Eyam Parish Council
Email: eyamparishcouncil@gmail.com
Website: www.eyamparishcouncil.com

IT and Social Media Policy

Contents

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 staff, Councillors 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.

1. Computer use

1.1 Hardware

1.1.1 Council computers and devices will be provided for Council purposes only.

1.1.2 Council computers and devices should be locked when left unattended to prevent unauthorised access.

1.1.3 All Council computers and devices should be password protected and be configured to automatically prompt for a password after a period of inactivity.

1.1.4 Multi-Factor Authentication should be used for all Council email and software accounts used by Councillors, staff and authorised users.

1.1.5 Council computers and other devices should be treated with good care at all times.

1.1.6 Council computers and devices should be kept clean, and every precaution taken to prevent damage by food, drink and spillages.

1.1.7 All Council computers and electronic devices will be listed on the Council's Asset Register.

1.1.8 Equipment should not be dismantled or reassembled without seeking professional advice.

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

1.1.10 Personal disks, USB sticks, CDs, DVDs and other data storage devices are not to be used on Council computers. without the prior approval of the Clerk.

1.1.11 Staff, Councillors and authorised users should always use a secure and private network when using Council computers or devices to access the internet or online services.

1.1.12 Any faults or damages to Council computers or devices should be reported to the Clerk as soon as possible.

1.1.13 Councillors, staff, and other authorised persons that use Council Computers and devices must do so in an ethical and respectful manner and in accordance with this policy. Accessing inappropriate, illegal or offensive content on any device or 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.

2. Equipment

2.1 Portable devices

2.1.1 Portable devices include the use of laptop computers, tablets and mobile phones which have email capability and access to the internet used for Council purposes.

2.1.2 All portable devices must be kept safe and secure when not in use. Portable equipment should not be left unattended and should never be left in parked vehicles or at or non-Council premises or workspaces.

2.1.3 All portable devices should have Multi-Factor Authentication when accessing Council email and software accounts.

2.1.4 Any faults or damages to Council owned portable devices should be reported to the Clerk as soon as possible.

2.1.5 Photographs or videos taken by staff or Councillors, using a portable device on Council premises, must have the permission of the Clerk and/or person(s) being recorded.

2.1.6 Under no circumstances should any non-public meeting or conversation be recorded using a portable device without the permission of those present. This does not affect statutory rights under The Openness of Local Government Regulations 2014.

2.1.7 The Council does not permit staff or Councillor to use webcams in the workplace, other than for remote meetings, conference calls or other official Council business.

2.1.8 If transferring data by email or by other means, this should be done through a secure or private network.

2.1.9 Councillors, staff, and other authorised users who open any email attachments should ensure that any cached copies are deleted immediately after use.

2.1.10 Prior to the disposal of any Council computer or device, and in the event of a user leaving the Council, the Clerk is to be given access the device to ensure that all Council data and documents are removed.

2.2 Use of personal devices

2.2.1 Staff must not use personal laptops and portable devices for work purposes or connect them to the Council's private wireless network.

2.2.2 Staff should not transfer nor store Council documents and files on a personal computer or portable device. Personal computers and portable devices should not be used to access data on the Council's cloud storage.

2.2.3 When sending work emails, staff should use a Council email account, using a Council computer or device only. Work emails should not be sent from personal devices.

2.2.4 In cases of legal proceedings against a member of staff or a Councillor(s), personal computers and devices may need to be temporarily taken possession of.

2.2.5 Wherever possible those using a personal computer or device should maintain a clear separation between the personal data processed on the Council's behalf and that processed for their own personal use.

2.2.6 Councillors and other authorised users who use a personal device for Council business must ensure that they:

- password protect their device(s).
- configure their device(s) to automatically prompt for a password after a period of inactivity.
- password protect any documents containing confidential information that are sent as attachments to an email and notify of the password separately.

- Councillors and other authorised users should keep personal data separate from Council data where possible.
- always use a secure or private network.
- ensure that confidential 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 and where there is a risk of a data breach.

2.2.7 Personal information and sensitive data should not be saved or processed on any personal computers, accounts or cloud services.

2.2.8 If transferring data using personal removable media (e.g. USB drives or CDs), the data on the media must be deleted immediately, once the transfer is complete.

2.2.9 Councillors and other authorised users must take responsibility for understanding how their personal device(s) works in respect to the above rules when accessing Council servers/services via their own IT equipment.

2.2.10 Councillors and other authorised users are personally liable for their own device(s) and for any costs incurred because of data loss or damage from viruses or hardware failures.

2.2.11 Councillors and other authorised persons that use personal computers and devices must do so in an ethical and respectful manner and in accordance with this policy. Accessing inappropriate, illegal or offensive content on any device or 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.

3. Health and safety

3.1.1 Councillors, staff, and other authorised users who work in Council offices will be provided with an appropriate workstation.

3.1.2 Any staff, Councillors or authorised user who feel that their workstation requires changes to make it compliant must speak to the Clerk.

