TIBSHELF PARISH COUNCIL
Information Security Policy

Adopted 17.10.2023
Full Council meeting – Minute no: 1023/3207

Introduction
This policy sets out Tibshelf Parish Council's position of the use of the Internet, email and other parish council computer systems and data contained therein. Any deliberate breach of this policy will be dealt with under the disciplinary policy.

.

Internet Usage
The use of the Internet by staff is permitted where use is part of the normal execution of an employee's job responsibilities. Any information (including email messages) that has been downloaded from the Internet by whatever means should be checked for computer viruses. This policy is necessary in order to avoid the Parish Council's information systems being subjected to computer hacking and software viruses.

Appropriate Usage
The Parish Council's computer connections are to be used for the Parish Council's business/provision of services. Connections to the Internet must only be via IT equipment authorised for the purpose. The Parish Council reserves the right to periodically examine its computer equipment, directories, files and their contents to ensure compliance with the law and with Parish Council policies.

Non-permitted Usage
The following is not allowed. This list is not exhaustive: • Downloading any software or electronic files without the required virus protection measures in place • Making or posting indecent remarks and proposals • Visiting websites that contain obscene, hateful or other objectionable material or distributing and forwarding such material • Soliciting for personal gain or profit • Gambling • Conducting illegal activities • Hacking, i.e., attempting unauthorised access into or intentionally interfering with any Internet/Intranet gateway/system/server • Uploading/downloading commercial software in violation of its licence agreement • Receiving newsgroup emails that are unrelated to the business of the Parish Council.

Security
All staff must report Internet security weaknesses that they become aware of to the Parish Clerk or the Chair of the council. The distribution of any information through the Internet, the web, computer-based online services, email and messaging systems is subject to the scrutiny and approval of the Parish Council, which reserves the right to determine the suitability and confidentiality of information disseminated.

Virus Protection
The world wide web and email are high risk sources of computer virus infections. It is essential that all material received over the Internet and via email is checked before use or distribution. Email attachments must be virus checked before distributing further. Viruses that are detected must be reported to the Parish Clerk or the Chair of the council. The final responsibility for virus checking will always remain with the user.

Passwords
Computer and email passwords are to be changed every six months (minimum) and must contain at least 1 capital letter and 1 numerical character to ensure the passwords are "strong" or use three random words.

Confidential and Personal Information
Members of the council and staff are prohibited from revealing or publicising confidential or personal information that they have not been specifically authorised to do so. Such information includes but is not limited to:

• Financial information not already publicly disclosed through authorised channels
• Personal information

• Operational information
• Information provided to the Parish Council in confidence or under a non-disclosure agreement
• Legal proceedings
• Information that might provide an external organisation with a business advantage
• Computer programs
• Databases and the information contained therein

Information security incident
An information security incident occurs when data or information is transferred or is at risk of being transferred to somebody who is not entitled to receive it, or data is at risk from corruption.

An Information Security Incident includes:
The loss or theft of data or information
The transfer of data or information to those who are not entitled to receive that information.
Attempts (either failed or successful) to gain unauthorised access to data or information storage or a computer system.
Changes to information or data or system hardware, firmware, or software characteristics without the council's knowledge, instruction, or consent
Unwanted disruption or denial of service to a system
The unauthorised use of a system for the processing or storage of data by any person.

When to report.
All events that result in the actual or potential loss of data, breaches of confidentiality, unauthorised access or changes to systems should be reported as soon as they happen.

Action on becoming aware of the incident.
Follow the information security procedure, according to the type of incident.

How to report.
The Parish Clerk must be contacted by email or telephone. They will log the incident and forward it on to the relevant departments.

The Parish Clerk will require you to supply further information, the nature of which will depend upon the nature of the incident. However, the following information must be supplied:

- Contact name and number of person reporting the incident.
- The type of data or information involved.
- Whether the loss of the data puts any person or other data at risk
- Location of the incident
- Inventory numbers of any equipment affected.
- Date and time the security incident occurred.
- Location of data or equipment affected.
- Type and circumstances of the incident.

The outcomes of these actions are to be reported to the Parish Clerk for inclusion in the incident details for the Council’s investigation.

TIBSHELF PARISH COUNCIL
Information Security Policy

What to Report.
All Information Security Incidents must be reported.

Examples of Information Security / Misuse Incident Protocols
Information Security Incidents are not limited to this list, which contains examples of some of the most common incidents.

Malicious Incident
Computer infected by a Virus or other malware, (for example spyware or adware)
An unauthorised person changing data.
Receiving and forwarding chain letters – Including virus warnings, scam warnings and other emails which encourage the recipient to forward onto others.
Social engineering - Unknown people asking for information which could gain them access to council data (e.g., a password or details of a third party).
Unauthorised disclosure of information electronically, in paper form or verbally.
Falsification of records, Inappropriate destruction of records
Denial of Service, for example
Damage or interruption to Tibshelf Parish Council equipment or services caused deliberately e.g., computer vandalism.
Connecting non-council equipment to the council network
Unauthorised Information access or use.
Giving information to someone who should not have access to it - verbally, in writing or electronically.
Printing or copying confidential information and not storing it correctly or confidentially.

Access Violation
Disclosure of logins to unauthorised people
Disclosure of passwords to unauthorised people e.g., writing down your password and leaving it on display.
Accessing systems using someone else's authorisation e.g., someone else's user id and password
Other compromise of user identity e.g., access to network or specific system by unauthorised person

Environmental
Loss of integrity of the data within systems and transferred between systems.
Damage caused by natural disasters e.g., fire, burst pipes, lighting etc.
Deterioration of paper records
Introduction of unauthorised or untested software
Information leakage due to software errors.

Inappropriate use
Accessing inappropriate material on the internet
Sending inappropriate emails
Using unlicensed Software
Misuse of facilities, e.g., phoning premium line numbers.

Theft / loss Incident
Theft / loss of data – written or electronically held.
Theft / loss of Tibshelf Parish Council equipment including computers, monitors, mobile phones.

Accidental Incident, sending an email containing sensitive information to 'all staff' by mistake.

Receiving unsolicited mail of an offensive nature, e.g., containing pornographic, obscene, racist, sexist, grossly offensive, or violent material

Receiving unsolicited mail which requires you to enter personal data.

Mis keying

Receiving unauthorised information.

Name	Date	Signed to confirm I have read and understood this document.

TIBSHELF PARISH COUNCIL
Information Security Policy
