IT Code of Practice for Members

1. Introduction

Oswestry Town Council has agreed to support elected Members in their role by providing laptops recognising that they increasingly rely on the use of IT equipment and services to enable them to perform their duties. Whilst the aim is to provide facilities for Members to use freely in pursuit of their role, there are, however, management and legal issues which should be borne in mind to ensure the effective and appropriate use of IT. This Code of Practice is intended to inform all Members who have use of Council computer facilities what is considered acceptable or unacceptable use.

2. Ownership

The equipment and software supplied by Oswestry Town Council will remain the property of the Council. If membership of the Council ceases, the supplied equipment and software must be returned in full working order.

3. Use of Council IT Equipment and Services

3.1 Personal use of Council IT equipment and services is permitted provided it does not violate this Code of Practice and does not impede or conflict with Council business. In any event, such equipment shall not be used for election purposes.

3.2 A Member should not use Council equipment and software for political purposes unless it could reasonably be regarded as likely to facilitate, or be conducive to, the discharge of the functions of the council or of the office to which a Member has been elected or appointed.

3.3 Any private usage, or private data held on equipment, is at a Member's discretion. The Council accepts no liability for any consequences (including financial or other loss) which may arise through the private use of equipment and software provided.

3.4 The Council's approved software packages (limited access to Microsoft Office) will be loaded on all equipment as appropriate Members should be

aware that they must not consciously load any unauthorised or unlicensed software, shareware or software obtained from the internet.

3.5 Private hardware must not be connected to the Council's computer unless the approval of the Town Clerk is granted. If in doubt Members should consult with the Town Clerk.

The Town Council will be indemnified by the Member for the costs of putting problems right should they occur, and its IT provider will not support private hardware. The Council may occasionally require verification of license agreement or original disks associated with the hardware as part of any audits carried out.

3.6 Any software or data files, including word processed documents and spreadsheets, must be checked for viruses before being loaded onto equipment, or transmitted to colleagues, or the Council. The standard set-up for a machine provided by the Council will, by default, automatically carry out a virus check.

4. Internet & E-mail

4.1 E-mail is a common means by which the Council, Members and officers communicate. E-mail should be treated like any other form of communication and the same principles should apply. The Council will monitor the use of internet and e-mail for compliance with all Council policies.

4.2 The internet is not secure, and e-mail should not be used for the transmission of sensitive or confidential information unless the information is protected, such as via the use of encryption.

4.3 Elected Members are expressly forbidden to access, display or disseminate information which is pornographic, involves threats of violence, promotes illegal acts, racial or religious hatred, or discrimination of any kind and any other material which may offend.

4.4 All private internet-use should be in accordance with 4.3

5. Security & Confidentiality

5.1 A Member should take all reasonable precautions to ensure the equipment is secure. When travelling with computer equipment, store it out of sight to

deter theft, e.g., store laptops in the car boot. If you are travelling via public transport don't leave information or equipment unattended. This also applies when visiting other offices. Laptops and other portable equipment should not be left in a vehicle overnight. Ensure you have somewhere safe to store it at home.

5.2 Council computer equipment is not insured. Appropriate measures should be taken to ensure that Council equipment is safeguarded from unauthorised access or usage.

5.3 All Members have a duty to ensure that information about members of the public, staff and sensitive non-personal Council information is handled appropriately. Sensitive information should only be made available to people authorised to view it.

5.4 Where passwords are provided these must remain confidential and not shared with others.

5.5 Privately owned personal computers or personal email accounts should not be used for Council business.

5.6 If a Member has any concerns about the security of their computer, please contact the IT provider the first instance.

5.7 It is good practice for Members to segregate Council and non-Council information, e.g., constituency work, held on computer by using separate computer or email folders.

6. Consequential Damage

6.1 The rules and advice contained within this policy, when observed, should provide users with a degree of protection from claims for consequential damage. Such claims could be encountered where the rules and advice have been ignored in respect of the following:

- Physical damage to equipment;
- Unauthorised changes to the PC configuration;
- Adding, removing or changing hardware (internal or external);
- Corruption of software configuration;

- Unauthorised changes to software configuration Virus contamination;
- Unauthorised access Unauthorised use or distribution of information;
- Use of unlicensed software Software piracy.

Recovery or correction may result in a charge being levied against the user and may also attract sanctions and/or criminal proceedings depending upon the circumstances.

7. Sanctions

7.1 Users are warned that any misuse or abuse of computer facilities may result in the use of the computer being withdrawn and reported to the Monitoring Officer;

7.2 There is an obligation on all Members who have, or have access to, computer facilities to become familiar with this Code and to observe the rules and guidelines set out. Ignorance of these guidelines will not be considered to be a reasonable defence. This section must be considered together with the Council Code of Conduct for Members.

8. Legal Requirements

8.1 The Council will, at all times, comply with the law as it refers to any of the facilities that are, or may become, available to Council users. In addition, the Council will endeavour to observe best practice and operational guidelines published in respect of such facilities by any relevant professional body.

8.2 Where potential criminal activity is suspected, the Council will refer the matter for police investigation. This course of action does not presume guilt but may be necessary to prevent the potential corruption of evidence. The legal rights of individuals will be observed. Any referral of this kind may be followed, within an appropriate timescale, by internal investigation, which may lead to the imposition of sanctions.

8.3 The Council, its Members and officers are obliged to comply with a range of legislation affecting ICT and its usage. This includes:

- Freedom of Information Act 2000;
- Computer Misuse Act 1990;

- Obscene Publications Act 1989;
- Data Protection Act 2018 (incorporating GDPR);
- Copyright Designs and Patents Act 1988

A Member should be aware of, and comply with, the Council's policies on Data Protection and Corporate Information Security.

9. Support

9.1 Support for all equipment and software provided by the Council will be provided by its IT provider United Technology helpdesk@united-technology.co.uk

9.2 The majority of support is capable of being provided remotely.

9.3 Where remote support is inappropriate or unsuccessful, a Member may be asked to drop the equipment off to the Guildhall.

I agree to the conditions of use as set out in this policy

Signed:

Dated:

This policy will be reviewed in 2025 following the local council elections