WITNEY
TOWN COUNCIL

INFORMATION TECHNOLOGY POLICY

Scope of this policy

This policy applies to all Councillors, employees, and other authorised users, regardless of their working location or pattern, including those who are home-based, office-based, or work on a flexible or part-time basis. It sets out the expectations for the appropriate use of IT equipment and systems provided by Witney Town Council.

Computer use

1.1 Hardware

1.1.1 Council computer equipment is provided for council purposes only.

1.1.2 Locking computers when leaving desk; all Councillors, employees, and other authorised users must lock their computers when leaving their desks to prevent unauthorised access. This applies to all Council and personal devices used for Council work.

1.1.3 All computer and other electronic equipment supplied should be treated with good care at all times. Computer equipment is expensive, and any damage sustained to any equipment will have a financial impact on the Council.

1.1.4 Computer and electronic hardware should be kept clean, and every precaution taken to prevent food and drink being dropped or spilled onto it.

1.1.5 All computer and mobile equipment will carry a number which is logged against the current owner of that equipment. A database of equipment issued will be kept.

1.1.6 Equipment should not be dismantled or reassembled without seeking advice.

1.1.7 Councillors, employees, and other authorised users are not to purchase any computer or mobile equipment (including software) unless previously authorised.

1.1.8 Personal disks, USB stick, CDs, DVDs, data storage devices etc cannot be used on Council computers without the prior approval of the Council's IT provider.

1.1.9 The Council has a number of wireless networks. Using a portable device to make personal Wi-Fi hot spots which bypass existing WiFi is not allowed.

1.1.10 Any faults or necessary repairs must be reported to the Deputy Town Clerk.

1.1.11 All council-issued devices are managed and patched by the council's IT provider. Critical security updates and patches are deployed within 72 hours of release or notification, subject to operational requirements and change control.

1.1.12 Local administrator rights are removed from council-issued devices. Where administrative access is required for a specific task, temporary access will be provided and controlled by the IT provider.

1.1.13 All council-issued computers and endpoints are protected by Microsoft Defender for Endpoint (EDR), providing continuous monitoring and protection against malware and other threats. Users must not disable or tamper with security controls.

1.1.14 Employees are not permitted to use personal mobile phones for council business. The only permitted use of a personal mobile phone is the Microsoft Authenticator application to support Multi-Factor Authentication (MFA).

Equipment

2.1 Portable equipment

2.1.1 Portable equipment includes laptop computers, netbooks, tablets, mobile and smart phones with email capability and access to the internet etc.

2.1.2 It is particularly emphasised that council back-up procedures specific to portable equipment should be followed at all times.

2.1.3 All portable computers must be stored safely and securely when not in use in the office, i.e. when travelling or when working from home. Portable equipment (unless locked in a secure cabinet or office) should be kept with or near the user at all times; should not be left unattended when away from council premises and should never be left in parked vehicles at any council or non-council premises.

2.1.4 It is important to ensure all portable devices are protected with encryption in case they are lost or stolen. All smartphones or tablets that hold council data, including emails and files, must be protected with a pin code. Where possible, these devices should also be programmed to erase all content after several unsuccessful attempts to break in. Any security set on these devices must not be disenabled or removed.

2.1.5 If an item of portable equipment is lost or damaged this should be reported to the Deputy Town Clerk. If the loss or damage is due to an act of negligence, the individual responsible may be liable to meet the cost of the loss/damage. Further details relating to employees can be found under Section 16 of the Staff Handbook.

2.1.6 To protect confidential information, unless it is a requirement of the job and this has been authorised, it is forbidden for photographs or videos to be taken on council premises, without the

prior written permission of the Senior Management Team. This includes mobile telephones with camera function, camcorder, tape or other recording device for sound or pictures - moving or still.

2.1.7 Under no circumstances should any non-public meeting or conversation be recorded without the permission of those present. This does not affect statutory rights (under The Openness of Local Government Regulations 2014).

2.1.8 In addition, the Council does not permit webcams (which may be pre-installed on many laptops) to be used in the workplace, other than for conference calls for council purposes. If there is any doubt as to whether a device falls under this clause, advice should be sought from the Deputy Town Clerk.

2.2 Use of own devices

2.2.1 Personal laptops and other computers or other devices should not be brought into work by employees and used to access council IT systems during working hours, unless this has been authorised by the employee's line manager. This is to ensure that no viruses enter the system, to prevent time being wasted during working hours on personal use and to assist in maintaining security, confidentiality, and data protection.

