# SHOTTISHAM PARISH COUNCIL

## INFORMATION TECHNOLOGY POLICY

JANUARY 2026

# SHOTTISHAM PARISH COUNCIL
# INFORMATION TECHNOLOGY POLICY

## Purpose of the IT Policy

The purpose of an IT policy is to establish clear parameters for how councillors, staff, 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.

Councils will also need to 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

As an IT provider, the council has the right to monitor the use of its IT equipment and systems, 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, staff, 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 the council.

## Computer use

### 1.1 Hardware

**1.1.1** Council computer equipment is provided for council purposes; however reasonable personal use is permitted by the clerk. The clerk is asked to restrict any personal use to before or after working hours.

**1.1.2** 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.

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

**1.1.4** Equipment should not be dismantled or reassembled without seeking advice.

**1.1.5** The clerk is not to purchase any computer or mobile equipment (including software). Unless previously authorised.

**1.1.6** Personal disks, USB stick, CDs, DVDs, data storage devices etc cannot be used on council computers without the prior approval of the clerk.

**1.1.7** Any faults or necessary repairs must be reported to 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** 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 working from home or when travelling. Portable equipment should be kept securely stored at home and should never be left in parked vehicles.

**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** Multi-Factor Authentication (MFA) is a security process that requires users to verify their identity using two or more independent methods—for example, entering a password (something you know) and confirming a code sent to your mobile device (something you

have). This significantly reduces the risk of unauthorised access to systems and sensitive data. NALC recommends implementing MFA as a best practice to enhance information security and support compliance with data protection obligations under the UK GDPR and the Data Protection Act 2018.

**2.1.6** If an item of portable equipment is lost or damaged this should be reported to the council by the clerk. If the loss or damage is due to an act of negligence, the individual responsible may be liable to meet the first £200 of the loss/damage.

**2.1.7** 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 at council meetings, without the prior written permission of the council. This includes mobile telephones with camera function, camcorder, tape or other recording device for sound or pictures - moving or still.

**2.1.8** 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).

**2.1.9** 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.

### 2.2 Use of own devices

**2.2.1** The council recognise that the clerk may wish to use their own smartphone, tablet, laptop etc to access their council email account to read emails or to access council documents from the cloud. 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** However, the same security precautions apply to personal devices as to the council's desktop equipment. 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** When using the council system, the clerk is expected to use the device in an ethical and respectful manner and in accordance with this policy. 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 may result in disciplinary action, including summary dismissal (without notice). 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 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.

**2.2.6** When the clerk intends to use their own devices via the council's infrastructure, they must ensure that they:

- use a 6-digit pin, strong password (i.e. one which uses three random words (e.g. PurpleCandleRiver) or finger print (preferably the latter to protect their device from being accessed. For smartphones and tablets this should lock the device after three failed login attempts;
- configure their device to automatically prompt for a password after a period of inactivity of more than 5 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 council if their device is 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.

**2.2.7** Personal information and sensitive data should never be saved on the clerk's own devices as this may breach confidentiality agreements, especially if the device is used by other people from time to time.

**2.2.8** 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.

**2.2.9** Prior to the disposal of any device that has work data stored on it, and in the event of a user leaving the council, the clerk should ensure that all passwords, user access shortcuts and any identifiable data are removed from the device.

**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 council. If any hazards are detected at a workstation, including 'noises' from the IT equipment, this should be reported immediately to 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. This approach is endorsed in NALC guidance.

In addition to strong passwords, Multi-Factor Authentication (MFA) should be enabled wherever possible. MFA requires users to provide two or more independent forms of verification—for example, a password (something you know) and a code sent to your phone (something you have). This significantly reduces the risk of unauthorised access to systems and personal data.

To further strengthen account security:

- Default passwords provided by vendors or the IT provider must be changed immediately upon installation or setup.
- Service or System (e.g. Website) 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.

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 the council.
- Administrative credentials must be stored securely and only accessible to authorised personnel with a copy provided to the Chair, in a sealed envelope, 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.
- 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 unauthorized passwords will be treated as a security incident.

**4.1.6** Responsibility

- The clerk is responsible for creating and maintaining secure passwords for their accounts.

**Monitoring**

**5.1.1** The council reserves the right to inspect any files stored on its council laptop to ensure compliance with this policy as well as relevant legislation.

**5.1.5** 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.

**5.1.6** The clerk and councillors 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.

**5.1.7** 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.

**5.1.8** The council reserves the right to inspect all files stored on its computer system 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.

**Remote working**

**6.1.1** Increased IT security measures apply to working from home, whilst travelling, or any other different venue), as follows:

- 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;
- papers, files or computer equipment must not be left unattended unless arrangements have been made for them to be kept in a locked 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;

**6.1.2** 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. The clerk and councillors need to be careful not to introduce viruses onto the email system 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. The clerk is 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 and the clerk as to what may and may not be done.

