**GNOSALL PARISH COUNCIL**
(Including the Wards of Moreton and Knightley)

**Chief Officer to the Council:**
Ms Jennifer Marshall
The Grosvenor Centre, High Street, Gnosall,
Stafford, ST20 0EX.
Booking Secretary: Michelle Farmer (CSO)

**Telephone:** 01785 822 685
**Email:**
chiefofficer@gnosallparishcouncil.gov.uk
cso@gnosallparishcouncil.gov.uk
**Website:** www.gnosallparishcouncil.gov.uk

# IT & CYBERSECURITY POLICY

| | |
|---|---|
| **Written:** | **February 2026** |
| **Formally adopted by Council:** | **March 2026** |
| **Review:** | **March 2027** |

*This document defines the Council's Information and Communications Technology (ICT) Policy.*

## *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.*

*All Staff and Councillors are responsible for the safety and security of Gnosall Parish Council's IT and email systems. By adhering to this IT and Email Policy, Gnosall Parish Council aims to create a secure and efficient IT environment that supports its mission and goals.*

# Contents

## PURPOSE OF THE IT POLICY

The purpose of this 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.

## 1. INTRODUCTION

1.1 Gnosall Parish Council has a duty laid down in the Data Protection Act 2018 and the General Data Protection Regulations, to ensure the proper security and privacy of its computer systems and data. All users have, to varying degrees, some responsibility for protecting these assets and complying with this policy.

1.2 The Council uses its computer, software packages and the internet (including websites, emails and social media), to further the efficiency of its business and to provide the best service possible to its customers, partners and the public. Any disruption to the use of these facilities will be detrimental to the Council and may result in actual financial loss.

1.3 This policy applies to all individuals who use Gnosall Parish Council's IT resources, including computers, networks, software, devices, data and email accounts.

GENERAL PRINCIPLES

1.4 All employees, members and other users should be aware of the increasingly sophisticated scams and risks posed to cybersecurity and when in any doubt should seek guidance from the Chief Officer. 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.

1.5 All employees, members and other users of council IT equipment must be familiar with and abide by the regulations set out in the council's 'Data Privacy and Protection Policy.

1.6 All hardware, software, data and associated documentation produced in connection with the work of the Council, are the legal property of the Council.

1.7 All council devices will have appropriate antivirus software installed.

1.8 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.

1.9 All software installed on council devices must be fully licensed by the

Council and no software should be installed without authorisation from the Chief Officer.

## 2. GENERAL IT POLICY

GOVERNANCE, ROLES AND RESPONSIBILITIES

| | | |
|---|---|---|
| 2.1 | Council: | Approves and reviews this policy annually and oversees IT risk management. |
| | Chief Officer/ Responsible Officer: | Ensures compliance, oversees ICT provider, ensures maintenance of assets and asset registers. |
| | Data Protection Officer : (DPO) | Ensures GDPR compliance and advises on data breaches, DPIAs, and privacy matters. |
| | IT Provider: | Maintains hardware and software, applies updates, and provides technical support. |
| | Users: | Councillors and staff must comply with this policy, use Council devices responsibly, and report incidents. |

EMPLOYEES/VOLUNTEERS

2.2 All employees will be assigned a council email address as appropriate.

2.3 Personal use of Council IT equipment is permitted but should be kept to a minimum during working hours. Reasonable use of the internet during working hours is permitted.

2.4 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.

MEMBERS

2.5 All members will be provided with a council e-mail address and must use this for all council business.

2.6 Members are reminded that any e-mail sent or received in their capacity as a Parish Councillor is Council data and any e-mails may have to be disclosed following requests under the Data Protection Act or Freedom of Information Act. This includes e-mails on Personal Accounts when acting as a Councillor.

2.7 A copy of all e-mails received on the councillor e-mail accounts is kept on the server in line with the council's Data Privacy & Protection Policy.

2.8 Members using social media in their capacity as councillors must make it

clear they are speaking in a personal capacity and not representing the view of the council.

2.9 Members should ensure they are adhering to the Council's code of conduct when using social media.

2.10 Members must ensure that, if any personal devices are used to access council systems (including email, websites and data), then those systems are password protected and access is restricted solely to the member.

## 3. USE OF THE INTERNET (WEBSITES)

DOMAINS

3.1 The Chief Officer is the registrant of any and all Council Parish domains, retaining control over the domain names and all related services, such as emails and websites.

3.2 Services delivered by the council should be delivered under the council's service name i.e. @gnosallparishcouncil.gov.uk.

3.3 With reference to services delivered by the council in partnership with an external organisation, it may be appropriate to use the council domain, but using a specific, separate domain is more likely.

3.4 Council staff or members should not register domains in their own names. All domains should be owned wholly by the council under the Chief Officer title to ensure there are no continuity or renewal issues, particularly should that person leave the council.

3.5 Clearly defined ownership and control of assets and data should be maintained to avoid conflicts and ensure smooth transitions.

