Biddulph Town Council

INFORMATION TECHNOLOGY POLICY

WRITTEN BY:
Sarah Haydon

NEW POLICY:
January 2026

APPROVAL DATE:
Finance Strategy & Management Committee – 16 February 2026

Town Council – 10 March 2026

REVIEW DATE:
January 2027

INTRODUCTION
1.1 Biddulph Town Council has a duty to ensure the proper security and privacy of its computer systems and data. All users have some responsibility for protecting these assets.

1.2 The Chief Officer is responsible for the implementation and monitoring of this policy but may delegate that responsibility to another officer.

1.3 The Town Council will make available devices that can access emails and documents for meetings, if a councillor does not have a suitable personal device.

OBJECTIVES OF THE POLICY
2.1 This policy sets out how the council manages its Information Technology (IT) and Cyber Security.

2.2 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.

SCOPE OF THIS POLICY

3.1 This policy applies to all councillors, staff, and other authorised users, regardless of their working location or pattern. It sets out the expectations for the appropriate use of IT equipment and systems. .

GENERAL PRINCIPLES

4.1 All councillors and employees will be assigned a council email address.

4.2 All councillors, employees, and other authorised users should be aware of the increasingly sophisticated scams and risks posed to cybersecurity and when in doubt should seek guidance from the Chief Officer. As a general rule, users will never be asked to share passwords by email and users should be aware of odd language used in emails which may indicate a fraudulent email.

4.3 All councillors, employees and other users of IT equipment must be familiar with and abide by the regulations set out in the council's 'Data Protection (GDPR) and Retention Policy'.

4.4 All council devices will have up-to-date antivirus software installed and this must not be switched off for any reason without the authorisation of the Chief Officer. Personal devices should have up-to-date antivirus software installed.

4.5 All users are reminded that deliberate unauthorised use, alteration, or interference with computer systems, software or data is a breach of this policy and in some circumstances may be a criminal offence under the Computer Misuse Act 1990.

4.6 All software installed on council devices must be fully licensed and no software should be installed without authorisation from the Chief Officer.

TRAINING AND GUIDANCE

5.1 Employees and volunteers will be provided with regular cybersecurity training as is appropriate for their role and level of systems access.

5.2 Councillors will be provided with a brief overview of cybersecurity measures as part of their induction and may be provided with more in-depth training as required.

MONITORING

6.1 The council reserves the right to monitor all activity on company devices. This includes monitoring of clocking in and out, email activity and internet usage for the purposes of ensuring compliance with our policies and procedures and of ensuring compliance with the relevant regulatory requirements. Information acquired through such monitoring may be used as evidence in disciplinary proceedings. Monitoring usage will mean processing personal data.

6.2 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.

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

6.4 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 concluded.

6.5 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.

6.6 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.

6.7 The council reserves the right to inspect all files stored on its computer systems in order to assure compliance with this policy. The council also reserves the right to monitor the types of sites being accessed and the extent and frequency of use of the internet at any time, both inside and outside of

working hours to ensure that the system is not being abused and to protect the council from potential damage or disrepute.

6.8 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.

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

HARDWARE

7.1 Council computer equipment is provided for council purposes only.

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

7.3 All computer and other electronic equipment 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.

7.4 Computer and electronic hardware should be kept clean, and every precaution taken to prevent food and drink being dropped or spilled onto it. Do not use water to clean a computer or phone. Store devices in a dry place. Ensure the air vents on your device can't overheat, you can do this by using a cloth or compressed air cleaner. Avoid extreme temperatures – ensure IT devices are not left in direct sunlight or outside. Ensure cords are stored suitably and keep the devices away from young children and pets. Make sure you shut down properly when you finish using the computer. This will help the battery last longer and prevent overheating. Keep your laptop on a stable surface to prevent damage by falls, etc. Clean your device by using a soft microfibre cloth and/or compressed air. You do not need to use any chemicals or wipes.

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

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

7.7 Personal disks, USB sticks, CDs, DVDs, data storage devices etc cannot be used on council computers without the prior approval of the Chief Officer.

7.8 The council has a wireless network. Using a portable device to make personal Wi-Fi hot spots which bypass existing Wi-Fi is not allowed.

7.9 Any faults or necessary repairs must be reported to the Chief Officer.

EQUIPMENT

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

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

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

8.4 It is important to ensure all portable devices are protected with encryption in case they are lost or stolen. All council-provided smartphones or tablets that hold council data, including emails and files, should be protected with a pin code. 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 two factor authentication is preferable, it significantly reduces the risk of unauthorised access to systems and sensitive data. Any security set on these devices must not be disenabled or removed

8.5 If an item or portable equipment is lost or damaged this should be reported to the Chief Officer. If the loss or damage is due to an act of negligence, the individual responsible may be liable to meet the cost of the loss/damage.

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

Officer. This includes mobile telephones with camera function, camcorder, tape or other recording device for sound or pictures – moving or still.

