WINKLEIGH PARISH COUNCIL
USE OF OWN DEVICE POLICY

This procedure is a document that sets out Winkleigh Parish Councils approved and agreed practices. Any deviation must be by resolution of the full Council.

DOCUMENT NO:	WPCP/34
Lead author(s):	
Developed by:	Winkleigh Parish Council
Approved by:	Resolution RR061/04/2019
Ratified/Adopted	24/04/2019
Approval date:	24/04/2019
Minutes:	44.3.19
Review date:	APCM May 2020
Version no:	1

Version Control And Revisions:

Version	Point	Description of Change	Date
			/
			/

THIS IS A CONTROLLED DOCUMENT

Whilst this document may be printed, the electronic version maintained on the Winkleigh Parish Council website is the controlled copy. Any printed copies of this document are not controlled.

WINKLEIGH PARISH COUNCIL

Use Your Own Device (UYOD) Policy for Councillors

INTRODUCTION

Winkleigh Parish Council has purchased a Linx 10-inch tablet, with detachable keyboard, for the use of each individual Council Member, with Microsoft Office 365 (Home) installed using Microsoft encryption and running BT Symantec anti-virus protection,

Any Council Member who does not wish to use this Council provided device may use their own personal device provided they comply with this policy and the use has been approved by Winkleigh Parish Council.

This policy is supported by Winkleigh Parish Councils

- Privacy Statement,
- Data Retention Policy
- Data Protection Policy
- Information Protection Policy
- Information Security Policy
- Computer and Telephone Security Policy
- Removable Media Policy
- Social Media Policy
- Risk Management Policy

LEGAL REQUIREMENTS

Using your own device raises several data protection concerns since the device is owned by the user rather than the data controller (Winkleigh Parish Council)

It is crucial that the data controller ensures that all processing for personal data which is under his control remains in compliance with the General Data Protection Regulations 2018.

The Data Protection Act states *"The seventh principle says: appropriate technical and organisational measures shall be taken against accidental loss or destruction of, or damage to, personal data. It means you must have appropriate security in place to prevent the personal data you hold from being accidently or deliberately compromised. This is relevant if personal data is being processed on devices which you may not have direct control over".*

Permitting a range of devices to process personal data held by Winkleigh Parish Council gives rise to several questions a data controller must answer in order to continue to comply with its data protection obligations. **It is important to remember that the data controller must remain in control of the personal data for which they are responsible, regardless of the ownership of the device used to carry out the processing.**

The Data Protection Act 1998 (DPA) requires that the data controller must take appropriate technical and organisational measures against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data

Where personal data is stored on a device it will be important to consider the safe and secure deletion of the data throughout the lifecycle of the device, and particularly if the device is to be sold or transferred to a third-party.

Inappropriate use of personally-owned devices or unsatisfactory procedures could involve a breach of the Code of Conduct, the Data Protection Act 1998, and the General Data Protection Regulation ("GDPR").

There are, therefore, several matters which should be considered which allow personally-owned devices to be used for purposes related to Parish Council matters and practices:

(a) If the device is lost or stolen, confidential information might be accessible to third parties. This could lead to a fine being imposed by the ICO.

(b) If the member ceases to be a councillor, confidential information will, unless it is deleted, remain accessible to the ex-member and could be used for unauthorised purposes or disclosed to third parties. The continuing accessibility of this data would be contrary to the GDPR (for example Articles 5 and 24) and could result in a fine being imposed (even if no personal data is illegitimately disclosed).

(c) If a personally owned device is used in an insecure manner, and/or is used by family members, the device could be affected by malware/spyware which could lead to a fine being imposed by the ICO.

For these reasons and in order to comply with GDPR Article 24.2, Winkleigh Parish Council have written a Use Your Own Device policy which sets out the conditions under which personally-owned devices may be used by members for Parish Council business.

Non-compliance of this policy exposes both councillors and the council to risks. If a breach of this policy occurs the council may discipline councillors in line with the council's Disciplinary Procedure, Data Protection Policy and Code of Conduct.

