ICT POLICY – MISTLEY PARISH COUNCIL

1. Introduction

1.1 Mistley Parish Council uses its computer network, software packages and the internet, (including e-mails), to further the efficiency of its business and to provide the best service possible to its customers and partners. Any disruption to the use of these facilities will be detrimental to the Council and may result in actual financial loss. This Policy sets out how the Council intends to regulate the use of those facilities.

1.2 The Council has a duty laid down in the Data Protection Act 2018, to ensure the proper security and privacy of its computer systems and data. All users have, to varying degrees, some responsibility for protecting these assets. Users also have a personal responsibility for ensuring that they and, where appropriate, the staff they supervise or have control over, comply fully with this policy – See also the Council's Information and Data Protection Policy.

1.3 For the purposes of this document the terms "computer" (or "computer system") and "computer data" are defined as follows:

1.4 "Computer" (or "computer system") means any device for automatic storing and processing of data and includes mainframe computer, minicomputer, microcomputer, personal computer (whether hand-held laptop, portable, standalone, network or attached to a mainframe computer), workstation, word processing system, desk top publishing system, office automation system, messaging system or any other similar device;

1.5 "Computer data" means any information stored and processed by computer and includes programs, text, geographic, pictures, video and sound.

1.6 Failure to comply with any aspect of this policy may result in a breach of personal data as defined by the Data Protection Act 2018/UK GDPR. For more information, refer to the Council's Personal Data Breach Policy.

2. Procedures - 2.1 General Operation

2.1.1 All hardware, software, data and associated documentation produced in connection with the work of the Council, are the legal property of the Council.

2.1.2 The Council will maintain an external support contract for the hardware, major items of software and provision of internet facilities.

2.1.3 The Council will not knowingly breach copyright of another person.

2.1.4 The Council will include an assessment of risks from its use of IT in its Risk/Financial Risk assessment.

2.1.5 The Council will routinely back up its essential data and organise contingency plans.

2.1.6 The Council will make a detailed inventory of its ICT equipment on its Asset Register.

2.1.7 The Council will consider the location of equipment and provide documentation to ensure optimum physical security.

2.1.8 The Council will maintain a record of training to each individual user.

2.1.9 The disposal of any ICT equipment, software, waste or data must be authorised, undertaken safely and properly documented.

2.2 Copyright and licences

2.2.1 The Clerk is responsible for ensuring all computer software packages and non-electronic media for use within an information environment are used in accordance with the terms and conditions of use as set out in the licence agreement.

2.3 Compliance with Legislation

2.3.1 The Council's policy in respect of the requirements of the Data Protection Act 2018/UK GDPR is set out in its Information and Data Protection Policy.

2.3.2 Under the Computer Misuse Act 1990, the following are criminal offences, if undertaken intentionally:

- Unauthorised access to a computer system or data;
- Unauthorised access preparatory to another criminal action;
- Unauthorised modification of a computer system or data.

2.3.3 All users should be made aware that deliberate unauthorised use, alteration, or interference with a computer system or its software or data, whether proprietary or written "in-house", will be regarded as a breach of the Council policy and may be treated as gross misconduct. In some circumstances such a breach may also be a criminal offence.

2.3.4 It is an offence under the Copyright, Design and Patent Act to copy licensed software without the consent of the copyright owner. All copying is forbidden by the Act, unless it is in accordance with the terms and condition of the respective licence or contract.

2.4 Security

2.4.1 Consideration must be given to the secure location of equipment and documentation to help safeguard the Council's ICT assets. Portable equipment must be locked away when not in use and must not be removed from the premises without permission.

2.4.2 Only persons authorised by the Parish Clerk may use Council computer systems. The authority given to use a system must be sufficient but not excessive and users must be notified that the authority given to them must not be exceeded.

2.4.3 Operating procedures are required to control use of ICT equipment.

2.4.4 Security incidents relating to any aspect of this policy must be reported immediately to the Clerk.

2.5 Passwords

2.5.1 Access to the Council's computers is subject to a password and must be changed every six months.

2.5.2 System level passwords will be stored in a secure manner and be available in a business continuity event.

2.5.3 Passwords must not be inserted into email messages or other forms of communication.

2.5.4 Strong passwords contain upper and lower case characters, digits and punctuation characters, and are not based on personal information.

2.6 Emails

2.6.1 All emails that are used to conduct or support official Council business must be sent using a Parish Council/Parish Councillors email address. The Clerk should be copied into all correspondence.

