SHAW-CUM-DONNINGTON PARISH COUNCIL

INFORMATION TECHNOLOGY POLICY

Introduction

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.

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 email 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 (reasonable interpreted as in the opinion of the council). Any personal use of our computers and systems should not interrupt our daily council work in any way. Councillors, staff and other authorised users are asked to restrict any personal use to official lunch breaks or 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 spilt onto it.

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

1.1.5 Councillors, staff and other authorised users are not to purchase any computer or mobile equipment (including software) with Council money unless previously authorised.

1.1.6 Personal discs, USB sticks, CDs, DVDs, data storage devices etc. cannot be used on council computers without the prior approval of the council.

Equipment

2.1 Portable equipment

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

2.1.2 All portable computers must be stored safely and securely when not in use in the office, e.g. when travelling, they should not be left unattended and should never be left in parked vehicles or at any council or non-council premises.

2.1.3 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 disabled or removed.

2.1.4 If an item of portable equipment is lost or damaged, this should be reported to the council. If the loss or damage is due to an act of negligence, the individual responsible may be liable to meet the first £150 of the loss/damage.

2.1.5 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).

2.2 Use of own devices

2.2.2 The council recognises that some councillors, staff and other authorised users 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 and accessing documents stored on the council's Dropbox account – or to store data on the council's server(s) or access data in other services. 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 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. 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, including 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.

2.2.5 In cases of legal proceedings against the council or external stakeholders, 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 strong password (e.g. one which uses three random words, such as PurpleCandleRiver) or a fingerprint (preferably the latter) 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 30 minutes;
- ensure secure Wi-Fi networks are used;
- ensure that work-related data cannot be viewed or retrieved by family or friends who may use the device;
- inform the clerk if their device(s) is/are lost, stolen or inappropriately accessed where there is a 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 Any work done on a 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 of saving to the Dropbox Cloud.

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, councillors, staff and other authorised users are required to allow the IT provider access to the device to ensure that all passwords, user access shortcuts and any identifiable data are removed from the device.

2.2.10 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.

Password and Authentication Policy

3.1.1 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:

- Initial user account passwords must be generated by the IT provider.
- 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

3.1.2 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 staff from the IT provider with appropriate approvals and logging.
- Administrative credentials must be stored securely and only accessible to authorised staff with a copy provided to the Chair of the council, in a sealed envelope, only to be accessed in an emergency.

3.1.3 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).

3.1.4 Password change requirements

- Immediately change password if compromise is suspected.

3.1.5 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.

3.1.6 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.

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 or at an external stakeholder's premises or any other different venue), 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 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 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 office.

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. 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 sets 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, staff 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 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 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 on the 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 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 council systems or at home.

9.1.2 Personal use of social networking/media and chat sites is 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.

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 about external stakeholders 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, staff and other authorised users should be aware that parishioners or other local organisations may read the personal weblogs of councillors, staff and other authorised users to acquire information, for example about their work, internal council business and employee morale. 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 outside working hours:

- Contacts from any of the council's databases should not be downloaded and connected with on LinkedIn or other social networking sites with electronic address book facilities, unless this has been authorised.
- Any blog that mentions the council, its current work, councillors, employees, other users associated with the council, partner organisations, local groups, suppliers or 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 my employer/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, councillors, staff and other authorised users and partners must inform the clerk that they are writing this and gain agreement before going 'live'.
- The council expects councillors, staff and other authorised users to be respectful about the council and its current or potential staff, including employees, councillors, clerks, and authorised 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 or videos that include employees or other workers wearing uniforms or clothing displaying the council's name or logo should not be posted on social media if they could reflect negatively on the individual, their role, their colleagues or the council. Additionally, photos, videos or audio recordings must not be taken on council premises without explicit permission
- Comments posted by councillors, staff and other authorised users 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, staff and other authorised users 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 councillors, staff and other authorised users which includes 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, staff and other authorised users 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, staff and other authorised users 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, staff and other authorised users 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.
- Councillors, staff and other authorised users 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, staff and other authorised users who use X.com, LinkedIn or other social media/networking sites for council development purposes must ensure they provide the council with login details, including password(s), so that these sites can be accessed and updated in their absence.
- Councillors, staff and other authorised users 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.
- During your employment/ involvement with the council, you may create or obtain access to a variety of professional contacts and confidential information. This includes, but is not limited to, contacts made through professional networking platforms such as LinkedIn, where those contacts have been established or maintained in your capacity as a councillor, member of staff or other authorised user. All such contacts will be considered council property and may be subject to disclosure upon request.

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, staff and other authorised users 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.

Policy adopted on xxx