Wiggenhall St Mary Magdalen Parish Council

Email, Internet and Computer System Use
Policy & Procedure for Councillors

1.   INTRODUCTION

This document sets out the Council's policy for general computer use in compliance with the General Data Protection Regulations (GDPR).

2.   OBJECTIVES

The objectives of the policy are to ensure that the services made available to Councillors are used:

- In accordance with the values, principles and standards of the Council
- Ensure GDPR is complied with
- So as not to incur legal liability

3.   ACCEPTANCE OF THE POLICY

The policy applies to all Parish Council Councillors. All Councillors are required to sign to indicate their acceptance of the policy content at the time of joining the Council and will be asked to re-affirm their understanding and acceptance of the policy on an annual basis.

Each Councillor is responsible for individually complying with this policy.

4.   SECURITY

Access to the Councillors network and files, including Internet services, is restricted to individual users and MUST not be shared accounts.

- The access of each user is controlled by means of their own password
- Passwords <u>must</u> be kept confidential and not disclosed to others; disclosure could result in Internet or email misuse being attributed to the owner of the password
- Care should be taken not to leave a device that is connected to the Internet/system unattended or unlocked
- Breaches of security of the computer system e.g. disclosure of personal passwords, giving unauthorised access to emails to external parties, may result in action from the Information Commissioners Office (ICO)
- For further protection of personal data, all files containing names, telephone numbers, addresses and email addresses, etc. must be password protected. These files are likely to take the form of internal databases, registers etc.
- If you suspect there has been data breach or your email/IT has been hacked you must inform the Clerk immediately. The Clerk will then contact the council's Data Protection Officer for guidance on the most appropriate way to deal with the breach.

5.   GUIDANCE

This section of the document provides guidance on the acceptable use of the Council's email and Internet services and contacts databases.

5.1   Email Usage

The Council's email system enables users to email Officers and Members of the Council, as well as individuals outside of the organisation. Users should be aware that once an email is sent to an individual outside of the Council, it is beyond the Council's control and is not guaranteed to be confidential.

Hoax and/or suspect emails should be reported to the Clerk/Deputy Clerk. They should not be opened or forwarded but "double deleted" i.e. deleted from the users "Inbox" and then "Deleted Items".

5.1.2 Prohibited Email Activities

The following email activities may breach the councils 'code of conduct' and/or prompt action by the Information Commissioners Office:

- Examining, changing or using another person's files, output or user name without explicit authorisation
- Sending or forwarding any material that is obscene, defamatory or hateful, or which is intended to annoy, harass or intimidate others
- Sending or forwarding emails which are likely to damage the reputation of the Council
- Sending or forwarding electronic chain letters
- Soliciting emails that are unrelated to Council activities or soliciting non Council business for personal gain or profit
- Intentionally interfering with the normal operation of the Council's network, including the propagation of computer viruses and the generation of sustained high volume network traffic
- Sending or forwarding attachments of such size or arrangement as to cause disruption to the Council's network *(see Section 5.1.5)*

5.1.3 Personal Email Use

The use of Wiggenhall St Mary Magdalen Parish Council email for personal purposes is not permitted.

5.1.4 Email Awareness

Email is not a secure method of transmission – it should not be assumed that any email communication is secure or private. Users should take this into account particularly when emailing confidential or sensitive information.

5.1.5 Email Best Practice

- Ensure that each email has a specific target audience.
- Be selective, especially when deciding who should be copied in on an email. This ensures that only those who really require the information receive it, and avoids wasteful emails and wasted time/resources.
- If you are copying in a recipient(s) who you think have not given permission for their email to be circulated use Bcc to protect their information
- The circulation of emails **with attachments** to large groups should be avoided.
- When sending emails to a large number of people the recipients' addresses should be entered into the **BCC** (blind copy) field. Users should contact the Council's IT Administrator if assistance is required
- Emails should not be kept in separate folders in an individual's folder list longer than is necessary, if at all.
- Time should be set aside on a regular basis for "housekeeping", in order to delete old or unwanted items from mailboxes. This is essential in order to ensure the efficient operation of the email system and helps to keep mailboxes organised and ensure that councils GDPR retention policy is complied with.
- The 'Inbox', 'Sent Items' and 'Deleted Items' folders should be examined as part of a housekeeping routine, performed at a minimum frequency of once a month. Contact the council's IT Administrator for assistance if you are unsure of how to complete any of the processes described in this policy.

5.1.6 Email Etiquette

Email is all about communication with other people, and as such some basic courtesy should be observed.

- Always include a subject line in your message
- When replying to an email, include enough of the original message to

provide a context
- An email signature is a good way of providing detail of who is sending the email, and the details of how to respond
- Consider the tone and language used, and the use of plain English. When sent externally emails represent and reflect upon the Council
- Avoid using capitals throughout as this is equivalent to shouting

5.2   Database Usage

In accordance with the Data Protection Act, no personal details/data from any contacts databases e.g. Parish Council Contacts, should be given out to external parties at any time.

No personal data/databases should be kept on any storage facility e.g. CD's, DVD's 3 ¼" discs, USB's laptops or personal home based computers, as this could result in legal action from third parties.

Any communication by a councillor that is **not** associated directly with Wiggenhall St Mary Magdalen Parish Council business (i.e it is carried out by a councillor acting on their own by or on behalf of another) is **not** considered as acting as a councillor by the ICO 'the business of the council'. Therefore you are not covered by the council's data protection fee requirement to the Information Commissioners Office https://ico.org.uk/for-organisations/data-protection-fee/ and as such you will be responsible (as an individual) for complying with ALL the General Data Protection Regulations regarding data security.

6.   ACCESS CONTROL AND MONITORING

The following will apply when the services are accessed from the Council's network.

6.1   Email Monitoring

The Council monitors email activity, so that compliance with this policy and other relevant policies and regulations can be effectively managed.

6.2   Email Viruses

Continuous virus checking of all incoming email will take place. However, it is possible that a new virus may not be detected by the Council's virus scanner and users should be wary of opening attachments to emails from an unknown source; in particular attachments with names ending in "exe" should not be opened.

If you receive notification of a virus via chain email do not forward to anyone. Advise the council's IT Administrator of the details who will investigate the virus threat.

Section 5.1 gives additional information on dealing with hoax/suspect emails.

6.3   Email Filtering

Users should note that the Council's Internet Services Provider, filters incoming email for porn and spam as well as scanning for email viruses.

Approved at the meeting of the Full Council June 2023
Amendments will be made as and when the size and nature of the council changes or when new legislation is introduced.

WIGGENHALL ST MARY MAGDALEN PARISH COUNCIL

Email, Internet and Computer System Use Policy

ACCEPTANCE SLIP

I have received, read and understood the Council's Email, Internet and Computer Use Policy.   I understand that: -

- My use of Wiggenhall St Mary Magdalen Parish Council email will be monitored for management and security purposes.

- If I use my own computer/laptop/tablet for council business I confirm I am responsible for ensuring I comply with IT security and data protection as required under the General Data Protection Regulations.

- Breaches of the policy may result in action being taken against me by the Information Commissioners Office

Signed   …………………………………………………………………………………..

Name   …………………………………………………………………………………...

Date   …………………………………………………………………………………...

Please return completed forms to Clerk, Wiggenhall St Mary Magdalen Parish Council Offices