Uffington
Parish Council

Document	:	**Bring Your Own Device (BYOD)**
Date created	:	June 2025
Source document	:	Various
Created by	:	D Hatton (Clerk)
Date adopted	:	July 2025
Date of next review	:	July 2027

Uffington Parish Council Bring Your Own Device (BYOD) Policy

The following definitions are used throughout this policy.

- '**Devices**' – computers (all types), tablets, smartphones and storage devices
- '**Parish Council Business**' – is any activity undertaken in the role of member or employee of Uffington Parish Council.
- '**Personal Data**' – as defined in Article 4(1) of the General Data Protection Regulations UK, "any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, identification number, location data, online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person".
- '**Personally owned**' – ownership of a device by a person or legal entity which is NOT Uffington Parish Council.

Introduction

The purpose of this policy is to ensure as far as possible that personally owned devices used by members and staff to conduct Uffington Parish Council business are used in a manner that protects personal data as required by statute.

Risks

The following risks have been identified as inherent in the use of personally owned devices when conducting Parish Council business:

Event/Action	Risk
Inadequate or lack of appropriate security measures used to control device access.	Personal data may be accessible to third parties.
Device used in an unsecure manner.	Device could become affected by Malware which could result in personal data being accessed by third parties.
Device lost or stolen.	Personal data might be accessible to third parties.

Device sold or given away.	Personal data might be accessible to third parties if not sufficiently restored to factory setting and data transferred/cleared.
Member ceases to be a member of the Parish Council. Clerk ceases to be employed by the Parish Council.	Personal data may remain accessible and could be used for unauthorised purposed or disclosed to third parties.

Access to devices

Devices used for Parish Council business should be able to be secured by a password or biometric access control, such as fingerprint recognition.

Password should comply with the following rules:

1) Should not be written down.
2) Should not be saved for automatic access.
3) Should not be disclosed or shared to any other person.
4) Should be changed on a regular basis.
5) Should comprise of a mix of letters, numbers and symbols.

Devices should be configured to automatically lock if left idle.

Safe usage of devices

Devices should have appropriate levels of up-to-date anti-virus and anti-malware software.

Home networks should be password protected.

Care should be taken if using an 'open' network.

Retention and use of Personal Data

Personal data received for the purposes of Parish Council business must be permanently deleted from the device once the Parish Council business is completed.

Personal data must NOT be retained for any other purpose than that originally intended unless:
1) express permission has been obtained for the Parish Council to retain the data.

2) The Parish Council is required by law to retain the personal data.

Personal data must NOT be shared with any other person or organisation without the express permission of the data subject (e.g. Identity of the data subject in communication with a District Council representative should be redacted unless permission is given).

Lost or stolen devices

In the event of a device being lost or stolen, or is suspected of being lost or stolen, the Clerk and Chair of the Parish Council must be informed. The Parish Council will work with the owner of the device to identify and minimise any potential data risk and take any appropriate action, including reporting of any breach to the ICO if necessary.

Repair of devices

The repair and maintenance of the device remains the sole responsibility of the owner.

Transfer or disposal of a device used for Parish Council business

If at any point the device is disposed of or transferred to a new owner, all data relating to Parish Council business must be removed in a manner which prevents recovery. All access facilities to Parish Council business related data must be removed from the device.

Leaving the Parish Council

If a member leaves the Parish Council or the Clerk ceases to be an employee of the Parish Council for any reason the following actions must take place:

1) All personal data received while conducting Parish Council business must be permanently deleted including any back up copies of data held.
2) All access facilities to Parish Council business must be permanently deleted.
3) Any hard copy of personal data received while conducting Parish Councils business must be securely disposed of.