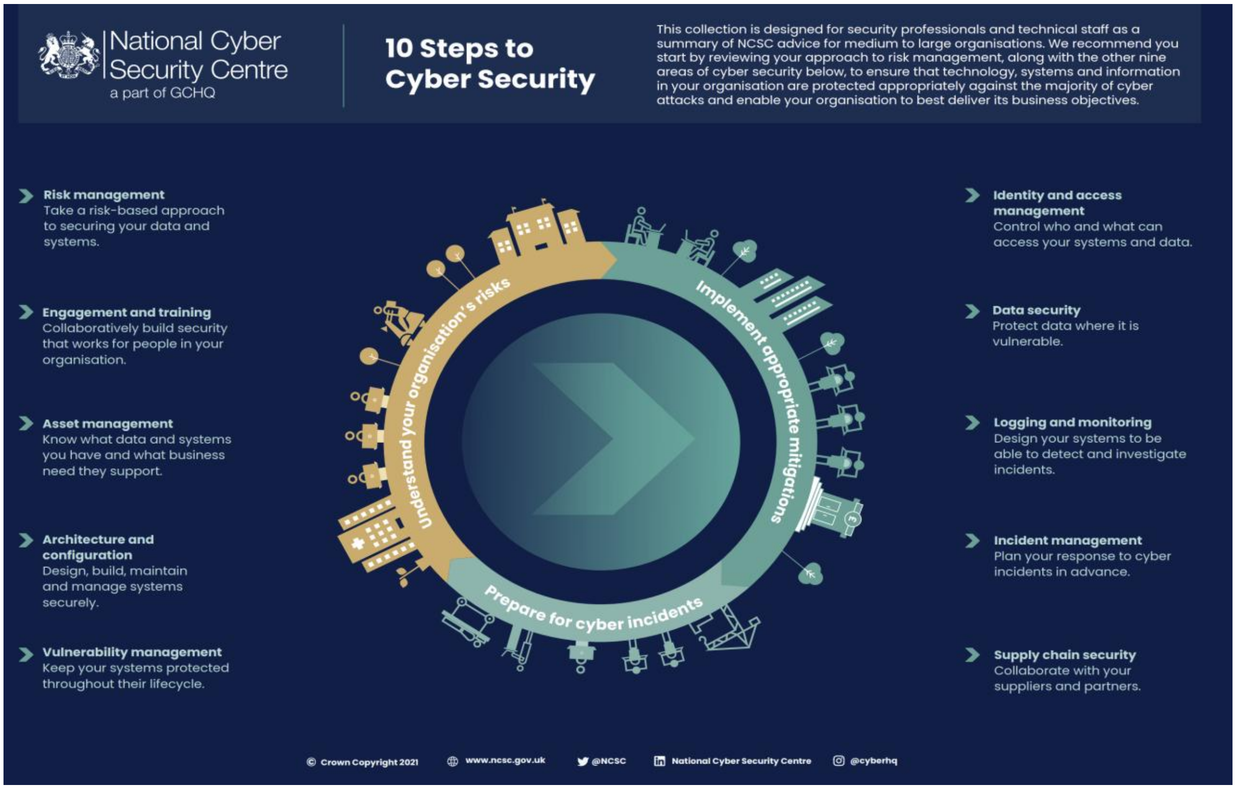
FIRSDOWN PARISH COUNCIL
Mrs AC Purves FSLCC, Parish Council Clerk
“Cranbourne”, White Way, Pitton, Salisbury, Wilts, SP5 1DT
Tel: 07598 054675
https://www.firsdown-pc.gov.uk
e-mail: clerk@firsdown-pc.gov.uk

Firsdown Parish Council Cyber Security Policy

Introduction

Cyber security covers IT hardware, software, data and information. The risk of data theft, scams, and security breaches can have a detrimental impact on IT systems, information and reputation. As a result, Firsdown Parish Council (FPC) has created this policy to outline the security measures to put in place to ensure IT systems and information remains secure and protected.

The government’s National Cyber Security Centre has published the following steps to ensure good cyber security practices.