2.2.2 The Council recognises that Councillors may wish to use their own smartphones, tablets, laptops etc to access our servers, private clouds or networks for normal council purposes, including, but not limited to, reading their emails, accessing democratic documents. Any such use of personal devices will be at the discretion of the council, but consent for standard systems (MS Windows, Mac OS X, Linux - in commercial configurations) will normally be permitted. Such devices should be kept up to date so that any vulnerabilities in the operating system or other software on the device are appropriately patched or updated.

2.2.3 However, the same security precautions apply to personal devices as to the Council's desktop equipment. For continuity purposes, calls made to external parties should be made on council landlines or mobile phone numbers to ensure that only these numbers are used and/or stored by the recipient, rather than personal numbers (excluding Councillors). Any emails sent from own devices should be sent from a Council email account and should not identify the individual's personal email address.

2.2.4 Councillors, staff, and other authorised persons that use council systems are expected to use all devices in an ethical and respectful manner and in accordance with this policy and sections 13 and 16 of the Staff Handbook. Accessing inappropriate websites or services on any device via the IT infrastructure that is paid for or provided by the council carries a high degree of risk, and, for employees, may result in disciplinary action.

2.2.5 In cases of legal proceedings, the council may need to temporarily take possession of a device, whether council-owned or personal to retrieve the relevant data.

2.2.6 Wherever possible the user should maintain a clear separation between the personal data processed on the Council's behalf and that processed for their own personal use, for example, by using different apps for council and personal use. If the device supports both work and personal profiles, the work profile must always be used for work-related purposes.

2.2.7 Councillors, staff, and other authorised users who intend to use their own devices via the council's infrastructure must ensure that they:

- use a 6-digit PIN, a strong password (i.e. one which uses three random words (e.g. PurpleCandleRiver) or fingerprint to protect their device(s) from being accessed. For smartphones and tablets this should lock the device after three failed login attempts.
- configure their device(s) to automatically prompt for a password after a period of inactivity of more than two minutes.
- always password protect any documents containing confidential information that are sent as attachments to an email and notify the password separately (preferably by a means other than email).
- for smartphones and tablets, activate the automatic device wipe function (where available). Note that use of the remote wipe function may also involve the removal of the individual's personal data. Councillors, staff, and other authorised users are therefore advised to keep personal data separate from council data where possible.
- ensure secure WiFi networks are used.
- ensure that work-related data cannot be viewed or retrieved by family or friends who may use the device.
- inform the Deputy Town Clerk if their device(s) is/are lost, stolen, or inappropriately accessed where there is risk of access to council data or resources. To prevent phones being used, they will need to retain the details of their IMEI number and the SIM number of the device as their provider will require this to deactivate it.

2.2.8 Personal data relating to councillors, staff, and other authorised users, associates, residents, external stakeholders should not be saved to any personal accounts with external third-party storage cloud service providers as this may breach data protection legislation or create a security risk if the device is lost or stolen. This applies especially if the passwords used to store/access data are saved onto the device, or if the service permits councillors, staff, and other authorised users to remain logged in between sessions.

2.2.9 Personal information and sensitive data should never be saved on councillors, staff, or other authorised users own devices as this may breach confidentiality agreements, especially if the device is used by other people from time to time.

2.2.10 If removable media are used to transfer data (e.g. USB drives or CDs), the user must also securely delete the data on the media once the transfer is complete.

2.2.11 Councillors, staff, and other authorised users who open any attachments should ensure that any cached copies are deleted immediately after use. The Council's IT provider will provide

assistance or training in doing this if needed. Additional risks include data belonging to the council being accessed by unauthorised persons if the device(s) is lost, stolen, or used without the owner's permission.

2.2.12 Any work done on user's own equipment should be stored securely and password protected and should always be backed up in accordance with the council's standard backup procedures.

2.2.13 If transferring data, either by email or by other means, this should be done through an encrypted channel, such as a virtual private network (VPN) or a secure web protocol (https://). Unsecured wireless networks should not be used.

2.2.14 Prior to the disposal of any device that has work data stored on it, and in the event of a user leaving the council, councillors, staff, and other authorised users are required to allow the Council's IT provider access to the device to ensure that all passwords, user access shortcuts and any identifiable data are removed from the device.

