EMAIL POLICY

1. INTRODUCTION

Chattisham and Hintlesham Parish Council ("the Council") provides email facilities for use by Councillors who have access to a desktop, laptops and/or mobile devices. This Policy sets out the Council's policy for the use of these facilities and more general computer use in compliance with the General Data Protection Regulations ("the GDPR") and the Data Protection Act 2018 ("the Act").

2. OBJECTIVES

The objectives of the Policy are to ensure that the facilities made available to Councillors are used in accordance with the values, principles, and standards of the Council.

Ensure the GDPR and the Act is complied with by ensuring only Council approved email accounts are used for Council business; and

Overall, to comply with any data protection legislation from time to time in force in England including the Data Protection Act 1998 or 2018 or any successor legislation.

3. ADOPTION OF THIS POLICY

This Policy was adopted by the Council on the 11th March 2021 (CHPC152/20) and applies to all Council Councillors and its employees.

Each Councillor and employee of the Council are responsible for individually complying with this Policy.

This Policy will be reviewed on a regular basis, and no less than annually, by the Clerk who will, if considered necessary, report thereafter, and as soon as practicable, to the Council accordingly.

4. SECURITY

Each Councillor is provided with a Council email account for the sole purpose of conducting Council business.

The access of each user is controlled by means of their own password.

Passwords must be kept confidential and not disclosed to others; disclosure could result in the 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) under GPDR legislation.

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 a data breach or your email/IT has been hacked, you must inform the Clerk immediately. The Clerk will then report this breach to 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

Hoax and/or suspect emails should be reported to the Clerk where relevant. They should not be opened or forwarded but “double deleted” i.e. deleted from the user's “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 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

5.1.3 Personal Email Use

The use of 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, except those sent to Councillors.

When sending emails to a large number of people the recipients' addresses should be entered into the BCC (blind copy) field. 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.

Councillors are encouraged to set aside time 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 Council’s Freedom of Information 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.

When a Councillor or employee of the Council leaves the Council (for whatever reason), will, in consultation with the Clerk, delete their email account with immediate effect.

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.

Consider the tone and language used and the use of plain English. When sent externally emails represent and reflect upon the Council.

5.2 Database Usage

In accordance with the GDPR and the Act, no personal details/data from any contacts databases e.g. 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 14” discs, USB’s laptops or personal home-based computers, as this could result in legal action from third parties.

Each Councillor and Council employees will be responsible for complying with ALL the GDPR and the Act regarding data security.

6. ACCESS CONTROL AND MONITORING

The following will apply when the facilities are accessed from the Council’s network.

6.1 Email Viruses

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.

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

7. INFORMATION COMMISSIONERS OFFICE

This Policy should be read together with all guidance provided and available from the Information Commissioners Office; at www.ico.org.uk.