KESGRAVE TOWN COUNCIL

Email, Internet and Computer System Use Policy and Procedure

1. INTRODUCTION

Council provides email facilities for use by Councillors and this document sets out Council's policy for the use of these services and more 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 are used:

- in accordance with Council's Code of Conduct;
- to ensure GDPR is complied with by ensuring only Council approved email accounts are used for Council business;
- to minimis the risk of incurring legal liability;
- so as not to threaten the integrity of Council's IT services.

3. SECURITY

- Access to email accounts is restricted to individual users, is confidential and must not be shared.
- 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 any email misuse being attributed to the owner of the password.
- Care should be taken not to leave a device that is connected to a Councillor's email account unattended or unlocked.
- Breaches of security e.g. disclosure of password, giving unauthorised access 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.
- Any suspected breach or hack of an email account must be advised immediately to the Clerk.

4. GUIDANCE

This section provides guidance on the acceptable use of the Council's email. It must be read in conjunction with the Council's other policies, e.g Data Protection (General).

Email usage

- Council's email system enables users to email officers and Council members, as well as externally. Users should be aware that once an email is sent externally, it is beyond Council's control and is not guaranteed to be confidential.
- Hoax and/or suspect emails received should be reported to the Clerk. These should not be opened or forwarded but "double deleted" i.e. deleted from the users "Inbox" and then from "Deleted Items".

Prohibited email activities

The following email activities may breach Council's '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 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 Council's network, including the propagation of computer viruses and the generation of sustained high volume network traffic; and
- sending or forwarding attachments of such size or arrangement as to cause disruption to Council's network.

Personal email use
The use of Council's email for personal purposes is not permitted.

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.

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 the blind copy facility (BCC) to protect their personal data.
- 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 Clerk if assistance is required.
- 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 Council's Document and Electronic Data 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.

Email etiquette
Email involves communication with others and some basic courtesies should be observed:
- always complete the subject line in a new message;
- when replying to an email, enough of the original message should be included to provide a context. An email signature is a good way of providing detail of who is sending the email, and the details on how to respond.
- consider the tone and language used, and the use of plain English. When sent externally emails represent and reflect upon Council.
- use of capitals should be avoided in the text as this is interpreted as shouting.

Database usage
- In accordance with the Data Protection 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 personal storage facility e.g. USBs, laptops, tablets, smart phones or home-based computers, as this could result in legal action from third parties.
- Any communication that is not associated directly with Council business (i.e. it is carried out by a Councillor acting on their own or on behalf of another) is not considered as acting as a Councillor by the ICO 'the business of the Council'. Therefore, this is not permitted.

5. ACCESS CONTROL AND MONITORING

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

Email filtering and virus detection
- Users should note that Council's Internet Services Provider filters incoming email for unsolicited sites and spam as well as scanning for email viruses. However, it is possible that a new virus may not be detected and users should be wary of opening attachments to emails from an unknown source. In particular attachments with filenames ending in ".exe" should not be opened.
- Receipt of the notification of a virus via chain email should not be forwarded. The Clerk should be advised of the details and will investigate the virus threat.

Email access
On the receipt of a Freedom of Information or Subject Access Request it may be necessary for the Clerk to access Councillors' email accounts. Those concerned will be informed if this is necessary to allow Council to fulfil the request and its legal obligations.

Last review: 21 June 2021

Next review due: 21 June 2023 (or earlier if relevant legislation changes before this date)