Guidance will also be offered to councillors to support them in complying with this policy

Any Member wishing to apply to the Council to use their own device in accordance with the UYOD Policy must complete the UYOD User Agreement at Appendix A to this policy

WINKLEIGH PARISH COUNCIL

[DRAFT] Policy on personally-owned devices used by members

1) The purpose of this policy is to ensure so far as possible that personally-owned devices used by members are used in a manner which protects confidentiality, personal data and the confidentiality of council communications. This policy supplements the council's Computer and Telephone Security policy.

2) All members will be made aware, in accordance with the following policies, that the council reserve the right to access personally-owned devices for the purpose of ensuring the effectiveness of this policy, in the event of termination of membership or if it is suspected that there has been a breach of this policy or any other Council policy.

Privacy Statement,
Data Retention Policy
Data Protection Policy
Information Protection Policy
Information Security Policy
Computer and Telephone Security Policy
Removable Media Policy
Social Media Policy
Risk Management Policy

3) Members may apply to the Parish Council to use their own personal device rather than the Parish Council issued Linx Tablet.

4) With the approval of Winkleigh Parish Council, members may use personally-owned computers, smartphones, tablet computers and removable media devices ("approved devices") for purposes related to council business.

5) The Parish Clerk will maintain a list of approved devices setting out

- **(a)** the type and model of each device,
- **(b)** the date on which the device was encrypted, the date the encryption renews/ends, the provider of the encryption
- **(c)** the name of the user of that device.
- **(d)** A signed copy of the UYOD Agreement for each Member.

6) Individual Councillors are responsible for their approved device at all times. The Council is not responsible for the loss, theft of, or damage to the approved device or storage media on the device (e.g. removable memory card) howsoever caused.

7) The Council takes no responsibility for supporting councillor's own approved devices; nor has the council a responsibility for conducting annual PAT testing of personally-owned devices.

8) Approved personal devices must be secured by a password or a biometric access control (e.g. fingerprint scanner or facial recognition). Passwords should be sufficiently memorable that the user can avoid writing them down, but not obvious or easily guessed.

9) Approved devices must be configured so that they are automatically locked after being left idle for a set time of no more than 5 minutes in the case of mobile devices and 10 minutes in the case of desktop computers.

10) Approved devices must be encrypted in a manner approved by the Clerk as the Data Processor.

11) Councillors must not send council information to or from their personal email accounts.

12) Care must be taken to avoid using approved personal devices in a manner which could pose a risk to confidentiality, whether by clicking on links in suspicious emails, accessing potentially harmful websites, using potentially harmful application software, using wi-fi facilities in public places (e.g. coffee shops or airports), or otherwise. Some apps for smartphones and tablets may be capable of accessing sensitive information.

13) If an approved device is lost or stolen, or is suspected of having been lost or stolen, the Clerk, as Data Processor, must be informed as soon as possible so that such steps as may be appropriate may be taken to protect the council members email account.

14) Passwords to approved devices must be kept confidential and must not be shared with family members or third parties.

15) Approved devices must not be used/shared by family members or other persons unless the device has been configured for separate profiles and logins to ensure restricted access to files.

16) Approved anti-virus software must be used on approved computers and must be kept up to date at the members own expense. The latest security updates to the operating system and browser software must be routinely installed on approved computers.

17) Winkleigh Parish Council has paid for enough subscriptions for each member to install BT Symantec on personal computers, free of charge. This will conflict with any existing anti-virus software already installed on the computer. If a member using an approved personal computer, wishes to have BT Symantec installed on the personal computer approved for Parish Council business, then the Clerk will personally install the licence to that device. (The Clerk can remotely remove the device if a member leaves the council or wishes to use an alternative anti-virus software programme at their own expense)

18) Winkleigh Parish Council has subscribed to Microsoft Office 365 (Home) for each Councillor. If a member wishes this licence to be installed on a personal approved device, the clerk will carry out the installation. (The clerk can remotely close the Microsoft account in the event that the council member leaves the council)

19) Home Wi-Fi networks must be encrypted. Caution must be exercised when using public Wi-Fi networks as public Wi-Fi networks may not be secure.