2.2.15 Councillors, staff, and other authorised users must take responsibility for understanding how their device(s) work in respect to the above rules if they are accessing council servers/services via their own IT equipment. Risks to the user's personal device(s) include data loss as a result of a crash of the operating system, bugs and viruses, software or hardware failures and programming errors rendering a device inoperable. The Council will use reasonable endeavours to assist, but councillors, staff, and other authorised users are personally liable for their own device(s) and for any costs incurred as a result of the above.

Health and safety

3.1.1 Staff, and other authorised users who work in council offices will be provided with an appropriate workstation.

3.1.2 The council has a duty to ensure that regular appropriate eye tests, carried out by a competent person, are offered to employees using display screen equipment. Further details are set out in Section 3 of the Council's Staff Handbook.

3.1.3 Any VDU user who feels that their workstation requires changes to make it compliant must speak to their line manager.

If any hazards are detected at a workstation, including 'noises' from the IT equipment, this should be reported immediately to their Line Manager.

Password and Authentication Policy

4.1.1 All user accounts must be protected by strong, secure passwords. The Council follows the National Cyber Security Centre (NCSC) recommendations for creating passwords using three random words (e.g. PurpleCandleRiver). This method helps create passwords that are both

strong and easy to remember, while offering effective protection against common cyber threats such as brute-force attacks. This approach is endorsed in NALC guidance.

In addition to strong passwords, Multi-Factor Authentication (MFA) is enforced via Conditional Access using Microsoft Authenticator. Users are prompted to re-approve sign-in every 30 days. Phishing-resistant MFA is enabled for all compatible users. Users must not approve unexpected authentication prompts. Any suspicious requests must be reported to the IT provider immediately.

To further strengthen account security:

- Initial user account passwords must be generated by the IT provider.
- Default passwords provided by vendors or the IT provider should be changed immediately upon installation or setup.
- Service or System account passwords are generated and managed by the IT provider.
- The council recommends these practices as part of its commitment to robust information security and to support compliance with the UK GDPR and the Data Protection Act 2018.

4.1.2 Access to Passwords

- Passwords are personal and must not be shared under any circumstances.
- Only the assigned user of an account may access or use the associated password.
- In exceptional cases (e.g., incident response or employee offboarding), access to system credentials may be granted to authorised personnel from the IT provider with appropriate approvals and logging.
- Administrative credentials must be stored securely and only accessible to authorised personnel.

4.1.3 Password Storage and Management

- Passwords must not be stored in plain text or written down in insecure locations.
- Passwords must be stored using a council-approved, encrypted password manager (e.g., LastPass, Bitwarden, or KeePass).

4.1.4 Password Change Requirements

- Immediately change password if compromise is suspected.

4.1.5 Password Access Control and Logging

- All access to administrative or shared credentials must be logged and auditable.
- Attempts to access unauthorised passwords will be treated as a security incident.

4.1.6 Responsibility

- Users are responsible for creating and maintaining secure passwords for their accounts.

The IT security provider is responsible for:

- Managing system/service credentials.
- Enforcing password policies. Auditing and monitoring password-related security practices.

Monitoring

5.1.1 The council reserves the right to monitor and maintain logs of computer usage and inspect any files stored on its network, servers, computers, or associated technology to ensure compliance with this policy as well as relevant legislation. Internet, email, and computer usage may be monitored as part of the council's protection against computer viruses, ongoing maintenance of the system, and when investigating faults.

5.1.2 A security incident is any event which may compromise the confidentiality, integrity, or availability of the council's information or systems (including loss or theft of a device, suspected malware or virus infection, suspicious emails/links, unexpected MFA prompts, unauthorised access, or accidental disclosure). Any suspected or actual incident must be reported immediately to the Deputy Town Clerk and the council's IT provider, even if the user is unsure. Where possible the user should disconnect any affected device from the internet or network (for example turn off Wi-Fi) and must not attempt to investigate or "fix" the issue. Users must not delete emails, files, logs, browser history, or other information that may be required for investigation; suspected phishing emails must not be clicked, opened, replied to, or forwarded (unless instructed). If personal data or confidential council information may have been exposed, this must be reported immediately as legal and regulatory reporting deadlines may apply.

5.1.5 Monitoring of an employee's email and/or internet use will be conducted in accordance with Section 13 of the Staff Handbook.

