EAST GOSCOTE PARISH COUNCIL

DIGITAL USE AND COMMUNICATIONS (IT) POLICY

Approved by: Full Council	**Date:** 16.2.26
Last reviewed: 22.9.25	
Next review due: February 2027	

Information Technology Policy

Purpose of the IT Policy

The purpose of an IT policy is to establish clear parameters for how councillors, staff, and other authorised users use council-provided technology or equipment in the course of their duties. A well-defined policy helps to:

- Set expectations for appropriate use of equipment and systems;
- Raise awareness of risks associated with IT use;
- Safeguard the council's data and digital assets;
- Clarify what constitutes acceptable and unacceptable use;
- Outline the consequences of policy breaches.

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 expectations for the appropriate use of IT equipment and systems provided by East Goscote Parish Council.

1. Computer use and Hardware

1.1.1 Computer equipment is provided for council purposes; however reasonable personal use is permitted (reasonably interpreted as in the opinion of the Clerk). Any personal use of our computers and systems should not interrupt daily council work in any way. Councillors, staff, and other authorised users are asked to restrict any personal use to outside working hours.

1.1.2 All councillors, staff, and other authorised users must ensure devices auto-lock after inactivity (**5 minutes for mobile equipment**, **10 minutes for desktops)** to avoid unauthorised access. This applies to all council and personal devices used for work. Failure to comply may lead to disciplinary action.

1.1.3 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 any equipment will have a financial impact on the council.

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

1.1.5 All computer and mobile equipment will be logged against the current owner of that equipment. A database of equipment issued will be kept.

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

1.1.7 Councillors, staff, and other authorised users must not purchase any computer or mobile equipment (including software), on behalf of the council, unless previously authorised.

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

1.1.9 Any faults or necessary repairs must be reported to the Clerk.

2. Equipment

2.1 Portable Equipment

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

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

2.1.3 All portable computers must be stored safely and securely when not in use in the office, i.e. when travelling or when working from home. Portable equipment should not be left unattended when away from council premises and should never be left in parked vehicles.

2.1.4 It is important to ensure all portable devices are protected with encryption in case they are lost or stolen. All smartphones or tablets that hold council data, including emails and files, must be protected with a pin code. Where possible, these devices should also be programmed to erase all content after several unsuccessful attempts to break in. Any security set on these devices must not be disenabled or removed.

2.1.5 Multi-Factor Authentication (MFA) is a security process that requires users to verify their identity using two or more independent methods, for example, entering a password (something you know) and confirming a code sent to your mobile device (something you have). This significantly reduces the risk of unauthorised access to systems and sensitive data. NALC recommends implementing MFA as a best practice to enhance information security and support compliance with data protection obligations under the UK GDPR and the Data Protection Act 2018.

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

2.1.7 To protect confidential information, unless it is a requirement of the job and this has been authorised, it is forbidden for photographs or videos to be taken on council premises, without the prior permission of the Clerk. This includes mobile telephones with camera function, camcorder, tape or other recording device for sound or pictures - moving or still.

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

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

2.2 Use of own devices

2.2.1 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 reading their emails and accessing documents. 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.

2.2.2 However, the same security precautions apply to personal devices as to the council issued devices. Any emails sent from own devices should be sent from a council email account and should not identify the individual's personal email address.

2.2.3 Councillors, staff, and other authorised users 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.

2.2.4 In cases of legal proceedings against EGPC, the council may need to temporarily take possession of a device, whether council-owned or personal, to retrieve the relevant data.

2.2.5 Wherever possible the user should maintain a clear separation between the personal data processed on the council's behalf and that processed for their own personal use, for example, by using different apps for council and personal use. If the device supports both work and personal profiles, the work profile must always be used for work-related purposes.

2.2.6 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 (i.e. one which uses three random words (e.g. PurpleCandleRiver), a strong 6-digit pin, fingerprint ID, or face ID) to protect their device(s) from being accessed.
- configure their device(s) to automatically prompt for a password after a period of inactivity of more than 5 minutes.

