LITTLE OAKLEY PARISH COUNCIL
INFORMATION TECHNOLOGY POLICY

Adopted 8th April 2026 (Minute Number 25/154)
Reviewed biennially
Next Review Date February 2028

Purpose of the IT Policy

The purpose of an IT policy is to establish clear parameters for how councillors, employees and other authorised users use council-provided technology or equipment in the course of their duties. A well-defined policy helps to:

- Set expectations for appropriate use of equipment and systems;
- Raise awareness of risks associated with IT use;
- Safeguard the council's data and digital assets;
- Clarify what constitutes acceptable and unacceptable use;
- Outline the consequences of policy breaches.

Little Oakley Parish Council will also determine and clearly state whether limited personal use of IT equipment is permitted (for example, checking personal email or online shopping during lunch breaks).

Monitoring of IT Use

The council has the right to monitor the use of its IT equipment, provided there is a legitimate reason for doing so and councillors, employees and other authorised users are informed that such monitoring may take place. Any monitoring must be proportionate and comply with relevant data protection and privacy laws. Other persons may be included if they access or use council systems e.g. if they have a council e-mail address

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, 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 Little Oakley Parish Council (hereinafter referred to as 'the council').

Computer use

1.1 Hardware

1.1.1 Council computer equipment is provided for council purposes only.

1.1.2 All councillors, employees and other authorised users must lock their computers when leaving equipment unattended to prevent unauthorised access. This applies to all council and personal devices used for work. Failure to comply may lead to disciplinary action.

1.1.3 All computer and other electronic equipment supplied should be treated with good care at all times. 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 Equipment should not be dismantled or reassembled without seeking advice.

1.1.6 Councillors, employees and other authorised users must not purchase any IT equipment (including software) unless previously authorised.

1.1.7 Personal disks, USB sticks, CDs, DVDs, data storage devices etc cannot be used on council computers without the prior approval of the Chair or Vice-chair of the council.

1.1.8 Any faults or necessary repairs to any council-owned IT equipment must be reported to the Chair or Vice-chair of the council.

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 Council back-up procedures specific to portable equipment should be followed at all times.

2.1.3 All portable equipment must be stored safely and securely when not in use. Portable equipment should never be left unattended in a parked vehicle or at any third-party premises, except where it is entirely unavoidable for short periods (see 6.1.1).

2.1.4 All portable devices are to be protected with encryption in case they are lost or stolen. Laptops, smartphones or tablets that hold council data, including emails and files, must be protected with a pin or pass code. Any security set on these devices must not be disabled or removed.

2.1.5 If an item of portable equipment is lost or damaged this should be reported to the Chair or Vice-chair of the council. If loss or damage is due to an act of negligence, the individual responsible may be liable to disciplinary proceedings.

2.1.6 Under no circumstances should any council-owned or personal equipment be used to record conversations in non-public meetings without the permission of those present. This does not affect statutory rights (under The Openness of Local Government Regulations 2014).

2.1.7 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 Chair or Vice-chair of the council.

2.2 Use of personal devices

2.2.1 The Council recognises that some councillors, employees and other authorised users may wish to use their own equipment to access council data for normal council purposes, including, but not limited to, accessing their email accounts. 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.

2.2.2 The same security precautions apply to personal devices as to the council's IT equipment. For continuity purposes, calls made to external parties (such as external stakeholders or members of the public) should be made on council mobile phones where possible to ensure that only these numbers are used and/or stored by the recipient, rather than personal numbers. Any emails sent from own devices should be sent from a council email account and should not identify the individual's personal email address.

2.2.3 Councillors, employees and other authorised users are expected to use all devices in an ethical and respectful manner and in accordance with this policy. Accessing inappropriate websites or services on any device that is paid for or provided by the council, may result in disciplinary action including, for employees, summary dismissal (without notice). For workers or contractors, we may terminate the worker agreement. This is irrespective of the ownership of the device used. An example would be downloading copyright music illegally or accessing pornographic material.

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

2.2.5 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 accounts/logins for council and personal use. If a single device supports both work and personal profiles, the work profile must always be used for work-related purposes.

2.2.6 Councillors, employees and other authorised users who intend to use their own devices for council work must ensure that they:

- use a 6-digit pin, strong password, finger print or face ID to protect their device(s) from being accessed. For smartphones and tablets this should lock the device after ten 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, employees 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 council related data cannot be viewed or retrieved by family or friends who may use the device;

- inform the Chair or Vice-chair of the council if their device(s) are lost, stolen, or inappropriately accessed where there is risk of access to council data or resources. To prevent phones being used, the user needs to retain the details of the IMEI number and the SIM number of the device as the provider will require this to deactivate it.

2.2.7 Any work done on personal equipment should be stored securely and password protected and should always be backed up in accordance with the standard backup procedures.

