IT Policy

Introduction
This policy applies to all councillors, staff and authorised users all of whom are home based and work on a part-time or flexible basis. It sets out the expectations of for the appropriate use of IT equipment and systems provided by the Council.

Computer Use

1 Hardware

1.1 Any Council computer equipment is provided for council purposes only.

1.2 All councillors, staff 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 work. Failure to comply may lead to disciplinary action.

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

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.

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

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

1.7 Personal discs USB sticks CD's DVD's data storage devices etc should not be used on council computers.

1.8 Councillors, staff and other authorised users are expected to use all devices in an ethical and respectful manner. Accessing inappropriate websites or services on any device that is paid for or provided by the council carries a high degree of risk, and for employees may result in immediate disciplinary action. An example would be downloading copyright music illegally or accessing pornographic material.

2 Portable Equipment

2.1 Portable equipment includes laptop computers netbooks tablets mobile and smartphones with e-mail capacity capability and access to the Internet etc.

2.2 All portable computers must be stored safely and securely when not in use. Portable equipment should be always kept with or near the user; should not be left unattended and should never be left in parked vehicles or at any council or non-council premises.

2.3 All portable devices should be protected with encryption in case they are lost or stolen. All smartphones or tablets that hold council data including emails and files must be protective 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 dis enabled or removed.

2.4 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 £100 of the loss or damage

2.5 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 clerk. This includes mobile telephones with camera function camcorder tape or other recording device for sound or pictures moving or still.

2.6 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).

2.7 All portable equipment provided by the council must be returned promptly upon leaving the council.

3. Use of own devices

3.1 Personal laptops and other devices should not ordinarily be used for council business to ensure that there is a clear separation between council and personal use.

3.2 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.

3.4 Personal data relating to councillors, staff, other authorised users, residents or associations, should not be saved to any personal accounts with 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.

3.5 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 the devices used by other people from time to time. This data should never be accessed or processed on a personal device.

3.6 If removable media are used to transfer data, the user must also securely delete the data on the media once the transfer is complete.

3.7 Councillors staff and other authorised users who open any confidential attachments should ensure that any cached copies are deleted immediately after use. Additional risks include data belonging to the council being accessed by unauthorised persons if the device is lost stolen or used without the owner's permission.

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

3.9 Prior to the disposal of any device that has work data stored on it and in the event of a user leaving the council councillor staff and other authorised users are required to allow the chair or clerk access to the device to ensure that all passwords user access shortcuts and any identifiable data are removed from the device.

3.10 Councillors, staff and other authorised users must take responsibility for understanding how their devices work in respect to the above rules if they are accessing council information via their own equipment.

4 Health and Safety

4.1 Councillors, staff and other authorised users should ensure that their home workstations and equipment are sufficient to their needs. The HSE has provided a guide which is helpful for home assessment. Display screen equipment (DSE) workstation checklist.

4.2 Any changes, or additional equipment needs should be discussed with the council.

5 Password and Authentication

5.1 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.

5.2 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

5.3 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 leaving), 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 with a copy provided to the chair of Council, in a sealed envelope, only to be accessed in an emergency.

5.4 Password Storage and Management

- Passwords must not be stored in plain text or written down in insecure locations.

- Immediately change password if compromise is suspected.
- Attempts to access unauthorised passwords will be treated as a security incident.
- Users are responsible for creating and maintaining secure passwords for their accounts.

6 Monitoring and Investigation

6.1 The council reserves the right to monitor computer usage and inspect any files stored on its computers or council data held on personal computers to ensure compliance with this policy as well as relevant legislation.

6.2 The council has the right to monitor the use of electronic communications and the use of the internet in line with the Investigatory Powers (Interception by councils etc for Monitoring and Record Keeping Purposes Regulations) 2018

6.3 Monitoring of any employees' e-mail and or Internet use will be conducted in accordance with an impact assessment that the council has carried out to ensure that monitoring is necessary and proportionate. Monitoring is in the council's legitimate interests and is to ensure that this policy is being complied with.