- always password protect any documents containing confidential information that are sent as attachments to an email and notify the password separately (preferably by a means other than email).
- for smartphones and tablets, activate the automatic device wipe function (where available). Note that use of the remote wipe function may also involve the removal of the individual's personal data. Councillors, staff, and other authorised users are therefore advised to keep personal data separate from council data where possible.
- ensure secure 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 risk of access to council data or resources. To prevent phones being used, they will need to retain the details of their IMEI number and the SIM number of the device as their provider will require this to deactivate it.

2.2.7 Any work done on 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.

2.2.8 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 ensure that all passwords, user access shortcuts and any identifiable data are removed from the device.

2.2.9 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.

2.3 Leaving the Parish Council

2.3.1 If a Councillor ceases to be a member of the Council for any reason:
- all Personal Data received in the course of Council Business must be permanently deleted from Devices and from any email account used for Council Business; and
- All hard copies should be shredded or passed to the Clerk for destruction
- Councillors must return devices issued by the Council immediately

2.3.2 On the termination of employees' employment by the Council:
- employees must return Devices issued by the Council immediately;
- and all Personal Data or other information received in the course of Council Business must be permanently deleted from personally owned Devices.

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 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 Policy.

3.1.3 Any VDU user who feels that their workstation requires changes to make it compliant must speak to the Clerk.

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

4. Password and Authentication Policy

4.1.1 All user accounts must be protected by strong, secure passwords. The council follows the National Cyber Security Centre (NCSC) recommendations for creating passwords using three random words (e.g. PurpleCandleRiver). This method helps create passwords that are both strong and easy to remember, while offering effective protection against common cyber threats such as brute-force attacks. This approach is endorsed in NALC guidance.

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

To further strengthen account security:

- 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.

4.1.2 Access to Passwords

- Passwords are personal and must not be shared under any circumstances.
- Only the assigned user of an account may access or use the associated password.
- In exceptional cases (e.g., incident response or employee offboarding), access to system credentials may be granted to 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 the Council, in a sealed envelope, only to be accessed in an emergency.

4.1.3 Password Storage and Management

- Passwords must not be stored in plain text or written down in insecure locations.
- Passwords must be stored using Bitwarden, a council-approved, encrypted password manager.

4.1.4 Password Change Requirements

- Immediately change password if compromise is suspected.

4.1.5 Password Access Control and Logging

- All access to administrative or shared credentials must be logged and auditable.
- Attempts to access unauthorized passwords will be treated as a security incident.

4.1.6 Responsibility

- 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.

5. Monitoring (Council Issued Devices)

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, email, and computer usage is continually monitored as part of the council's protection against computer viruses, ongoing maintenance of the system, and when investigating faults.

5.1.5 The council will monitor the use of electronic communications and use of the internet if deemed necessary, in line with the Investigatory Powers (Interception by Councils etc. for Monitoring and Record-keeping Purposes) Regulations 2018.

5.1.6 Monitoring of an employee's 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. Monitoring is in the council's legitimate interests and is to ensure that this policy is being complied with.

5.1.7 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 purpose of seeking professional advice. Any external advisers will have appropriate data protection policies and protocols in place.

5.1.8 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.

5.1.9 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. You can find further details of these rights and how to exercise them in the council's data protection policy.

5.1.10 Such monitoring and the retrieval of the content of any messages may be for the purpose 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.

5.1.11 The council reserves the right to inspect all files stored on its computer systems in order to ensure 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.

5.1.12 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.

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

6. 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), 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;
- confidential papers, files or computer equipment must not be left unattended at a non-council premises unless arrangements have been made for them to be kept in a locked room or cabinet;
- 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.

7. 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 deal with 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 Clerk 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. Personal emails should not be used, and users should be aware that they are subject to Freedom of Information requests/subject access requests, if they relate to Council business or an individual and it is a criminal offence to block the release of data

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

7.1.6 Do not forward email messages unless the original sender is aware that the message may be forwarded and that the whole email chain has been checked for appropriate content.

7.1.7 It is good practice to copy and paste information from an email to pass it on, rather than forwarding on an email, in order to remove the IP address from the header.

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. The Copyright, Designs and Patents Act 1988 set out the rules. The copyright laws not only apply to documents but also to software. The infringement of the copyright of another person or organisation could lead to legal action being taken against the council and damages being awarded, as well as disciplinary action, including dismissal being taken against the perpetrator.

8.1.2 It is easy to copy electronically, but this does not make it any less an offence. The council's policy is to comply with copyright laws, and not to bend the rules in any way.