National Cyber Security Centre
a part of GCHQ

10 Steps to Cyber Security

This collection is designed for security professionals and technical staff as a summary of NCSC advice for medium to large organisations. We recommend you start by reviewing your approach to risk management, along with the other nine areas of cyber security below, to ensure that technology, systems and information in your organisation are protected appropriately against the majority of cyber attacks and enable your organisation to best deliver its business objectives.

- **Risk management** Take a risk-based approach to securing your data and systems.
- **Engagement and training** Collaboratively build security that works for people in your organisation.
- **Asset management** Know what data and systems you have and what business need they support.
- **Architecture and configuration** Design, build, maintain and manage systems securely.
- **Vulnerability management** Keep your systems protected throughout their lifecycle.
- **Identity and access management** Control who and what can access your systems and data.
- **Data security** Protect data where it is vulnerable.
- **Logging and monitoring** Design your systems to be able to detect and investigate incidents.
- **Incident management** Plan your response to cyber incidents in advance.
- **Supply chain security** Collaborate with your suppliers and partners.

Understand your organisation's risks
Implement appropriate mitigations
Prepare for cyber incidents

© Crown Copyright 2021 www.ncsc.gov.uk @NCSC National Cyber Security Centre @cyberhq https://www.ncsc.gov.uk/files/2021-10-steps-to-cyber-security-infographic.pdf

The Firsdown Parish Council Cyber Security Policy has been based on the Cyber Essentials Requirements for IT Infrastructure v 3.2

https://www.ncsc.gov.uk/files/cyber-essentials-requirements-for-it-infrastructure-v3-2.pdf

Purpose

The purpose of this policy is to:

- Protect FPC data and infrastructure
- Outline the protocols and guidelines that govern cyber security measures
- Define the rules for FPC IT assets

The following documents should also be read in conjunction with this policy:

- FPC GDPR Document retention and disposal policy
- FPC IT Policy

Confidential Data

FPC defines "confidential data" as:

1. Unreleased and classified financial information
2. Customer and supplier information
3. Employees' passwords and personal information
4. Council contracts and legal records

Scope

This policy applies to all FPC councilors, officers, remote workers, permanent employees, or any individuals with access to the company's electronic systems, information, software, and/or hardware. The following aspects of IT equipment and software are also in scope of this policy.

Hardware

The FPC laptop and mobile phone as detailed in the FPC IT Policy are in scope.
The domestic broadband router used by the clerk is *out of scope.* Cyber protection is provided by the ISP software firewall on the device.

FPC does not operate any IT server equipment or any networked hardware. Bring Your Own Devices (BYOD) are not supported by FPC.

Cloud Services

Data or services hosted on Cloud services are in scope. The applicant is always responsible for ensuring all controls are implemented, but some maybe provided by the

Cloud service provider.

FPC only uses Software as a Service (SaaS). Examples are Microsoft 365, email services and website hosting.

Cloud services such as Platform as a Service (PaaS) and Infrastructure as a Service (IaaS) are not used by FPC.

FPC does not provide any software or web applications that are available to 3rd parties. The FPC website is hosted by a 3rd party.

Responsibility for controls is as follows:

Firewalls	Cloud provider
Secure configuration	Cloud provider and FPC
Security Update Management	Cloud provider
User access control	FPC
Malware protection	Cloud provider

Web applications

Publicly available web applications are in scope by default. Examples are Facebook or Office 365. Ensuring that the latest version is in use and all security updates are installed is the best protection against cyber-attack.

Control measures

1. Firewalls

Applies to Routers, laptops/computers, SaaS

Aim to ensure that only secure and necessary network services can be accessed from the internet.

Users must:

- change default administrative passwords to a strong and unique password (see password-based authentication) – or disable remote administrative access entirely
- prevent access to the administrative interface (used to manage firewall configuration) from the internet
- block unauthenticated inbound connections by default
- ensure inbound firewall rules are approved
- Make sure you use a software firewall (Virtual Private Network software application such as NordVPN or Surfshark) on devices which are used on untrusted networks, such as public wifi hotspots

2. Secure configuration

Applies to Routers, laptops/computers, SaaS, mobile phones

Aim to ensure that devices and software are properly configured to reduce vulnerabilities and provide only the services required by their role.