6.4 The information obtained through monitoring may be shared internally with relevant councillors. The information may also be shared with external HR or legal advisors for the purposes of seeking professional advice any external advisors will have appropriate data protection policies and protocols in place.

6.5 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

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

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

7 Remote working

7.1 Increased IT security measures apply to those who are working away from their normal place of work (eg home office).

- If 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 deleing all logs and history records within the browser used. If the configuration of the device does not clearly support these actions, council documents 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.
- Papers files or computer equipment must not be left unattended.

- 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.

8 Email

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

8.2 On occasion, it would be quicker to action an issue by telephone or face to face rather than via protracted e-mail chains. E-mail 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.

8.3 These rules are designed to minimise the legal risks run when using e-mail 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 clerk rather than assuming they know the right answer.

8.4 All councillors, staff and other authorised users, who need to use e-mail as part of their role may be given their own council e-mail addresses. The council may at any time withdraw e-mail access should it feel that this is no longer necessary for the role or that the system is being abused.

8.5 E-mail messages sent using the council's email address are for council use only personal use is not permitted.

8.6 E-mail accounts should be regularly reviewed by users and any personal or sensitive information (such as in the case of recruitment, disciplinary action or dismissal) deleted once the purpose for which it was kept is no longer relevant.

9 Use of the Internet

9.1 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.

9.2 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.

9.3 Usually, a website will contain copyright conditions; these warnings should be read before downloading or copying. Copyright and database rights law can be complicated. Councillors staff and other authorised users should check with the clerk if unsure about anything.

9.4 The council does not permit the registration of any new domain names or trademarks relating to council names anywhere in the world, unless authorised to do so. Links from any of the councils' web pages should not be added to any other external sites without checking with the clerk first. Special rules apply to the processing of personal and sensitive personal data. For further guidance on this see the council's data protection policy.

9.5 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, some of the information may be less accurate than it appears.

10 Use of social media

10.1 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, 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.

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

10.3 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 others could be regarded as abusive, humiliating, racist,homophobic, 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 residents or other local organisation may read councillors, staff and other authorised users personal web logs 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.

10.4 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.

- Contacts from any of the councils' databases should not be downloaded and connected with on LinkedIn or other social networking sites with electronic addresses or 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 residents, 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 'comments and other content on this site are my own and do not represent the position or opinion of Chelmarsh Parish Council) writers must not claim or give the impression that they are speaking on behalf of the council.
- Any employee or councillor developing a site, or writing a blog that will mention the council, must inform the council 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 staff and council members and not to engage in any name calling or behaviour that will reflect negatively on its reputation, Any unauthorised used copyright materials, any unfounded or derogatory statements or any misrepresentation is not viewed favourably and could constitute gross misconduct.
- 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 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 persons might be considered a breach of data protection and a breach of privacy and confidentiality. 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 or other authorised users, anything to do with a disciplinary case, grievance allegation of bullying or harassment or discrimination, or legal issue, or any other 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 any other authorised users must be aware that they are personally liable for anything that they write or present online, including on an online forum, 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, racist, homophobic, 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, racist, harassing, libellous or creating a hostile work environment. Other councillors, staff or 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. They should not 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 of council.
- 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 social media networking sites for council development purposes must ensure they provide the council with login details including passwords 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 or other authorised users 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.

10.5 The council may from time to time monitor external postings on social media sites. Any employee who has a profile on social media must not misrepresent themselves or their role within 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.

10.6 Contact details and information gathered during employment / involvement with the council remain the property of the council. Councillors, staff and other authorised users leaving the council will be required to delete all council related data including contact details from any personal device.

11 Misuse

11.1 Misuse of IT equipment is not in line with the council's standards of conduct and will be taken seriously.

Nash Parish Council
c/o Nash Village Hall, Clee Hill Rd, Nash, Ludlow SY8 3AL
www.nashpc.org.uk