2.6.2 Non-work email accounts must not be used to conduct or support official Council business.

2.6.3 All emails that represent aspects of Council business or administrative arrangements are the property of the Council.

2.6.4 Email is not always a secure method of communication. Personal data and confidential information should be sent as a password protected attachment with the password being communicated verbally to the recipient.

2.6.5 When sending an email to multiple recipients, use the blind copy (bcc) function so that recipients email addresses are not shared.

2.6.6 All Councillors and Officers will have the following email disclaimer:

Data Protection – personal data you provide to the Council will be processed in line with the UK GDPR.

For more information on how we maintain the security of your information and your rights, including how to access personal data that we hold on you and how to complain if you have any concerns about how your personal details are processed, please see our Privacy Notice.

This email, and any attachments, may contain Protected or Restricted information and is intended solely for the individual to whom it is addressed. It may contain sensitive or protectively marked material and should be handled accordingly. If this email has been misdirected, please notify the sender immediately. If you are not the intended recipient you must not disclose, distribute, copy, print or rely on any of the information contained in it or attached, and all copies must be deleted immediately.

Whilst we take reasonable steps to try to identify any software viruses, any attachments to this email may nevertheless contain viruses which our anti-virus software has failed to identify. You should therefore carry out your own anti-virus checks before opening any documents. Mistley Parish Council will not accept any liability for damage caused by computer viruses emanating from any attachment or other document supplied with this e-mail.

It should also be noted that emails and attachments (whether sent or received) may need to be disclosed under the UK GDPR, Data Protection Act 2018 or the Freedom of Information Act 2000.

2.6.7 IT facilities provided by the Council for email should not be used for:

- the transmission of unsolicited commercial or advertising material, chain letters, or other junk-mail of any kind, to other organisations.
- the unauthorised transmission to a third party of OFFICIAL SENSITIVE material concerning the activities of the Council.
- the transmission of material which would infringe the copyright of another person, including intellectual property rights.
- activities that unreasonably waste staff effort or use networked resources, or activities that unreasonably serve to deny the service to other users.
- activities that corrupt or destroy other users' data.
- activities that disrupt the work of other users.

- the creation or transmission of any offensive, obscene or indecent images, data, or other material, or any data capable of being resolved into obscene or indecent images or material.
- the creation or transmission of material which is designed or likely to cause annoyance, inconvenience or needless anxiety.
- the creation or transmission of material that is abusive or threatening to others, or serves to harass or bully others.
- the creation or transmission of material that either discriminates or encourages discrimination on racial or ethnic grounds, or on grounds of gender, sexual orientation, marital status, disability, political or religious beliefs.
- the creation or transmission of defamatory material.
- the creation or transmission of material that includes false claims of a deceptive nature.
- so-called „flaming" – i.e. the use of impolite terms or language, including offensive or condescending terms.
- activities that violate the privacy of other users.
- unfairly criticising individuals, including copy distribution to other individuals.
- publishing to others the text of confidential messages written on a one-to-one basis, without the prior express consent of the author.
- the creation or transmission of anonymous messages – i.e. without clear identification of the sender.
- the creation or transmission of material which brings the Council into disrepute.

2.6.8 Any user who is unclear about the appropriateness of any material, should consult the Clerk prior to commencing any associated activity or process.

2.6.9 There may be instances when a user will receive unsolicited mass junk email or spam. It is advised that users delete such emails without reading them. Do not reply to the emails and do not click on any links within the emails.

2.7 Confidentiality

2.7.1 All Councillors and Officers must maintain the confidentiality of information they access as part of their role. There are also particular responsibilities under Data Protection Act 2018 to protect personal data. Any queries should be directed to the Clerk.

2.7.2 Care should be taken to ensure that when addressing emails to prevent accidental transmission to unintended recipients. Particular should be take if the email software autocompletes email addresses.

2.8 Removable Media

2.8.1 Removable media needs to be managed effectively to ensure data is secure and to prevent any loss of data.

Removable media includes:

- Optical Disks (CDs, DVD+-R/RW, BluRays, Minidisks etc.)
- External Hard Drives.
- USB Flash Drives (also known as pen drives).
- Memory Cards (Compact Flash, SD Cards inc Mini and Micro, xD Cards,

- Sony Memory Stick in Micro M2, Smart media etc.)
- Embedded Microchips (including Smart Cards and Mobile Phone SIM
- Cards).
- Music and Video Players (MP3, MP4 etc.)
- Digital Cameras.
- Backup Cassettes.
- Audio Tapes (including Dictaphones and Answering Machines).
- Mobile Phones

2.8.2 Non-Council owned removable media devices must not be used to store information to conduct Council business and must not be connected to Council IT system.

