuration of tablets and Apple computers.

We do not permit the use of staff's personal external devices (flash drives, SD cards etc) and pycf has only a single flash drive whose use is strictly controlled. We therefore do not need to block physical access to physical ports.

Our password policy (see above) means that we do not need to use a password manager. If a user forgets his device password, he can use the built-in security questions to reset it or request the IT Manager to reset it for him using the admin login. If a user forgets his Microsoft 365 password, the IT Manager can reset it by logging in as admin@pycf.org.uk

Multi-factor Authentication

Pycf's Microsoft 365 facility is set up so that by default all logins require 2-factor authentication. This is to prevent a "bad actor" from signing into an account to which he has no legitimate access even if he has learned its password, because the "second factor" in the authorisation involves sending a text or a call to a smart phone (which is not in possession of the bad actor), or an email to an **external** email address.

(Note that the office@pycf.org login does not have 2-factor authentication since it may be used by several staff members).

Tracking Applications

Facilities exist ("Find My Device", "Find My Phone") to track the location of a lost or stolen device, and if necessary, remotely lock it so that it cannot be nefariously used. Pycf configures its devices so that this facility is always enabled at the device.

Software Updates

All devices are configured so that their Operating Systems are set to update automatically and install as soon as they are released.

Encryption

If a laptop is stolen by someone who wishes to steal the data on its hard disk, they can circumvent the password protection by removing the disk from the laptop, plugging in a SATA/USB converter and using the disk as an external disk on their own computer, unless the disk has been encrypted. Windows 10 Pro and Windows 11 Pro provide have a built in facility Bitlocker which will encrypt the disk using an encryption key (a "Trusted Platform Module" -TPM) stored in a chip on the motherboard.

Pycf configures laptops so that Bitlocker is enabled, to take advantage of encryption for new laptops with a TPM chip. We recognise that some of our current laptops pre-date the introduction of onboard TPMs so that disk data is not encrypted.

Training and Awareness

Cyber Security Training Plan

Pycf recognises that for a cyber security policy to be effective, all users must be familiar with the policies and procedures. This will require some training. The pycf cyber security training plan requires staff to:

- Read this document to understand the need for security measures and be familiar with pycf policies;
- Read the pycf User Manual for using Sharepoint and Microsoft 365;
- Ask for specific tuition from the pycf IT Manager when necessary;.
- Learn how to recognise scam emails or phishing websites by completing the online study “Top Tips for Staff” – use the link below:

  https://www.ncsc.gov.uk/training/v4/Top+tips/Web+package/content/index.html#/
- Report any suspicious emails or websites to the IT Manager or Office Manager.

Bob Newnham 1/12/2023