



Wheatley Parish Council's IT Policy (Councillors) **Draft** : (for consideration 02.09.2024)

1. Introduction

Wheatley Parish Council (WPC) appreciates that more and more council business and communications utilise IT equipment and applications. WPC have engaged with preferred suppliers to provide systems and support to ensure the IT needs of WPC's councillors are met.

2. Scope of document

The Council makes use of IT systems, for data storage, communications and as a source of information. This policy is intended to:

- reduce barriers to councillor engagement and communication
- prevent inappropriate use of computer equipment (such as extended personal use or for accessing and circulating pornographic, racist, sexist or defamatory material that may cause harm to individuals or organisations)
- protect confidential, personal or commercially sensitive data
- protect the Council from the risk of financial loss, loss of reputation or libel
- prevent the introduction of viruses
- prevent the use of unlicensed software
- ensure that Council property is properly looked after
- monitor the use of computer facilities to ensure compliance with internal policies and rules and to detect abuse
- reduce barriers to councillor engagement and communication

3. Access to software for WPC business

- a) Access should be maintained in accordance with WPC policies and procedures with efforts made to protect software and access from misuse.
- b) Passwords/PINS or other authentication credentials should not be disclosed to anyone else. Any access issues should be reported to WPC's IT supplier.
- c) Passwords/PINS or other authentication credentials should be changed immediately if you believe it may have been compromised
- d) Any software defects or malfunctions should be brought to the attention of the Clerk and the council's IT provider.
- e) Access to WPC accounts will cease after you are no longer a councillor.
- f) You should never solicit, download inappropriate material from the internet or email, nor use it for online gambling, transmitting pornography, copyright information and/or software material, posting confidential items including council business, other councillors, council staff or members of the public.

- g) if you are using your own device to connect with your WPC account or to transfer data between the laptop/PC and any of the Council's computers you must ensure that you have obtained prior consent, comply with instructions and ensure that any data downloaded or uploaded is free from viruses.
- h) In some instances, remote monitoring of website/emails will be monitored, but only in extreme circumstances of suspicious or illegal behaviour. This may only be carried out under the supervision of the Clerk and will follow data protection legislation

4. WPC financial support for devices

At the time of writing this policy, many WPC councillors were happy to continue using their own devices to access their WPC accounts. However, to ensure no councillor is disadvantaged from this approach WPC have agreed to consider requests for WPC funded devices. Each application should be made to the Clerk and reviewed by the Finance/Staffing Committee.

5. Principles of use of WPC issued devices

All hardware and software issued to Councillors remains the property of the WPC. When using such equipment:

- a) The device should be operated in accordance with WPC policies and procedures and make every effort to protect both hardware and software from misuse/damage.
- b) The device will be set up with a password/code or other security measures. Any access issues should be reported to WPC's IT supplier.
- c) Your device will be insured by WPC against loss or damage within the UK, with the expectation that you take measures to ensure the safety and security of the device. Any loss or damage must be reported immediately to the Clerk. If taken outside of the UK, you must ensure the device is covered by your own insurance policy.
- d) Only you are authorised to use the device, it should not be loaned to family members of friends.
- e) You should never solicit, download inappropriate material from the internet or email, nor use it for online gambling, transmitting pornography, copyright information and/or software material, posting confidential items including council business, other councillors, council staff or members of the public.
- f) If you choose to download an app, please use a personal account. Any apps downloaded should be appropriate and in line with WPC policies
- g) Any issues should be reported to WPC IT providers.
- h) In some instances, remote monitoring of website/emails will be monitored, but only in extreme circumstances of suspicious or illegal behaviour. This may only be carried out under the supervision of the Clerk and will follow data protection legislation.
- i) Your device should be returned back to the council upon request, or at the end of your councillor tenure.

6. Breach of access or devices

Breach of this policy will be regarded as an offence/ and may be reported to the Full Council for consideration of further action required.

Anyone who considers that there has been a breach of this policy in relation to personal information about them held by the Council should raise the matter via the Council's formal grievance procedure.

<p>Date of policy: 11.07.2024 Approving committee: Full Council Reviewing Committee: Staffing Committee Date of committee meeting: 02.10.2024 Policy version reference: N/A Supersedes: N/A Policy effective from: 03.10.2024 Date for next review: 2026.</p>