2.8.3 Removable media must not be the only place where data is stored as it is liable to corrupt or lost. Copies of any data stored on removable media must also be remain on the source system until it has been successfully transferred.

2.8.4 All removable media devices must be scanned for viruses.

2.8.5 Data placed on removable media devices should be password protected.

2.8.6 All removable media devices that are no longer required or have become damaged should be disposed of securely via the IT support contractor.

2.9 Misuse

2.9.1 This Policy applies to the activities which constitute unacceptable use of the network operated by the Council. The policy applies equally to employees, Councillors, clients, visitors and others who may be allowed to use the facilities on a permanent or temporary basis.

2.9.2 All misuse of the facilities is prohibited as documented under the Emails section above, and deliberate actions or activities with any of the following characteristics:

- Wasting staff effort or networked resources;
- Corrupting or destroying another users data;
- Disrupting the work of other users;
- Other misuse of networked resources by the deliberate introduction of viruses;
- Playing games during working hours;
- Private use of the facilities without specific consent;
- Altering the set up or operating perimeters of any computer equipment without authority.

2.10 World Wide Web (WWW) resources

2.10.1 These facilities are provided for use to achieve Council objectives. Any use for unauthorised purposes will be regarded as gross misconduct. If you are unsure whether use would be authorised, you must seek advice from the Parish Clerk in advance.

2.11 Health and Safety

2.11.1 Computers are now a part of everyday life. If they are not used correctly, they can present hazards. Computers may be called Display Screen Equipment (DSE), Visual Display Units (VDU's) and the immediate environment where they are used i.e. desk/chair etc. is referred to as a workstation.

2.11.2 The Display Screen Equipment Regulations, 1992 regulate the use of computers at work and refer to the persons affected as "users".

2.11.3 "Users" are persons who "habitually use VDU's as a significant part of their normal work and regularly work on display screens for two/three hours each day or continuously for more than one hour spells". The Regulations also apply to employees working at home.

2.11.4 To meet the requirements of the Display Screen Equipment Regulations, the Council will provide a free eye test for all staff who use VDU equipment as a major part of their job role.

2.11.5 It is the Council's intention to optimise the use and application of display screen equipment within the Organisation, whilst safeguarding the health, welfare and job satisfaction or learning experience of those involved in using such equipment.

2.11.6 Staff "users" will have their name entered onto the list of "Designated Computer Users".

2.11.7 Risk assessments of all workstations are carried out to highlight any problems – this is done using the Workstation Assessment Questionnaire which is also a useful training tool.

2.11.8 If you are a "defined computer user":

- Your workstation must be designed for computer use. There must be sufficient space to position your keyboard so that you can rest your wrists in front of it;
- The screen should be fully adjustable and must be positioned to avoid glare from lights, windows etc.;
- Your chair must be of the fully adjustable type with five castors and must be adjusted to support your lower back. It must be set at the correct height for your desk. Your feet should rest on the floor and you may need a footrest;
- Report eyestrain, headaches or aching limbs to your Line Manager;
- Ensure your computer has an adjustable keyboard;
- Ensure your working environment is comfortable. Problems with ventilation, temperature or lighting should be reported to your Line Manager;
- Take a few minutes break every hour.

3. Mistley Parish Council's Website

3.1 Background

3.1.1 The Council's website can be found at https://www.mistleyparishCouncil.gov.uk

3.2 Updating the Site

3.2.1 The site will be updated on a daily basis or when required by Parish Council's Clerk. It is important that the site remains fresh, relevant and current. Should Councillors wish to have any content added or amended, please inform the Clerk.

3.2.2 Agendas will be uploaded onto the site at least 3 days prior to meeting dates. Minutes will be uploaded within the timeframe documented in the Council's Standing Orders.

3.2.3 Councillor details can be found on the website. Also listed are any Appointments to Outside Bodies and any Declarations of Interests, if any changes need to be made the Parish Clerk must be informed.

Review Body: Full Parish Council. Review period – annually each May. Adopted 30.06.25. Review Date May 2026.