5.1.6 The information obtained through monitoring may be shared internally, including with relevant councillors and IT staff if access to the data is necessary for performance of their roles. The information may also be shared with external HR or legal advisers for the purposes of seeking professional advice. Any external advisers will have appropriate data protection policies and protocols in place.

5.1.7 The information gathered through monitoring will be retained only long enough for any breach of this policy to come to light and for any investigation to be conducted.

5.1.8 Councillors, staff, and other authorised users have a number of rights in relation to their data, including the right to make a subject access request and the right to have data rectified or erased in some circumstances. You can find further details of these rights and how to exercise them in the council's data protection policy.

5.1.9 Such monitoring and the retrieval of the content of any messages may be for the purposes of checking whether the use of the system is legitimate, to find lost messages or to retrieve

messages lost due to computer failure, to assist in the investigation of wrongful acts, or to comply with any legal obligation (e.g. Freedom of Information & Data Subject Access requests).

5.1.10 The Council reserves the right to inspect all files stored on its computer systems in order to assure compliance with this policy. The council also reserves the right to monitor the types of sites being accessed and the extent and frequency of use of the internet at any time, both inside and outside of working hours to ensure that the system is not being abused and to protect the council from potential damage or disrepute.

5.1.11 Any use that the council considers to be 'improper', either in terms of the content or the amount of time spent on this, may result in disciplinary proceedings.

5.1.12 All computers will be periodically checked and scanned for unauthorised programmes and viruses.

5.1.13 The council's Microsoft 365 data (including Exchange Online, SharePoint Online, OneDrive for Business and Teams data where applicable) is backed up seven times per day and retained for seven years.

5.1.14 The council's Microsoft Azure workloads are backed up once per day and retained for one year.

5.1.15 Back-up and restore tests will be carried out periodically to confirm recoverability, and any issues will be addressed promptly.

5.1.16 Back-ups are protected against unauthorised access and stored in a manner that reduces the risk of loss through system failure or malicious activity.

5.1.17 The council's email and collaboration services (including Outlook, Teams, SharePoint and OneDrive) are protected using Microsoft Defender for Office 365, including anti-phishing and anti-spam controls, Safe Links and Safe Attachments protection. Users must remain vigilant, follow on-screen warnings and prompts, and report suspected phishing attempts to the IT provider.

Remote working

6.1.1 Increased IT security measures apply to those who work away from their normal place of work (e.g. whilst travelling, working from home, as follows:

- if logging into the council's systems or services remotely, using computers that either do not belong to the council or are not owned by the user, any passwords must not be saved, and the user must log out at the end of the session deleting all logs and history records within the browser used. If the configuration of the device does not clearly support these actions (for example at an internet café), council services should not be accessed from that device.

- the location and direction of the screen should be checked to ensure confidential information is out of view. Steps should be taken to avoid messages being read by other people, including other travellers on public transport etc.
- any data printed should be collected and stored securely.
- all electronic files should be password protected and the data saved to the council's system/services when accessible.
- papers, files or computer equipment must not be left unattended at non-Council premises unless arrangements have been made with a responsible person at the premises for them to be kept in a locked room or cabinet if they are to be left unattended at any time.
- any data should be kept safely and should only be disposed of securely.
- papers, files, data sticks/storage, flash drive or backup hard drives should not be left unattended in cars, except where it is entirely unavoidable for short periods, in which case they must be locked in the boot of the car. If staying away overnight, council data should be taken into the accommodation, care being taken that it will not be interfered with by others or inadvertently destroyed.
- where possible the ability to remotely wipe any mobile devices that process sensitive information should be retained in the case of loss or theft.
- Councillors, staff, and other authorised users who work away from the office with sensitive data may be equipped with a screen privacy filter for mobile devices and should use this at all times when accessing such data away from the office.

6.1.2 Those issued with a 'dongle' to enable internet access from a laptop via 3G or 4G networks whilst away from their normal workplace should note that the cost of internet access can be very high. Dongles should therefore be used for essential council purposes only, especially if abroad.

6.1.3 Similarly, use of paid for Wi-Fi access, for example at airports should be carefully monitored and restricted to essential council use.

Email

7.1.1 Council email facilities are intended to promote effective and speedy communication on work-related matters. Although we encourage the use of email, it can be risky. Councillors, staff, and other authorised users need to be careful not to introduce viruses onto council systems and should take proper account of the security advice below.