Users must:

- change any default or guessable account passwords (see password-based authentication)
- remove or disable unnecessary software (including applications, system utilities and network services)
- disable any auto-run feature which allows file execution without user authorisation (such as when they are downloaded)
- ensure users are authenticated before allowing them access to organisational data or services

3. Security update management

Applies to Routers, laptops/computers, SaaS, mobile phones

Aim to ensure that devices and software have the latest updates to prevent them being vulnerable.

You must make sure that all software in scope is kept up to date. All software on in-scope devices must:

- be licensed and supported
- removed from devices when it becomes unsupported or removed from scope by using defined sub-set that prevents all traffic to / from the internet
- have automatic updates enabled where possible
- be updated, including vulnerability fixes, within 14 days of their release

4. User access control

Applies to Routers, laptops/computers, SaaS, mobile phones

Aim To ensure that user accounts:
- are assigned to authorised individuals only
- provide access to only those applications, computers and networks the user needs to carry out their role

The following must be carried out:

- have in place a process to create and approve user accounts
- authenticate users with unique credentials before granting access to applications or devices (see password-based authentication)
- remove or disable user accounts when they're no longer required (for example, when a user leaves the organisation or after a defined period of account inactivity)
- implement MFA (Multi Factor Authorisation), where available – authentication to cloud services must always use MFA
- use separate accounts to perform administrative activities only (no emailing, web browsing or other standard user activities that may expose administrative privileges to avoidable risks)
- remove or disable special access privileges when no longer required (when a member of staff changes role, for example)
- ensure devices are locked by PINs or passwords when not attended.
- Devices must be powered down and physically secured – laptops behind lock and key, when not in use

Password-based authentication

All user accounts require the user to authenticate. Passwords must conform to the following:

- Between 8 and 12 characters which should include capitals, numeric and special characters
- Unique and random – not pets name or qwerty123 for example
- Use a different password for each application
- The use of a password manager application is recommended
- Passwords must not be disclosed or shared with other people or colleagues
- Organisations such as banks or HMRC will never telephone or email requesting password details
- By aware of your device screen being overlooked if used in public places, ensure password details or other confidential data cannot be seen by 3rd parties.

Passwords must be changed promptly if you know or suspect a password or account has been compromised.

Multi-Factor Authorisation

Where provided this must be used. Cloud based services must make use of a password and MFA.

Connection to wifi networks

Only connect devices to secure and trusted wifi networks – padlock symbol and requiring a password.

Public wifi networks often meet this criteria, but consider the use of a Virtual Private Network software application such as NordVPN or Surfshark to provide an additional level of security.

5. Malware Protection

Applies to Routers, laptops/computers, SaaS, mobile phones

Aim to restrict execution of known malware and untrusted software, from causing damage or accessing data.

If a system is infected, your organisation is likely to suffer from problems like malfunctioning systems, data loss, or onward infection that goes unseen until it causes harm elsewhere.

You can largely avoid the potential for harm by:

- preventing malware from being delivered to devices
- preventing malware from running on devices

Anti-malware software must be installed and configured correctly – e.g. Microsoft Windows Defender.

The anti-malware software used to protect your device must be configured to:

- be updated in line with vendor recommendations
- prevent malware from running
- prevent the execution of malicious code
- prevent connections to malicious websites over the internet

A common method for malware to be delivered to devices is via email. Emails can contain harmful executable files or internet links to sites that contain malware. Good email security is essential to prevent infection via malware.

Users must:

1. Verify the legitimacy of each email, including the email address and sender name
2. Avoid opening suspicious emails, attachments, and clicking on links
3. Look for any significant grammatical errors
4. Avoid clickbait titles and links
5. Contact the FPC Clerk regarding any suspicious emails
6. Organisations such as banks and HMRC will never send emails with embedded links. Such emails are likely to be harmful and contain links to malware links
7. Only download software from reputable sites such as Microsoft or Google Play store
8. Be wary of websites that are http and not https, if in doubt via the site security certificate

6. Data backups

Regular back-ups of data to another device or the Cloud means that there will be a recent version of information to allow recovery if data is lost or stolen.

Consider using automated back up so that users do not need to remember to do so. Microsoft Windows/Office 365 provides such as facility.

If using a USB or external hard drive for a manual back up, disconnect these devices once the backup is complete and store securely so that the backup device cannot be accessed by unauthorised individuals.

Adopted November 2025

Review date: March 2029, unless statutory changes require.