8.1.3 Councillors, 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 contains 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 available on the council's 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.

9. 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 should be restricted to breaks 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 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 councillors, staff, 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.

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

- 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, 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 East Goscote Parish 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, (e.g. "our current or potential plans, councillors, staff, and other authorised users, 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, councillors, 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 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. 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 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 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 Only designated individuals (typically the Clerk or Deputy Clerk) may post or manage Council social media accounts or public statements and communications must be factual, neutral, and free from partisan or inflammatory language. Upon leaving the council, access to any pages will be securely transferred to another operator.

9.1.7 Council WhatsApp groups are for official communication only. Participation is voluntary, and members consent to the visibility of their name and phone number. Members agree to the following:

- Sensitive or unrelated information must not be shared.
- Group content must not be forwarded, screenshotted, or shared externally without consent.
- Members must respect privacy, maintain confidentiality, and avoid unnecessary tagging or messaging.
- Group administrators must moderate discussions, ensure compliance with data protection, manage membership, and address breaches or misuse.

10. Website Management

The council's website is an essential communication tool and must be managed in a way that ensures accuracy, security, accessibility, and compliance with all relevant legislation and best practice guidance, including NALC digital communications guidance, the UK GDPR, the Data Protection Act 2018, and the Public Sector Bodies (Websites and Mobile Applications) Accessibility Regulations 2018.

10.1 Governance and Responsibilities

10.1.1 The website is owned by East Goscote Parish Council. Strategic oversight rests with the Full Council, and day-to-day management is delegated to the Clerk.

10.1.2 Only councillors, staff, or contractors authorised by the Clerk may upload, amend, or remove website content. No other individuals may access the website's content management system.

10.1.3 The council's IT provider is responsible for maintaining secure hosting, applying updates, managing system credentials, and ensuring appropriate backup and recovery arrangements are in place.

10.1.4 All administrative credentials for the website must be stored securely in accordance with the council's Password and Authentication Policy.

10.2 Content Standards

10.2.1 All information published on the website must be accurate, factual, and approved by the Clerk. Content must be reviewed regularly to ensure it remains current.

10.2.2 Personal data must not be published unless there is a lawful basis for doing so and the Clerk has authorised its publication. The council must comply with the UK GDPR, the Data Protection Act 2018, and the council's Data Protection Policy.

10.2.3 Content must not include copyrighted material unless permission has been obtained. The Copyright, Designs and Patents Act 1988 applies to all online content.

10.2.4 The website must not be used for political purposes, campaigning, or any content that could breach pre-election (purdah) rules.

10.2.5 Only the latest approved version of any document (e.g., agendas, minutes, policies) may be published.

10.3 Accessibility Requirements

10.3.1 The council is committed to ensuring that its website meets the requirements of the Public Sector Bodies (Websites and Mobile Applications) Accessibility Regulations 2018.

10.3.2 The website must aim to comply with WCAG 2.2 AA standards. This includes providing text alternatives for images, ensuring readable formatting, and avoiding inaccessible PDFs where possible.

10.3.3 A current Accessibility Statement must be published on the website. It must accurately reflect the website's compliance status and include a method for users to report accessibility issues. The statement must be reviewed annually or when significant changes are made.

10.3.4 Any accessibility issues identified must be logged and addressed within reasonable timescales.

10.4 Security and Technical Management

10.4.1 Website administrative passwords must be generated and managed by the IT provider and stored securely using the council-approved password manager.

10.4.2 The IT provider must ensure that the content management system, plugins, themes, and associated components are kept up to date and free from known vulnerabilities.

10.4.3 Regular backups must be taken and stored securely. Restoration procedures must be tested periodically.

10.4.4 Any suspected security incident or data breach involving the website must be reported immediately to the Clerk and handled in accordance with the council's Data Breach Procedure.

10.5 Domain Names and External Links

10.5.1 No new domain names may be registered without the approval of the Clerk and Full Council.

10.5.2 External links must not be added to the council's website without the Clerk's approval. Links must be checked periodically to ensure they remain safe and appropriate.

10.6 Records Management

10.6.1 Documents published on the website must comply with the council's retention schedule and be removed when no longer required.