COPYRIGHT

3.6 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.

3.7 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.

3.8 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).

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

TRADEMARKS, LINKS AND DATA PROTECTION

3.10 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.

3.11 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 Data Protection Policy.

3.12 The council may place relevant links on the website to enable residents to easily access appropriate information regarding the Council, Parish, local organisations or key service information such as Staffordshire County Council's Report It.

3.13 The website may include links to various outside bodies, including:

- Links to external organisations providing a public service – e.g. Stafford Borough Council, Staffordshire County Council
- Links to community partners
- Public service websites that provide information to the public, such as Police, Fire & Rescue Service, Safer Community Partnerships.
- Tourism websites that provide information to people wishing to visit the local area.
- Specific business websites providing public information, at the discretion of the Council.
- Contact for local churches.
- Links to websites of businesses who sponsor Council events or facilities.
- Local History and Museum websites.
- Links to websites of community groups or clubs which serve the Parish.
- The following Disclaimer to be used: "*Our website contains links to these other sites to provide information and for the convenience of the public. Gnosall Parish Council does not control these sites and so cannot guarantee that the information is up to date or correct. Gnosall Parish Council does not endorse any of the content of any businesses linked to the website nor any advertising linked to these websites*".

EDITORIAL CONTROL

3.15 The Chief Officer and selected members have editing rights for the Parish Council website and social media platforms. They can add, delete and amend specified areas of information on the Parish Council site and are

responsible for ensuring that the information is current and up to date.

3.16 Editorial Content Information needs to be accurate and in accordance with Parish Council Policy. The Code of Recommended Practice on Local Authority Publicity 2015 must be considered when matters of publicity are concerned.

3.17 The Public Sector Bodies (Websites and Mobile Applications) Accessibility Regulations 2018 require public sector websites to meet accessibility standards. They also apply to downloadable documents, mobile apps, intranets and extranets.

3.18 The Council will publish an accessibility statement on its website, and the Chief Officer will ensure compliance.

PROTOCOL FOR THE USE OF THE COUNCIL'S WEBSITE

3.19 The website and indeed email communications media may be used to:

- Post minutes and dates of meetings
- Advertise events and activities
- Publicise good news stories, linked websites or press pages
- Advertise Vacancies
- Post and communicate information from partners i.e. Police, Gnosall working groups, district councils etc.
- Announcing new information.
- Promulgate information required under the Transparency Code
- Give information on the Council, its policies and governance
- Refer resident queries to the Chief Officer, other staff or councillors.

## 4. USE OF THE INTERNET (SOCIAL MEDIA)

4.1 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.

4.2 Staff use of council devices to access personal social media networking/ media and chat sites should be restricted to breaks during working hours, or after hours with permission.

4.3 Council social media accounts will be operated by officers and/or members delegated access by the Chief Officer. Councillors, staff, and other authorised users who use Facebook, Instagram, 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.

4.4 All council social media messages must be non-political, uncontroversial and must be used to promote/highlight the Parish.

4.5 No social media accounts using the Gnosall Parish Council name and/or logo, or committee names, should be created without the approval of the Chief Officer.

4.6 Inappropriate comments and posts can adversely affect the reputation of the council, even if it is not directly referenced. If comments or photographs could reasonably be interpreted as being associated with the council, or if remarks about external stakeholders could be regarded as abusive, humiliating, sexual harassment, discriminatory or derogatory, or could constitute bullying or harassment, the council will treat this as a serious disciplinary offence.

4.7 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.

4.8 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:

- 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 the council. Even if the council is not mentioned, care should be taken with any views expressed on social media sites and any views should clearly be stated to be the writer's own (e.g. via a disclaimer statement such as: "The comments and other content on this site are my own and do not represent the positions or opinions of my employer/ the council.") Writers must not claim or give the impression that they are speaking on behalf of the council.
- Any 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, 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 in the first instance to the Chief Officer and to the Chair if the Chief Officer cannot be reached.
- 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 users. All such contacts will be considered council property and may be subject to disclosure upon request.

4.9 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.

## 5. PASSWORD AND AUTHENTICATION PROTECTION

5.1 All council computers and systems must be password protected to prevent unauthorised access. Different passwords should be used for different platforms and passwords should be changed frequently, to offer effective protection against common cyber threats such as brute-force attacks. This

approach is endorsed in NALC guidance.

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.

5.2 Where feasible, two factor authentication should be utilised.

5.3 Users should ensure that unattended devices are password protected, with screens locked.

5.4 Where possible, generic user accounts should be avoided.

5.5 Where users have unique access permissions and/or accounts for systems, these must not be shared with other users.

5.6 Different passwords should be used for different accounts and devices.

5.7 Passwords should be changed routinely.

5.8 Passwords should not be written down or left in unsecure locations.

5.9 Passwords must be stored using a council-approved, encrypted password manager.

5.10 Passwords should be immediately changed if compromise is suspected

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

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

## 6. COMPUTER USE

HARDWARE

6.1 Council computer equipment is provided for council purposes; however reasonable personal use is permitted (reasonable interpreted as in the opinion of the Chief Officer. Any personal use of our computers and systems should not interrupt our daily council work in any way. Councillors, staff, and other authorised users are asked to restrict any personal use to official lunch breaks or before or after working hours.

