Shotley Parish council

ELECTRONIC INFORMATION AND COMMUNICATIONS SYSTEMS POLICY - 2023

CONTENTS

CLAUSE

1. POLICY STATEMENT

1.1 Our electronic communications systems and equipment are intended to promote effective communication and working practices within our organisation and are critical to the success of our business. This policy outlines the standards we require users of these systems to observe, the circumstances in which we will monitor use of these systems and the action we will take in respect of breaches of these standards.

1.2 This policy does not form part of any employee's contract of employment and it may be amended at any time.

2. WHO IS COVERED BY THE POLICY?

2.1 This policy covers all individuals working at all levels, including Chair, Vice-Chair, Councillors, Committee and Working Group members, County and District Councillors, Clerk and Responsible Financial Officer, IT contractors, website editor and Locum Clerk/Rfo,

2.2 Third parties who have access to our electronic communication systems and equipment are also required to comply with this policy.

3. THE SCOPE AND PURPOSE OF THE POLICY

3.1 This policy deals mainly with the use (and misuse) of computer equipment, email, the internet, telephones, and voicemail, but it applies equally to the use of fax machines, copiers, scanners, CCTV, and electronic key fobs and cards.

3.2 Users specified at para 2.1 - members are expected to comply with this policy at all times to protect our electronic communications systems and equipment from unauthorised access and harm. Breach of this policy may be dealt with under our Disciplinary Procedure and, in serious cases, may be treated as gross misconduct leading to summary dismissal or loss of office.

4. PERSONNEL RESPONSIBLE FOR THE IMPLEMENTATION OF THE POLICY

4.1 The Clerk and Parish Council Chairman have overall responsibility for the effective operation of this policy but all members are equally responsible for adherence.

4.2 Users specified at para 2.1 are responsible for the success of this policy and should ensure that they take the time to read and understand it. Any misuse of our electronic communications systems or equipment should be reported to the Parish Clerk / PC chairman. Questions regarding the content or application of this policy should be directed to the Parish Clerk.

5. EQUIPMENT SECURITY AND PASSWORDS

5.1 The Clerk is responsible for the security of the equipment allocated to or used by them and must not allow it to be used by anyone other than in accordance with this policy.

Only the Clerk/Rfo and Chair are allowed access to the Parish Council email address. The Clerk is primarily responsible for answering/dealing with emails communications and no emails should be sent from the PC email address without prior knowledge/agreement from the Clerk.

During annual leave/sickness leave, the Chair may access the PC's email account and reply to communications of an urgent nature. An out of office automated response can be used to inform the person contacting the PC that their enquiry will be dealt by a certain date.

5.2 If given access to the email system or to the internet, the Clerk is responsible for the security of his/her terminal. If leaving a terminal unattended or on leaving the office they should ensure that he/she locks their terminal or log off to prevent unauthorised users accessing the system in their absence. Any member without authorisation should only be allowed to use terminals under supervision.

5.3 Desktop PCs /laptops and cabling for telephones or computer equipment should not be moved or tampered with without first consulting the Clerk-if applicable

5.4 Passwords are unique to each user and must be changed regularly to ensure confidentiality. Passwords must be kept confidential and must not be made available to anyone else unless authorised by the Chair of the Council following consultation with the Clerk. For the avoidance of doubt, on the termination of employment (for any reason), the Clerk/Rfo must provide details of their passwords to the Chair and return any equipment, key fobs or cards. The Chair must then ensure that passwords are changed immediately in line with GDPR.

5.5 Clerks/ Rfo's who have been issued with a PC/Laptop, I-Pad or mobile phone must ensure that it is kept secure/ encrypted at all times, especially when travelling. Passwords must be used to secure access to data kept on such equipment to ensure that confidential data is protected in the event of loss or theft. Clerks/Rfo's should also be aware that when using equipment away from the workplace, documents may be read by third parties, for example, passengers on public transport. In order to comply with GDPR, the Clerk must ensure that any restricted information is not displayed on any screen or able to be read by third parties.

6. SYSTEMS AND DATA SECURITY

6.1 The Clerk/Rfo and members of the Council should not delete, destroy or modify existing systems, programs, information or data which could have the effect of harming our business or exposing it to risk. The Clerk/RFO should always use backing up systems to protect important information.

6.2 The Clerk/Rfo should not download or install software from external sources without authorisation from the Chair of the Council. This includes software programs, instant messaging programs, screensavers, photos, video clips and music files. Incoming files and data should always be virus-

checked by the Clerk/Rfo before they are downloaded. If in doubt, the Clerk/Rfo should seek advice from the Chair. The following must not be accessed from the network: online radio, tv, video games or other such entertainment media.