2.2.8 Prior to the disposal of any device that has work data stored on it, or in the event of a user leaving the council, councillors, employees and other authorised users are required to allow an appropriate person access to the device to ensure that all passwords, user access shortcuts and any identifiable data are removed from the personal device.

2.2.9 Councillors, employees 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 data via their personal 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 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 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.

3.1.2 Any VDU user who feels that their workstation requires changes to make it compliant must speak to the Chair or Vice-chair of the council

3.1.3 If any hazards are detected at a workstation, including ‘noises’ from the IT equipment, this should be reported immediately to the Chair or Vice-chair of the council.

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.

To further strengthen account security:

- Initial user account passwords must be generated by the provider.
- Any default passwords provided by vendors must be changed immediately upon installation or setup.
- Website account passwords are generated and managed by the web 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.

For more guidance, see the NCSC's advice on password security: NCSC Password Guidance

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 with appropriate approvals..
- Administrative credentials must be stored securely and only accessible to authorised personnel with a copy provided to the Chair or Vice-chair of the council in a sealed envelope, which can only to be accessed in an emergency.

4.1.3 Password Storage and Management

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

4.1.4 Password Change Requirements

- Immediately change a password if any 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 IT equipment and accounts.

Monitoring

5.1.1 The council reserves the right to monitor and maintain logs of computer/laptop usage and inspect any files stored on its equipment to ensure compliance with this policy as well as relevant legislation. Internet, email, and computer usage is continually monitored where possible as part of the council's protection against computer viruses and when investigating faults.

5.1.5 Where possible, the council will monitor the use of electronic communications and use of the internet in line with the Investigatory Powers (Interception by Councils etc for Monitoring and Record-keeping Purposes) Regulations 2018.

5.1.6 Any monitoring of email accounts and/or internet use will be conducted when considered necessary and will always be proportionate. Monitoring is in the council's legitimate interests and is to ensure that this policy is being complied with.

5.1.7 The information obtained through monitoring may be shared internally, including with relevant councillors. 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.

5.1.8 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.

5.1.9 Councillors, employees 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.

5.1.10 Such monitoring and the retrieval of the content of any messages may be for the purposes of checking whether the use of the equipment is legitimate, to find lost messages or to retrieve messages lost due to equipment failure, to assist in the investigation of wrongful acts, or to comply with any legal obligation.

5.1.11 The council reserves the right to inspect all files stored on its equipment in order to assure compliance with this policy. The council also reserves the right to monitor the types of sites being accessed to ensure that the system is not being abused and to protect the council from potential damage or disrepute.

5.1.12 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.

5.1.13 All devices will be periodically checked and scanned for unauthorised programmes and viruses.

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, or at any other premises), as follows:

- if logging into the council's systems (eg email) 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 systems 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 accessed should be password protected;

- papers, files or computer equipment must not be left unattended at a remote premises unless arrangements have been made with a responsible person at the premises for them to be kept in a locked room or cabinet.;
- any data should be kept safely and should only be disposed of securely;
- papers, files, data sticks/storage, flash drives or backup hard drives should not be left unattended in a vehicle, 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 equipment and 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, employees and other authorised users who work away from their normal workplace with sensitive data should be equipped with a screen privacy filter for mobile devices and should use this at all times when accessing such data away from the normal workplace.

6.1.2 If a dongle is issued to enable internet access from a laptop via 3G or 4G networks whilst away from their normal workplace, users 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, any use of remote, paid for Wi-Fi access 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 the use of email is encouraged, it can have its risks. Councillors, employees and other authorised users need to be careful not to introduce viruses onto council equipment and should take proper account of the security advice detailed 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, employees 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, employees and other authorised users as to what may and may not be done. If there is something which is not covered in this policy, councillors, employees and other authorised users should ask an appropriate person rather than assuming they know the right answer.

7.1.4 All councillors, employees and other authorised users who need to use email as part of their role will be issued their own council-owned email address and account. The council may, at any time, withdraw email access, should it feel that this is no longer necessary for the role or that the system is being abused.

7.1.5 Email messages sent on the council's account are for council use only. Personal use is not permitted. The council will only accept communications from councillors and employees from their council-issued email address.

Use of the Internet

8.1 Copyright

8.1.1 Much of what appears on the internet is protected by copyright, therefore 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, which could result in disciplinary action, including dismissal, 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, employees and other authorised users should check with an appropriate person 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, without authorisation to do so. Links are not to be added from any of the council's web pages to any other external sites without checking first with the Chair or Vice-chair of the council.

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 council's website.

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 though, that as the internet is uncontrolled, much of the information may be less accurate than it actually appears.

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 (eg YouTube); social networking sites (such as Facebook, LinkedIn, X, 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.

9.1.2 The council has a separate policy for social media use which is available on the council website.

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.