



# **Normanby by Spital Parish Council**

## **Smaller Authorities IT Policy**

## **1. Introduction**

Normanby by Spital Parish Council henceforth known as “The Authority” recognises the importance of effective and secure information technology (IT) and email usage in supporting its business, operations, and communications.

This policy outlines the guidelines and responsibilities for the appropriate use of IT resources and email by council members, employees, volunteers, and contractors.

## **2. Scope**

This policy applies to all individuals who use IT resources, including computers, networks, software, devices, data, and email accounts. Everyone must adhere to this policy to maintain digital security.

## **3. Training and awareness**

The Authority will source regular training and resources to educate users about IT security best practices, privacy concerns, and technology updates. You should engage in regular training on email security and best practices as provided by LALC.

## **4. Using personal devices**

- Use strong passwords for all your accounts (preferably using a password manager)
- download the latest operating system security updates
- Use anti-virus software

## **5. Network and internet usage**

You must be careful about which Wi-Fi networks you join. Public Wi-Fi networks in coffee shops or on trains can be targeted by hackers. Always make sure you are using a trusted internet connection, which is password protected when carrying out official business.

## **6. Password and account security**

You are responsible for maintaining the security of your accounts and passwords. For business continuity, login details and passwords need to be stored securely so they can be accessed by trusted individuals in an emergency. The password to the Clerks email address and the email setup for other councillors is stored in a sealed envelope with the Personnel Committee Chair.

## **7. Email communication**

The Authority has provided you with an official email account for organisation-related communication only. You must make sure that emails are professional and respectful in

tone. You must always check you are sending any confidential or sensitive information to the correct recipients.

Always be cautious when downloading attachments and opening links to avoid phishing and malware. Before opening any attachments or clicking on links, verify the source by looking at the email it has come from carefully. Do not download and open anything if you are unsure who has sent it.

### **8. Email access**

The Authority reserves the right to check email communications to ensure compliance with this policy and relevant laws. Monitoring will be conducted in accordance with the Data Protection Act and GDPR. Clerks may need to access emails so that they respond to FOI or subject-access requests. If you are using a personal email account for council business, this is still subject to data protections laws and FOI requests.

### **9. Data management, data retention and security**

All sensitive and confidential data should be stored and transmitted securely. You must regularly backup any important data to prevent data loss and follow your organisation's data retention policies.

You should retain and archive emails in compliance with your data retention policies. Regularly review and delete unnecessary emails to maintain an organised inbox.

### **10. Reporting security incidents**

All suspected security breaches, including email breaches or incidents should be reported immediately to the clerk.

### **11. Compliance and consequences**

Breach of this IT and Email Policy may result in the suspension of IT privileges.

### **12. Policy review**

This policy will be reviewed annually to ensure its relevance and effectiveness. Updates may be made to address emerging technology trends and security measures.

### **13. Contacts**

For IT-related enquiries or assistance, users can contact the clerk.

The Clerk and councillors are responsible for the safety and security of IT and email systems.

Date of adoption: \_\_\_\_\_ Date for next review: \_\_\_\_\_