6.2 Locking computers when leaving desk, all councillors, staff, and other authorised users must lock their computers when leaving their desks to prevent unauthorised access. This applies to all council and personal

devices used for work. Failure to comply may lead to disciplinary action.

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

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

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

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

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

PORTABLE DEVICES

6.8 All portable devices (including tablets and mobile phones) must be protected to prevent unauthorised access. This can be by use of passwords, passcodes or other biometric measures as applicable.

6.9 Passcodes must be appropriate for the device and the level of risk that unauthorised access poses to the organisation; where devices can access council data or other systems, passcodes must be unique and not easily guessable.

6.10 Particular care must be taken when using removable media to transmit data as such media are easily lost or intercepted. Any sensitive information (including personal data, confidential documents or data which could impact on the rights or reputation of any person or organisation including the council) placed on removable media must be suitably password protected or encrypted.

6.11 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 (unless locked in a secure cabinet or office) should be always kept with or near the user; 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.

6.12 If an item of 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 first £100 of the loss/damage.

6.13 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 in council offices 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.

6.14 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).

6.15 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.

PERSONAL DEVICES

6.16 Personal laptops and other computers or other devices should not be brought into work and used to access council IT systems 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.

6.17 The Council recognises that some councillors, staff, and other authorised users may wish to use their own smartphones, tablets, laptops etc to access our servers, private clouds or networks for normal council purposes, including, but not limited to, reading their emails, accessing documents stored on the council's network or to store data on the council's server(s) or access data in other services. Any such use of personal devices will be at the discretion of the council, but consent for standard systems (MS Windows, Mac OS X, Linux- in commercial configurations) will normally be permitted. Such devices should be kept up to date so that any vulnerabilities in the operating system or other software on the device are appropriately patched or updated. Windows users should have a minimum of Windows 11 installed on their devices to avoid security concerns.

6.18 However, the same security precautions apply to personal devices as to the council's desktop equipment. For continuity purposes, calls made to external parties (such as external stakeholders) should be made on council landlines or mobile phone numbers to ensure that only these numbers are used and/or stored by the recipient, rather than personal numbers. Any emails sent from own devices should be sent from a council email account and should not identify the individual's personal email address.

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

6.20 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.

6.21 Personal data relating to councillors, staff, and other authorised users, associates, residents, external stakeholders should not be saved to any personal accounts with third-party storage cloud service providers (e.g. IONOS) 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.

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

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

6.24 Councillors, staff, 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.

6.25 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 because of the above.

## 7 HEALTH AND SAFETY

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

7.2 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 & Safety Policy.

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

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

## 8 MISUSE OF I.T.

8.1 IT systems will be monitored for misuse and all misuse is prohibited.

8.2 Misuse includes, but is not limited to:

- Creation or transmission of any offensive, obscene or indecent images, data or other material or any data capable of being resolved into obscene or indecent images or material
- Creation of material which is designed or likely to cause annoyance, inconvenience or needless anxiety.
- Creation or transmission of defamatory material
- Transmission of material which in any way infringes the copyright of another person
- Transmission of unsolicited commercial advertising material to networks belonging to other organisations
- Deliberate actions or activities with any of the following characteristics:
    - Wasting staff effort or networked resources
    - Corrupting or destroying other users' data
    - Violating the privacy of other users
    - Disrupting the work of other users
- Other misuse of the networked resources by the deliberate introduction of viruses/malware
- Playing games during working hours
- Altering the set up or operating perimeters of any computer equipment without authority.

8.3 Unauthorised access, use, destruction, modification and/or distribution of council information, systems or data is prohibited.

## 9 MONITORING

9.1 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.

9.2 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.

9.3 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.

9.4 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.

9.5 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.

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

9.7 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.

9.8 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.

9.9 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.

9.10 All computers will be periodically checked and scanned for unauthorised programs and viruses.

## 10 INCIDENT REPORTING

10.1 All members, employees or volunteers must report any incidents which could pose a risk to the council's systems or data security to the Chief Officer or designated I.T. point of contact without delay. This includes but is not limited to:

- Lost devices

- Potential risk arising from phishing emails/websites
- Passwords having been shared
- Unauthorised access to systems

## 11 TRAINING & AWARENESS

Gnosall Parish Council will provide training to educate users about IT security best practice, privacy concerns and technology updates. All employees and members will receive training in email security and best practice. All members and employees will be required to read and accept this policy as part of their Induction.

## 12 CONTACTS

For all IT-related enquiries or assistance, users should contact the Chief Officer.