6.3 Only equipment that has been PAT tested should be used.

6.4 The Clerk will monitor all emails passing through the PC's system for viruses. Members should exercise caution when opening emails from unknown external sources or where, for any reason, an email appears suspicious (for example, if its name ends in .exe). The Chair should be informed immediately if a suspected virus is received. The PC reserves the right to block access to attachments to emails for the purpose of effective use of the system and for compliance with this policy. The PC also reserves the right not to transmit any email message.

6.5 Members should not attempt to gain access to restricted areas of the network, or to any password-protected information, unless specifically authorised.

6.6 Clerks/Rfo's using laptops or Wi-Fi enabled equipment must be particularly vigilant about its use outside the office and take any precautions required by the Council from time to time against importing viruses or compromising the security of the system. The system contains information which is confidential to our business and/or which is subject to data protection legislation. Such information must be treated with extreme care and in accordance with our Data Protection Policy.

6.7 The PC must ensure that all systems used for business purposes, e.g. RBS accounting system, are securely backed up to a known recovery point whenever the system is used and updated.

6.8 The PC must ensure that all systems that are used for business purposes, e.g. RBS accounting system, are accessible by the Clerk and at least one other councillor so that business continuity is maintained in the event of unforeseen circumstances.

7. E-MAIL ETIQUETTE AND CONTENT

7.1 All Parish Councillors and the Clerk are provided with a dedicated email address which is to be used for all Parish Council electronic correspondence. Members should note that all Parish Council electronic correspondence may be subject to Freedom of Information requests.

7.2 Email is a vital business tool and should be used with great care and discipline. Council should always consider if email is the appropriate means for a particular communication and correspondence sent by email should be written as professionally as a letter. Messages should be concise and directed only to relevant individuals. Our standard disclaimer should always be included.

7.3 Clerk, Rfo and all Council members should not send abusive, obscene, discriminatory, racist, harassing, derogatory or defamatory emails. Anyone who feels that they have been harassed or bullied, or are offended by material received from a colleague via email should inform the Clerk/Chair. Complaints of such nature against Councillor members may be reported directly to the Monitoring Officer, particularly if there has been a breach of the Code of Conduct.

7.4 Members and the Clerk should take care with the content of email messages, as incorrect or improper statements can give rise to claims for discrimination, harassment, defamation, breach of confidentiality or breach of contract. Members and Clerk should assume that email messages may be read by others and not include anything which would offend or embarrass any reader, or themselves, if it found its way into the public domain.

7.5 Email messages may be disclosed in legal proceedings in the same way as paper documents. Deletion from a user's inbox or archives does not mean that an email cannot be recovered for the purposes of disclosure. All email messages should be treated as potentially retrievable, either from the main server or using specialist software.

7.6 In general, Members and the Clerk should not:

(a) send or forward private emails whilst carrying out PC work which they would not want a third party to read;

(b) send or forward chain mail, junk mail, cartoons, jokes or gossip;

(c) contribute to system congestion by sending trivial messages or unnecessarily copying or forwarding emails to those who do not have a real need to receive them;

(d) sell or advertise using our communication systems or broadcast messages about lost property, sponsorship or charitable appeals;

(e) agree to terms, enter into contractual commitments or make representations by email unless appropriate authority has been obtained. A name typed at the end of an email is a signature in the same way as a name written at the end of a letter;

(f) download or email text, music and other content on the internet subject to copyright protection, unless it is clear that the owner of such works allows this;

(g) send messages from another worker's computer or under an assumed name unless specifically authorised; or

(h) send confidential messages via email or the internet, or by other means of external communication which are known not to be secure.

7.7 Members and Clerk who receive a wrongly-delivered email should return it to the sender. If the email contains confidential information or inappropriate material (as described above) it should not be disclosed or used in any way.

7.8 E--mails from individual councillors to the Clerk automatically come into the public domain when received by the pc mail-box. This will facilitate the expedient response to any potential enquiries under the Data Protection or Freedom of Information Acts.

7.9 Councillors should make sure that they manage their mailboxes in an efficient manner and do not retain emails for longer than is necessary.

7.10 Upon receipt of any anonymous email, the Clerk will request that the sender identifies themselves in order to process the Email effectively. Should identification not be forthcoming, the sender will be notified that their email will not be able to be processed.

8. USE OF THE INTERNET

8.1 When a website is visited, devices such as cookies, tags or web beacons may be employed to enable the site owner to identify and monitor visitors. If the website is of a kind described in paragraph 11.2, such a marker could be a source of embarrassment to the visitor and us, especially if inappropriate material has been accessed, downloaded, stored or forwarded from the website. Such actions may also, in certain circumstances, amount to a criminal offence if, for example, the material is pornographic in nature.