10.6.2 Superseded documents must be removed promptly to avoid confusion or misinformation.

11. AI Usage Policy

11.1.1. EGPC recognises the growing use of Artificial Intelligence (AI) tools for administrative efficiency. AI may be used for:

- Drafting or summarising documents
- Reviewing policies
- Preparing grant applications
- Generating meeting notes or templates
- Research support

11.1.2 Rules for AI Use

- AI must not be used to process or upload personal data unless approved and GDPR-compliant
- AI outputs must always be reviewed by a human
- AI must not be used to make decisions affecting individuals
- Confidential or sensitive information must not be entered into AI tools
- AI-generated content must be checked for accuracy, bias, and compliance
- Councillors and staff must declare when AI has been used to produce a document

11.1.3 Approved AI Tools

- Microsoft Copilot
- Canva Magic write
- ChatGPT
- Otter AI

12. 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.

13. Cyber Incident Response

The council is committed to responding promptly and effectively to any actual or suspected cyber incident to minimise disruption, protect data, and comply with legal obligations under the UK GDPR, the Data Protection Act 2018, and NALC best practice guidance. The council will investigate the use/need of Cyber insurance under the current insurance policy.

13.1 Definition of a Cyber Incident

For the purposes of this policy, a cyber incident includes (but is not limited to):

- unauthorised access to council systems, accounts, or data
- suspected or confirmed malware, ransomware, or virus infection
- loss or theft of devices containing council data
- attempted or successful phishing attacks
- accidental disclosure of personal or confidential information
- website compromise or unauthorised changes

- any activity that suggests a breach of security controls

13.2 Reporting Requirements

13.2.1 All councillors, staff, and authorised users must report any suspected or actual cyber incident **immediately** to the Clerk.

13.2.2 If the incident involves personal data, the Clerk will assess whether it constitutes a data breach and follows the council's Data Breach Procedure, including notifying the ICO where legally required.

13.2.3 Users must not attempt to investigate or fix the issue themselves unless instructed to do so by the Clerk or the IT provider.

13.3 Initial Containment

13.3.1 Upon notification, the Clerk will take reasonable steps to contain the incident, which may include:

- isolating affected devices
- suspending user accounts
- resetting passwords
- contacting the IT provider for urgent technical support

13.3.2 Users must follow any instructions given to prevent further damage or data loss.

13.4 Investigation and Recovery

13.4.1 The Clerk, supported by the IT provider where necessary, will investigate the incident to determine:

- the cause
- the extent of the impact
- whether personal data was compromised
- what remedial actions are required

13.4.2 Recovery actions may include restoring systems from backups, removing malware, or applying additional security controls.

13.5 Communication

13.5.1 The Clerk will determine what internal or external communication is required, including:

- notifying affected individuals where personal data is involved
- informing councillors where service disruption may occur
- liaising with external advisers where appropriate

13.5.2 No councillor, staff member, or authorised user may communicate publicly about a cyber incident unless authorised by the Clerk.

13.6 Review and Learning

13.6.1 Following resolution, the Clerk will review the incident to identify lessons learned and improvements to policies, procedures, or technical controls.

13.6.2 Any recommended changes will be reported to Full Council for approval where required.

14. Backup Procedures

14.1.1 The council is committed to protecting its digital information against loss, corruption, or system failure. Routine backups form part of the council's core information-security controls.

14.1.2 A full backup of council data is completed **monthly** using an **external hard drive** designated for this purpose. The backup device is stored securely when not in use and is only accessed by the Clerk or authorised personnel.

14.1.3 Following each monthly backup, the Clerk will confirm that the process has completed successfully and that the backup is accessible and readable.

14.1.4 Backup media must not be left unattended in vehicles or unsecured locations. When transported, it must be kept out of sight and stored securely at all times.

14.1.5 In the event of data loss or system failure, the monthly backup will be used to restore council data as required.

15. Training and Review

15.1.1 Councillors and staff will be offered training on:

- Data protection and GDPR
- Cybersecurity
- Communication protocols
- AI usage

15.1.2 The Clerk or Deputy Clerk is responsible for conducting an **annual review** of this policy and updating it as required.

A hard copy of this policy was received by:

L Pizer Signed ..... Date .....

C Turlington Signed ..... Date .....

Signed..... (Chair)

Date.....