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

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

USE OF OWN DEVICES

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

9.2 The council recognises that some councillors may wish to use their own smartphones, tablets, laptops, etc to access our server or networks for normal council purposes, including, but not limited to, reading their emails, accessing documents stored on the council's network or to store data on the council's server 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, etc) 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. Employees must always use council-provided equipment – use of their own personal devices is not permitted.

9.3 Calls made to external parties must be made on council landlines or council-provided mobile phone numbers to ensure that only these numbers are used and/or stored by the recipient, rather than personal numbers.

9.4 Councillors, employees, 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.

9.5 In cases of legal proceedings against the council the council may need to temporarily take possession of a device to retrieve the relevant data.

9.6 Councillors who use their own devices via the council's infrastructure must ensure that they:

- Use a strong password to protect their device(s) from being accessed. For smartphones and tablets this should lock the device after a number of failed login attempts.
- Configure their device(s) to automatically prompt for a password after a period of inactivity.
- Always password protect any documents containing confidential information that are sent as attachments to an email, and notify the password separately.
- For smartphones and tablets, activate the automatic device wipe function (where applicable). Note that use of the remote wipe function may also involve the removal of the individual's personal data. Councillors are therefore advised to keep personal data separate from council data where possible;
- 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 Chief Officer if their device(s) is/are lost, stolen, or inappropriately accessed where there is risk of access to council data or resources. To prevent phones being used, they will need to retain the details of their IMEI number and the SIM number of their device as their provider will require this to deactivate it.

9.7 Personal data relating to councillors, employees, and other authorised users, associates, residents, external stakeholders, etc 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. This applies especially if the passwords used to store/access data are saved onto the device, or if the service permits councillors, staff, and other authorised users to remain logged in between sessions.

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

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

9.10 Councillors, employees, and other authorised users who open any 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(s) is lost, stolen, or used without the owner's permission.

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

9.12 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, employees, and other authorised users are required to allow the council's IT provider access to the device to ensure that all passwords, user access shortcuts and any identifiable data are removed from the device.

9.13 Councillors must take responsibility for understanding how their device(s) work in respect of the above rules if they are accessing council servicers/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 rending a device inoperable. The council will use reasonable endeavours to assist, but councillors are personally liable for their own device(s) and for any costs incurred as a result of the above.

HEALTH AND SAFETY

10.1 Employees and other authorised users will be provided with an appropriate workstation.

10.2 The council has a duty to ensure that regular appropriate eye tests, carried out by a competent person, are offered to employees using display screen equipment. Further details are set out in the council's 'Health and Safety and Wellbeing at Work Policy.'

10.3 Any VDU user who feels that their workstation requires changes to make it compliant must speak to the Chief Officer.

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

PASSWORD AND AUTHENTICATION POLICY

11.1 All user accounts must be protected by strong, secure passwords. 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 are generated by the council's IT provider.
- Default passwords provided by vendors or the council's IT provider must be changed immediately upon installation or setup.

11.2 Passwords are personal and must not be shared under any circumstances.

11.3 Only the assigned user of an account may access or use the associated password.

11.4 In exceptional circumstances (eg incident response or employee offboarding), access to system credentials may be granted to authorised personnel from the council's IT provider.

11.5 Administrative credentials must be stored securely and only accessible to authorised personnel.

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

11.7 Immediately change a password if compromise is suspected.

11.8 All access to administrative or shared credentials must be logged and auditable.

11.9 Attempts to access unauthorised passwords will be treated as a security incident.

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

11.11 The council's IT security provider is responsible for managing system/service credentials, enforcing password policies, and auditing and monitoring password-related security practices.

REMOTE WORKING

12.1 Increased IT security measures apply to those who work away from their normal place of work (eg whilst travelling, working from home, etc), 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 a premises unless arrangements have been made with a responsible person at a 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, employees, 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.

EMAIL

13.1 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, employees, 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.

13.2 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.

13.3 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 the policy, councillors, employees, and other authorised users should ask the Chief Officer, rather than assuming they know the right answer.

13.4 All councillors, employees, and other authorised users who need to use email as part of their role will 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.

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

13.6 If you think that someone else may have accessed or be able to access your email account, advise the Chief Officer.

13.7 If you have accidentally sent personal data to someone who does not have a legitimate reason to hold this, contact the Chief Officer, as this may need to be reported to the Information Commissioners Officers.

13.8 Councillor email addresses will be provided on the Biddulph Town Council website. We ask that you check your emails regularly and provide a response within 7 days of an email. You can set up an auto-response for when you are away.

13.9 Please use the council's standard email signature.

13.10 You are responsible for taking all reasonable precautions to keep your email secure, and any devices safe, secure and in good working order.

From the Social Media Press and Public Communication Policy:

EMAIL AND LETTER COMMUNICATION

23.1 Many of the same principles outlined in the above sections are applicable to email and letter communication, however, there are a few additional points which relate specifically to this form of communication:

- Official correspondence regarding Town Council matters must be provided on either Town Council letterhead or a Town Council email address.
- Town Council letterhead or emails must not be used for any communication which is not authorised by the Town Council: Emails and letters to the public, press or external companies which relate to Town Council matters but are not official Town Council communication, must make clear that the matter is a personal communication only.
  Emails or letters from councillors or officers must never be sent anonymously or under a pseudonym.
- For Town Council matters, councillors must not use an officers personal email or postal address unless specifically directed otherwise (for instance in the event of a town hall closure or email outage, and only at the Chief Officer's direction or as directed by the Emergency Plan / Business Continuity Plan.)
- Any confidential information on emails or letters must be appropriately encrypted, refer to the GDPR policy regarding this matter.'