3.1.3 Any hazards detected at a workstation should be reported immediately to the Clerk.

3.1.4 The Council has a duty to ensure that appropriate eye tests, carried out by a competent person, are offered to employees using display screen equipment and this is recommended every 2 years, or sooner if advised. The employer can either arrange a test directly or offer reimbursement for a test arranged by the employee.

4. Password and Authentication Policy

4.1.1 All Council software and email accounts must be protected by strong, secure passwords. Multi-Factor Authentication should be enabled wherever possible.

4.1.2 Passwords must not be shared under any circumstances and only the assigned user of an account may access or use the associated password. In exceptional cases (e.g., incident response), access to system credentials may be granted to authorised personnel.

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

4.1.4 Passwords must be changed immediately if compromise is suspected.

4.1.5 Attempts to access unauthorized passwords will be treated as a security incident.

4.1.6 A hard copy of administrative credentials must be stored securely and only accessible to authorised personnel with a copy accessible to the Chair of Council, in a sealed envelope, only to be accessed in an emergency.

5. Monitoring

5.1.1 The Council reserves the right to monitor and maintain logs of computer usage and inspect any files stored on its network, servers, computers, or associated technology to ensure compliance with this policy as well as relevant legislation. Internet, work email, and Council computer usage may be monitored as part of the Council's protection against computer viruses, ongoing maintenance of the system and when investigating faults.

5.1.2 The Council will monitor the use of electronic communications and use of the internet in line with the Regulation of Investigatory Powers Act 2000 (RIPA) and Investigatory Powers Act (IPA) 2016.

5.1.3 Monitoring of an employee's work email 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.

5.1.4 The information obtained through monitoring may be shared internally, including with relevant Councillors and IT staff if access to the data is necessary for 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.

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 Councillors, staff, 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.

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 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.

5.1.9 Any use that the Council considers to be 'improper' either in terms of the content or the amount of time spent on this, may result in disciplinary proceedings.

5.1.10 All computers may be periodically checked and scanned for unauthorised programmes and viruses.

6. Remote working

6.1.1 The following steps should be taken to reduce risk when working remotely or away from their normal place of work:

- staff should only use a Council computer or portable device when logging into the Council's systems or services.
- the location and direction of a computer screen should be checked to ensure confidential information is out of view.
- any data that has been printed should be collected and stored securely or destroyed.
- all electronic files should be password protected and all data saved to the Council's system/services when accessible.
- papers, files or computer equipment must never not be left unattended.
- data sticks/storage, flash drive or backup hard drives should not be left unattended and always password protected.
- A secure or private network should always be used when accessing the internet and online accounts.

6.1.2 The Council will not cover costs for the use of a 'dongle' or paid for Wi-Fi.

7. Email

7.1.1 All Councillors and staff will be provided with a Council email address or shall use a personal email address that is to be used for Council business only.

7.1.2 Email messages sent on the Council's account are for Council business use only. Personal use is not permitted.

7.1.3 The Council may, at any time, withdraw email access, should it feel that this is no longer necessary for the role or should the user cease to be a Councillor or staff member.

8. 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, as set out in The Copyright, Designs and Patents Act 1988.

8.1.2 Copyright conditions on websites, documents and other online materials should be read before downloading or copying.

8.1.3 Councillors, staff, and other authorised users who are unsure about what information can be copied or downloaded should check with the Clerk.

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.

8.2.2 Links from any pages on the Council's website to any other external sites will require the permission of the Clerk.

8.3 Accuracy of information

8.3.1 Staff, Councillors and authorised users should ensure all information taken from websites and online sources is accurate, reliable and up to date.

9. Use of social media

9.1.1 Staff, Councillors and authorised users are personally responsible for any information or content posted online through social networking sites, blogs or other forms of social media.

9.1.2 Personal use of social media networking sites by staff is not permitted during working hours.

9.1.3 Inappropriate comments, postings and photographs, on Council or personal social media that could reasonably be interpreted as being associated with the Council, or if remarks about any individual or groups could be regarded as abusive, offensive, humiliating, sexual harassment, discriminatory or derogatory, or could constitute bullying or harassment, could result in disciplinary action.

9.1.4 To protect both the Council and its interests, staff and Councillors are 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/or used on any social networking sites.
- Any online post that expresses a view about the Council, its work, Councillors, employees, other users associated with the Council, partner organisations, local groups, suppliers or parishioners, must state that the views expressed are theirs alone and do not represent the views of the Parish Council.
- Any employee who is developing a site or writing a blog that will mention the Council, 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, Councillors and staff and not to engage in any name calling or any behaviour that will reflect negatively on its reputation.
- 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 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 and posted online without explicit permission.
- Comments posted on any sites should be factual, accurate and professional and should not compromise the Council in any way.
- Inappropriate conversations with a parishioner, contractors or stakeholders should not take place on any social media or networking sites.
- 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. 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 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 and staff, 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 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 employment/involvement with the Council, staff and Councillors 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 another 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 formally through the Grievance Procedure.

9.1.6 It is important to note that contact details and information collected through Council business 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 contact details from any personal device/equipment.

Misuse

Misuse of Council computers, IT systems and equipment that 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.