



SAFFRON WALDEN  
TOWN COUNCIL

# Electronic Information & Communication System Policy (IT Policy)

Version	Adopted Policy Date	Minute Reference	Review Date
1	April 2019	F&E 538-19	2022
2	November 2022	F & E 159-22	October 2025
3	October 2025	F&E 147-25	October 2027

## **1. Email**

- 1.1. Increasingly, e-mail messages are now used as the routine method of correspondence. This facility, together with access to the internet, is available through the Council's computer network.
- 1.2. The following guidance is given to ensure that the facility is properly used and not abused.
- 1.3. The overriding principle is that e-mail messages are to be controlled and processed to the same standards as for normal correspondence. Because e-mails, both received and sent, are processed on an individual personal computer, in the majority of instances without the knowledge of a Line Manager, there must inevitably be a high degree of trust from everyone in the use of e-mails.
- 1.4. SWTC reserves the right to monitor and read emails on a case-by-case basis and in the event of any suspect security breach
- 1.5. We also monitor e-mails for compliance reasons and to ensure that unauthorised disclosure of confidential information is not passed via the e-mail system.

## **2. Outgoing messages**

- 2.1. No potentially offensive messages are to be sent. Defamation, harassment and breaches of the Council's discrimination policy are all potential risks. Please also be wary of the temptation to send off a hasty message that, on reflection, would seem unwise. A good rule is to reply later or the next day if annoyed or offended by action taken or a communication received; allowing yourself a "cooling off period" can avoid putting yourself in the wrong.
- 2.2. All e-mails are to be restricted to the Council's professional work and personal e-mails should not be sent without manager approval.
- 2.3. Always check the state of attachments to see that you are sending the correct draft.

## **3. Virus protection**

- 3.1. Our e-mail facility is protected by anti-virus software. All anti-virus updates are to be processed without delay.
- 3.2. Nobody may introduce to their PC any disk without our permission.
- 3.3. If a suspicious e-mail message is received, for example from an unidentifiable sender, especially with attachments, it should not be opened. Particular caution is needed where the message is from a familiar

source but there is no text in the message. In such circumstances please telephone the sender before opening that attachment to see if they have indeed sent a bona fide message to you. Where there is still doubt, the message should be deleted without being opened.

- 3.4. No-one is to connect any 3<sup>rd</sup> party, unauthorised device (ie mobile phone, laptop, pc, tablet or the like) to any Town Council owned IT device or equipment. Should it be necessary to connect a personal or 3<sup>rd</sup> party device to the Council system, specific authorisation and verification must be sought from the Town Clerk who will in turn take reference to the Town Council's appointed IT provider. Prior to any authorisation being granted, it is likely that a personal device will be vetted/virus checked (and the like) by the Council's independent IT provider. Permission for this vetting/checking must be given prior to any connection to any Town Council device or equipment

#### **4. Internet use**

- 4.1. In no circumstances should any individual within the Council visit sites that could reasonably be regarded as pornographic, discriminatory or offensive. Users must also be wary of breach of copyright from inappropriate downloads.
- 4.2. Please note that we may monitor internet access for the purpose of enforcing this policy.
- 4.3. Failure to follow this policy will be regarded as a disciplinary offence and could lead to the termination of employment.

#### **5. Computer Use - Including the use of email/Internet**

- 5.1. It is very important that the Council is able to keep its data secure and ensure that computer systems are used only for their proper purpose. To assist with this, all employees are required to comply with instructions that may be issued from time to time regarding the use of Council-owned computers or systems.
- 5.2. You should ensure that when leaving a computer for any lengthy period, that you lock your terminal, or log off if appropriate.
- 5.3. You must not attach any device to Council IT equipment without authorisation from the Town Clerk and you must not open attachments or click on links unless you know you can trust the source. Council portable IT devices must be kept secure and password protected at all times.
- 5.4. Your computer password is an important piece of confidential information and you should treat it that way. Do not share it with others, and make sure that it is not written down anywhere where an unauthorised person can find it.
- 5.5. Unauthorised access to any of the Council's systems will amount to gross

misconduct.