From the Data Protection (GDPR) and Retention Policy:

ACCEPTABLE USE OF PERSONAL DEVICES AND EMAIL ACCOUNTS

9.1 Despite the problems associated with personal devices, at present some use is unavoidable. Therefore personal devices and email for council business should only be used where there is no reasonable alternative option, and only when sufficient measures are in place to manage the risk. All Town Councillors are provided with a Town Council email address. This should be used for all Town Council business.

9.2 All personal devices used for council business must be pin and passcode secured and have a facility to remotely wipe data. They must only be used on Wi-Fi networks with an appropriate level of security.

9.3 No personal information should be sent to personal email addresses or downloaded on to personal devices. Anonymising or removing the personal information from an email or attachment may allow the information to be shared in a low risk way. The personal information, if needed and adheres to the principles outlined in the GDPR, may then be provided over the phone, thus preventing the physical storage or retention of such information.

9.4 Where the downloading or retaining of information on a personal device or the sending of personal information to a personal email account, is unavoidable, the following must be adhered to:

- Only the minimum and least identifiable method of sharing the information should be given (for instance using initials rather than a full name).
- Documents must be appropriately encrypted and password protected. The password for the information must not be sent via email, but rather provided over the phone. A text message may be acceptable if the email is not accessible from that phone.
- Any email that includes personal information must contain a statement that informs the user that personal information is contained within, and must only be used for the intended purposes and deleted immediately when the information is no longer required.
- The receiver of the email must have previously agreed to receive this information and handle in accordance with the IT Acceptable Use Agreement (which includes deleting the information as soon as possible).

9.5 Where a person becomes aware of a privacy breach on a network, device or email account that contains information relating to council business, they must inform the Chief Officer immediately so appropriate remedial action and reporting can take place. This includes reporting where an email is hacked, phishing software located or where a device is lost or stolen.

9.6 As per the IT acceptable use agreement, emails to Biddulph Town Council email addresses must not routinely be forwarded to any other personal or organisational email addresses held by the same councillor, other than in exceptional circumstances and only where the measures in place under section

9.4 are adhered to. This means that it is not permissible to put an auto-forward on for emails to be automatically sent to a personal, business, district council or county council email address.'

USE OF THE INTERNET

14.1 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.

14.2 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.

14.3 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).

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

14.5 Copyright and database right law can be complicated. Councillors, employees, and other authorised users should check with the Chief Officer if they are unsure about anything.

14.6 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 Chief Officer.

14.7 Special rules apply to the processing of personal and sensitive personal data. For further guidance on this, see the council's 'Data Protection (GDPR) and Retention Policy.'

14.8 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

15.1 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.

15.2 Personal use of social networking/media and chat sites are not permitted during working hours, unless as part of the employees role.

15.3 The council recognises the importance of councillors, employees, 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 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, employees, and other authorised users should be aware that residents or other local organisations may read councillors, employees, and other authorised users' personal weblogs, 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.

15.4 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 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, 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 view 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 (eg 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, employees, and other authorised users, partners, must inform the Chief Officer that they are writing this and gain agreement before going 'live'.
- The council expects councillors, employees, and other authorised users to be respectful about the council 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, employees 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, employees, and other authorised persons, 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, employees, and other authorised users anything to do with a disciplinary case, grievance, allegation of bullying/harassment or discrimination, or legal issue; any other secret, confidential, or propriety 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, employees, 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, libelous, 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, libelous or creating a hostile work environment. In addition, other councillors, employees, 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 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 Chief Officer.
- Councillors, employees, 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, employees, 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, employees, and other authorised users who have left the council must not post any inappropriate comments about the council or its councillors, employees, and other authorised uers 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, employee or other authorised user. All such contacts will be considered council property and may be subject to disclosure upon request.

15.5 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, employees, 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.

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

MISUSE

16.1 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.

HELP OR SUPPORT

17.1 If you are having difficulties accessing or using your email, you can call the council's IT provider (Prism Solutions) on 0345 121 7770.

RELATED POLICIES

18.1 This policy should be read alongside the Town Council's:

- Health and Safety and Wellbeing at Work Policy
- Code of Conduct for Members

- Employee Code of Conduct
- Data Protection (GDPR) and Retention Policy
- Social Media, Press and Public Communication Policy
- Councillors Handbook
- General Privacy Notice for Staff, Councillors and Role Holders
- General Privacy Notice for Members of the Public
- Publication Scheme and Guidance

For info: The current 'Councillor Email and IT Use Guidance' document will be archived. All the information contained within it is contained within this new 'Information Technology Policy.'