**7.1.4** All councillors and the clerk who need to use email as part of their role will normally be given their own council 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.

**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 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 and the clerk 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 should check with the 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 council or the 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.

### 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.

### 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 the council system or at home.

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

**9.1.3** The council recognises the importance of councillors and the clerk 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.

However, inappropriate comments and postings can adversely affect the reputation of the council, even if it is not directly referenced. If comments or photographs could reasonably be interpreted as being associated with the council, or if remarks could be regarded as abusive, humiliating, sexual harassment, discriminatory or derogatory, or could constitute bullying or harassment, the council will treat this as a serious disciplinary offence. Councillors and the clerk should be aware that parishioners or other local organisations may read councillors, and the clerk's personal weblogs, to acquire information, for example, about their work, internal council business, and employee moral. Therefore, even if the council is not named, care should be taken with any views expressed.

**9.1.4** To protect both the council and its interests, everyone is required to comply with the following rules about social media, whether in relation to their council role or personal social networking sites, and irrespective of whether this is during or after working hours:

- Any blog that mentions the council, its current work, councillors, employees, other users associated with the council, partner organisations, local groups, suppliers, parishioners, should identify the author as one of its councillors or employees and state that the views expressed on the blog or website are theirs alone and do not represent the views of the council. Even if the council is not mentioned, care should be taken with any views expressed on social media sites and any views should clearly be stated to be the writer's own (e.g. via a disclaimer statement such as: "The comments and other content on this site are my own and do not represent the positions or opinions of the council. Writers must not claim or give the impression that they are speaking on behalf of the council.
- Any employee who is developing a site or writing a blog that will mention the council, our current or potential plans or councillors, must inform the council that they are writing this and gain agreement before going 'live'.
- The council expects councillors and the clerk to be respectful about the council and its current or potential users and not to engage in any name calling or any behaviour that will reflect negatively on its reputation. Any unauthorised use of copyright materials, any unfounded or derogatory statements, or any misrepresentation is not viewed favourably and could constitute gross misconduct.
- Photos, videos, or audio recordings must not be taken at council meetings without explicit permission
- Comments posted by councillors and the clerk on any sites should be knowledgeable, accurate and professional and should not compromise the council in any way.
- Inappropriate conversations with external stakeholders should not take place on any social networking sites, including forums.
- Any writing about or displaying photos or videos of internal activities that involves current councillors and the clerk, might be considered a breach of data protection and a breach of privacy and confidentiality. Therefore, their permission should be gained prior to uploading any such material. Details of any kind relating to any events, conversations, materials or documents that are meant to be private, confidential or internal to the council should not be posted. This may include manuals; procedures; training documents; non-public financial or operational information; personal information regarding other councillor and the clerk, anything to do with a disciplinary case, grievance, allegation of bullying/harassment or discrimination, or legal issue; any other secret, confidential, or proprietary information or information that is subject to confidentiality agreements. This does not affect statutory requirements to publish information including under the Freedom of Information Act.
- Councillors and the clerk must be aware that they are personally liable for anything that they write or present online (including on an online forum or blog, post, feed or website). Councillors should always be mindful of the Members Code of Conduct and Nolan Principles. Employees may be subject to disciplinary action for comments, content, or images that are defamatory, embarrassing, pornographic, proprietary,

harassing, libellous, or that can create a hostile work environment. They may also be sued by other organisations, and any individual or council that views their comments, content, or images as defamatory, pornographic, proprietary, harassing, libellous or creating a hostile work environment. In addition, other councillors and the clerk can raise grievances for alleged bullying and/or harassment.

- Postings to websites or anywhere on the internet and social media of any kind, or in any press or media of any kind, should not breach copyright or other law or disclose confidential information, defame or make derogatory comments about the council or its councillors or clerk, or disclose personal data or information about any individual that could breach data protection legislation.
- Contacts by the media relating to the council, should be referred to the clerk or Chair.
- Councillors and staff who use sites such as LinkedIn and Facebook must ensure that the information on their profile is accurate and up to date and must update their profile on leaving the council.
- Councillors and staff who have left the council must not post any inappropriate comments about the council or its councillors, staff, and other authorised users on LinkedIn, Facebook, X.com or any other social media/networking sites.

**9.1.5** Note that the council may, from time to time, monitor external postings on social media sites. Any employee who has a profile (for example on LinkedIn or Facebook) must not misrepresent themselves or their role with the council. Councillors and staff are also advised that social media sites are not an appropriate place to air council concerns or complaints: these should be raised with the council or formally through the grievance procedure.

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

**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.