7.1.2 On occasion, it will be quicker to action an issue by telephone or face to face, rather than via protracted email chains. Emails should not be used as a substitute for face to face or telephone conversations. Councillors, staff, and other authorised users are expected to decide which is the optimum channel of communication to complete their tasks quickly and effectively.

7.1.3 These rules are designed to minimise the legal risks run when using email at work and to guide councillors, staff, and other authorised users as to what may and may not be done. If there is something which is not covered in the policy, councillors, staff, and other authorised users should ask the IT Provider, rather than assuming they know the right answer.

7.1.4 All councillors, staff, and other authorised users who need to use email as part of their role will normally be given their own council email address and account.

7.1.5 Email messages sent on the council's account are for council use only. Personal use is not permitted.

Use of the Internet

8.1 Copyright

8.1.1 Much of what appears on the Internet is protected by copyright. Any copying without permission, including electronic copying, is illegal and therefore prohibited. The Copyright, Designs and Patents Act 1988 set out the rules. The copyright laws not only apply to documents but also to software. The infringement of the copyright of another person or organisation could lead to legal action being taken against the council and damages being awarded, as well as action being taken against the perpetrator.

8.1.2 It is easy to copy electronically, but this does not make it any less an offence. The council's policy is to comply with copyright laws, and not to bend the rules in any way.

8.1.3 Councillors, employees, and other authorised users should not assume that because a document or file is on the Internet, it can be freely copied. There is a difference between information in the 'public domain' (which is no longer confidential or secret information but is still copyright protected) and information which is not protected by copyright (such as where the author has been dead for more than 70 years).

8.1.4 Usually, a website will contain copyright conditions; these warnings should be read before downloading or copying.

8.1.5 Copyright and database right law can be complicated. Councillors, staff, and other authorised users should check with the Deputy Town Clerk if unsure about anything.

8.2 Trademarks, links and data protection

8.2.1 The Council does not permit the registration of any new domain names or trademarks relating to the council's names or products anywhere in the world, unless authorised to do so. Nor should they add links from any of the council's web pages to any other external sites without checking first with the Deputy Town Clerk.

8.2.2 Special rules apply to the processing of personal and sensitive personal data. For further guidance on this, see the council's data protection policy, a copy of which is available on the Town Council's website here Document Data Protection Policy - Witney Town Council

8.3 Accuracy of information

8.3.1 One of the main benefits of the internet is the access it gives to large amounts of information, which is often more up to date than traditional sources such as libraries. Be aware that, as the internet is uncontrolled, much of the information may be less accurate than it appears.

8.3.2 Artificial intelligence (AI) tools (for example, chat-based assistants) may be used to support council work only where the content is non-confidential and does not include personal data. Council confidential information, sensitive data, and personal data must not be entered into any AI service unless a managed approval process has been completed and appropriate safeguards are in place. Only council-approved AI services should be used for council business and users must not upload council documents or data into personal AI accounts or unapproved services. Users must review and validate any AI-generated output before use, as AI output may be inaccurate or incomplete and must not be treated as a substitute for professional judgement or appropriate approvals. Use of AI must comply with this policy and the council's obligations under the UK GDPR and the Data Protection Act 2018, including confidentiality and data minimisation.

Use of social media

9.1.1 Social media includes blogs; Wikipedia and other similar sites where text can be posted; multimedia or user generated media sites (YouTube); social networking sites (such as Facebook, LinkedIn, X (formerly known as Twitter), Instagram, TikTok, etc.); virtual worlds (Second Life); text messaging and mobile device communications and more traditional forms of media such as TV and newspapers. Care should be taken when using social media at any time, either using council systems or at home.

9.1.2 Personal use of social networking/media and chat sites by employees are not permitted during working hours.

9.1.3 The council recognises the importance of councillors, staff, and other authorised users joining in and helping to shape sector conversation and enhancing its image through blogging and interaction in social media. Therefore, where it is relevant to use social networking sites as part of the individual's position, this is acceptable**. Further details of this can be found in the Council's social media Policy.**

Misuse

Misuse of IT systems and equipment is not in line with the council's standards of conduct and will be taken seriously. Any inappropriate or unauthorised use may lead to formal action, including disciplinary proceedings or, in serious cases, dismissal for employees.

It is important to note that all contact details and information remain the property of the council. In addition, councillors, employees, and other authorised users leaving the council will be required to delete all council-related data including residents contact details from any personal device/equipment.