8.2 The Clerk/Rfo, whilst using PC equipment, should therefore not access any web page or any files (whether documents, images or other) downloaded from the internet which could, in any way, be regarded as illegal, offensive, in bad taste or immoral. While content may be legal in the UK, it may be in sufficient bad taste to fall within this prohibition. As a general rule, if any person (whether intended to view the page or not) might be offended by the contents of a page, or if the fact that our software has accessed the page or file might be a source of embarrassment if made public, then viewing it will be a breach of this policy.

8.3 The Clerk/Rfo, whilst using PC equipment, should not under any circumstances use pc systems to participate in any internet chat room, post messages on any internet message board/social media sites or set up or log text or information on a blog or wiki, even in their own time. However, the controlled use of Social Media by way of brief informative, formal and objective posts is acceptable at certain times, particularly if in an attempt to reach a broader audience with any news items.

9. PERSONAL USE OF SYSTEMS

9.1 We permit the incidental use of internet, email to send personal email, browse the internet when researching items for the PC, subject to certain conditions set out below. Personal use is a privilege and not a right. It must be neither abused nor overused and we reserve the right to withdraw our permission at any time.

9.2 The following conditions must be met for personal usage to continue:

(a) use must be minimal and take place substantially out of normal working hours

(b) personal emails must be labelled "personal" in the subject header;

(c) use must not interfere with PC commitments;

(d) use must not commit the PC to any marginal costs; and

(e) use must comply with all pc policies (see paragraph 7, Email etiquette and content and paragraph 8, Use of the internet).

9.3 The Clerk/Rfo should be aware that personal use of PC systems may be monitored (see paragraph 10) and, where breaches of this policy are found, action may be taken under the

disciplinary procedure (see paragraph 11). The PC reserves the right to restrict or prevent access to certain telephone numbers or internet sites if we consider personal use to be excessive.

10. MONITORING OF USE OF SYSTEMS

10.1 Our systems enable the PC to monitor telephone usage and emails. For business reasons, and in order to carry out legal obligations in our role as an employer, use of our systems including the telephone and computer systems, and any personal use of them, may be monitored by the Chair. Monitoring is only carried out to the extent permitted or as required by law and as necessary and justifiable for business purposes.

10.2 We reserve the right to retrieve the contents of messages or check searches which have been made on the internet for the following purposes (this list is not exhaustive):

(a) to monitor whether the use of the email system or the internet is legitimate and in accordance with this policy;

(b) to find lost messages or to retrieve messages lost due to computer failure;

(c) to assist in the investigation of wrongful acts; or

(d) to comply with any legal obligation.

11. INAPPROPRIATE USE OF EQUIPMENT AND SYSTEMS

11.1 Access is granted to the internet, telephones and other electronic systems for legitimate business purposes only. Incidental personal use is permissible provided it is in full compliance with our rules, policies and procedures (see paragraph 9, Personal use of systems) and does not incur unauthorised expenditure.

11.2 Misuse or excessive use or abuse of the PC's telephone or email system, or inappropriate use of the internet in breach of this policy will be dealt with under our Disciplinary Procedure. Misuse of the internet can, in certain circumstances, constitute a criminal offence. In particular, misuse of the email system or inappropriate use of the internet by participating in online gambling or chain letters or by creating, viewing, accessing, transmitting or downloading any of the following material will amount to gross misconduct (this list is not exhaustive):

(a) pornographic material (that is, writing, pictures, films and video clips of a sexually explicit or arousing nature);

(b) offensive, obscene, or criminal material or material which is liable to cause embarrassment to the Parish Council,

(c) a false and defamatory statement about any person or organisation;

(d) material which is discriminatory, offensive, derogatory or may cause embarrassment to others;

(e) confidential information about the Parish Council or any of its members or associates (which you do not have authority to access);

(f) any other statement which is likely to create any liability (whether criminal or civil, and whether for you or the Parish council); or

(g) material in breach of copyright.

Any such action will be treated very seriously and is likely to result in summary dismissal.

11.3 Where evidence of misuse is found we may undertake a more detailed investigation in accordance with our Disciplinary Procedure, involving the examination and disclosure of monitoring records to those nominated to undertake the investigation and any witnesses or managers involved in the Disciplinary Procedure. If necessary, such information may be handed to the police in connection with a criminal investigation.

12. GDPR related policies and requirements are listed within their dedicated section and must be adhered to at all times.

Policy reviewed and approved by Council: March 2023 To be reviewed: March 2024