20) Except in the case of an emergency, members must not copy data from approved devices to other personally-owned devices. The data must be securely deleted when the emergency has passed.

21) Councillors may view council information via their mobile devices but must not store the information on their devices, or on cloud servers linked to their mobile devices. In some cases, it may be necessary for councillors to download council information to their mobile devices in order to view it (for example, to view an email attachment). Members must delete this information from their devices as soon as they have finished viewing it. Where personal or sensitive data is used in this way devices all files MUST be encrypted. Council information accessed through these services is confidential, in particular information about Members or the clerk.

22) Where such devices are used to process data of a personal or sensitive nature appropriate encryption of files or devices must be used. All such data should be deleted from mobile devices as soon as work has been completed. The clerk will retain master copies of all parish council business in accordance with the Council's Data Retention Policy if a document/email has been deleted.

23) Appropriate cloud storage services may be used with the permission of the Clerk, as Data Processor Officer. Services which do not encrypt data before the data is uploaded (for example Dropbox, Box and SugarSync) will not be approved. Other cloud storage services which encrypt data before it is uploaded, may be approved.

24) If an approved device needs to be repaired, appropriate steps must be taken to ensure that confidential information cannot be seen or copied by the repairer. The clerk should be consulted prior to any repair being carried out by any third parties.

25) In the event that an approved device needs to be disposed of, confidential material must be destroyed or wiped using a recognised method to put the data beyond recovery, to the satisfaction of The Data Controller. Merely deleting the files, single-pass overwriting, or reformatting the disk is insufficient.

26) In the event of a member leaving the council, appropriate steps must be taken to the satisfaction of the Data Processor to remove the members email account and other data belonging to the Parish Council, from approved devices and cloud storage services used by that member. The date on which those steps are taken and the date on which those steps are approved by the Data Processor must be recorded in the list of approved devices.

Winkleigh Parish Council

Use Your Own Device (UYOD) User Agreement

THIS AGREEMENT is dated ……..……is made **BETWEEN**:

Winkleigh Parish Council
and

……, A Parish Councillor of Winkleigh Parish Council

WHEREAS:

1) The WPC has approved the use of your personal device, namely

……..……(MAKE/MODEL) in relation to Parish Council business.

This device is encrypted by ……

2) In reliance upon approval of the use of your personal device, you have agreed to accept the engagement on the terms and conditions of this Agreement and the Use Your Own Device Policy.

IT IS HEREBY AGREED as follows:

1. Definitions and Interpretations

1.1. In this Agreement where mentioned the following mean:

"Agreement"	The binding contract between Winkleigh Parish Council and You.
"Commencement Date"	Means the date on which this Agreement comes into authority.
"The Device"	Personal desktop computer, laptop, notebook, tablet, Mobile Telephone.
"the Organisation"	Winkleigh Parish Council
"Councillor"	A person elected or co-opted as a member of the Winkleigh Parish Council
"Termination Date"	Means at the end of Membership as a Councillor to Winkleigh Parish Councillor

I have read, understood and agree to abide by the Winkleigh Parish Council Use Your Own Device Policy and User Agreement

To be Completed by Council Member

My Approved Personal Device is encrypted via……..

I DO/DONOT wish the Clerk to install Microsoft Office 365 (Home) on my approved personal device

I DO/DONOT wish the Clerk to install BT Symantec Anti-Virus Protection on my approved personal device

The organisation - Winkleigh Parish Council	
Name	Mr Alan Mathewman
Position	Proper Officer/Clerk/RFO
Signature	
Date	

The Councillor	
Name	
Signature	
Date	

WPC Completion only

Microsoft Office 365 Licence Ref ……

Installation Date…….. by ……..

Removal Date…….. By ……..

BT Symantec Anti-Virus device protection Licence Ref ……

Installation Date…….. by ……..

Removal Date…….. By ……..