## **6. Internet Use**

- 6.1. Employees with access to the internet on Council-owned devices should use that access responsibly.
- 6.2. Reasonable personal use is permitted provided the rest of this policy is complied with.
- 6.3. From time to time the Council may block access to sites which it considers inappropriate but whether or not a specific site has been blocked, employees must not use the internet to view or download offensive or sexually explicit material. Any attempt to do so may, depending on the circumstances, amount to gross misconduct leading to dismissal.
- 6.4. Employees must not download any software, plugins or extensions on to Council-owned devices unless this is first cleared by an appropriate manager. Employees should also refrain from downloading music, video or any other entertainment content on any Council-owned device.
- 6.5. Firewalls and anti-virus software may be used to protect the Council's systems. These must not be disabled or switched off without express permission from management.

## **7. Email**

- 7.1. All email correspondence should be dealt with in the same professional and diligent manner as any other form of correspondence.
- 7.2. If you have a Council email account you should be mindful of the fact that any email that you send will be identifiable as coming from the Council. You should therefore take care not to send anything via email that may reflect badly on the Council. In particular, you must not send content of a sexual, racist or discriminatory nature, junk mail, chain letters, cartoons or jokes from any email address associated with work.
- 7.3. Using an Council/work email address to send inappropriate material, including content of a sexual, racist, discriminatory or harassing nature, is strictly prohibited and may amount to gross misconduct resulting in summary dismissal. Should you receive any offensive or inappropriate content via email you should inform a member of management of this as soon as possible so that they can ensure that it is removed from the system. You should also report such breaches in accordance with our Harassment and Bullying or Grievance policies.
- 7.4. You should also take care that emails will be seen only by the person intended. Particular care should be taken when sending confidential information that the email has been correctly addressed, marked 'private' /'confidential' and not copied in to those not authorised to see the

information. Sending confidential information via email without proper authorisation or without taking sufficient care to ensure that it is properly protected will be treated as misconduct.

## **8. Privacy**

- 8.1. Monitoring of email and internet usage may take place without notice. You should have no expectation of privacy in respect of personal and business use of email and the internet whilst at work.
- 8.2. Your work email remains the property of the Council and therefore you should not use your work email to send or receive any information that you regard as private. The Council may, in the course of its business, read emails that you have sent or received - although in the absence of evidence of wrongdoing the Council will try to avoid reading personal emails if possible.

## **9. Social Media**

- 9.1. An employee's behaviour on any social networking or other internet site must be consistent with the behaviour required of employees generally. Where it is possible for users of a social media site to ascertain who you work for, then you should take particular care not to behave in a way which reflects badly on the Council.
- 9.2. You must avoid making any social media communications that could damage our business interests or reputation, even indirectly. You must not use social media to:
  - a) defame or disparage or make any other inappropriate comment about us, our staff or any customer, client or other third party;
  - b) harass (including sexually harass), bully or unlawfully discriminate against staff, customers, clients or other third parties;
  - c) make false or misleading statements; or
  - d) impersonate colleagues or third parties.
- 9.3. Because social media interactions can be copied and widely disseminated in a way that you may not be able to control, the Council will take a particularly serious view of any misconduct that occurs through the use of social media.
- 9.4. You should make it clear in social media postings, or on your personal profile, that you are speaking on your own behalf. Write in the first person and use a personal email address. Be respectful to others when making any statement on social media and be aware that you are personally responsible for all communications which will be published on the internet for anyone to see.

- 9.5. You must not operate a social media account or profile or express an opinion that purports to be operated/made on behalf of the Council without express permission to do so from your manager. You must not comment on social media about sensitive business-related topics, such as our performance, or do anything to jeopardise our trade secrets, confidential information and intellectual property. You must not include our logos or other trade marks in any social media posting or in your profile on any social media.
- 9.6. Any misuse of social media that you see should be reported to your manager.
- 9.7. Breach of this policy may result in disciplinary action up to and including dismissal. You may be required to remove any social media content that we consider constitutes a breach of this policy. Failure to comply with such a request may in itself result in disciplinary action.