GOODMANHAM PARISH COUNCIL
INFORMATION TECHNOLOGY POLICY – JANUARY 2026

1. Introduction

Goodmanham Parish Council recognises the importance of effective and secure information technology (IT) usage in supporting its business, operations and communications.

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

2. Scope

This policy applies to all individuals who use Council IT resources, including computers, software, devices, and data.

Resources include access to .gov.uk email addresses and any associated digital storage.

3. Acceptable use of IT resources

Council IT resources, where provided, are to be used for official council-related activities and tasks. Personal use should be limited and should not interfere with Council work responsibilities.

All users must adhere to ethical standards, respect copyright and intellectual property rights, and avoid accessing inappropriate or offensive content.

4. Device and software usage

The Council will provide the Clerk with a laptop for Parish Council activities. This will be held by the Clerk at home, and must not be used by any other person.

Unauthorised installation of software on the laptop, including personal software, is strictly prohibited due to security concerns.

5. Data management and security

All sensitive and confidential Goodmanham Parish Council data should be stored and transmitted securely using approved methods.

Regular data backups should be performed using the removable hard disc held by the Clerk to prevent data loss, and secure data destruction methods should be used when necessary.

6. Email communication

Any Email communication by the Clerk or Councillors relating to Council business must be through the Accounts provided by the Council. These are for official communication only. Emails should be professional and respectful in tone.

All Council-related emails must comply with the current legislation, including the Freedom of Information Act and Data Protection Act.

Be cautious when opening email attachments or clicking on links to prevent phishing and malware threats.

7. Whatsapp

The Group will bet set up and managed by the Clerk. All Council-related communications on WhatsApp must comply with the current legislation, including the Freedom of Information Act and Data Protection Act.

Council members must use their official council WhatsApp group only for council-related communications. Messages that contain sensitive or confidential information should not be shared on WhatsApp.

WhatsApp may be used for quick, informal communications regarding council matters. Official council business should be conducted through formal channels such as council email or meetings.

The Clerk and Council members must maintain professionalism and respect in all communications. Use of the official council WhatsApp group for personal or non-council related matters is strictly prohibited.

8. Personal Phones

The Council relies on use of personal phones for Council business. Any official business call must make clear that it is on behalf of the Council i.e. making it clear it is from a Clerk or Councillor.

9. Password and account security

The Clerk and Councillors are responsible for maintaining the security of their accounts and passwords. Passwords will be issued by the Clerk and must not be shared with others. 4

10. Reporting security incidents

All suspected security breaches or incidents should be reported immediately to the Clerk for investigation and resolution.

12.1.26