CLYMPING PARISH COUNCIL

IT - INFORMATION SECURITY POLICY

1. Introduction

1.1 Clymping Parish Council considers the security of electronic information to be very important.
1.2 This Policy sets out how the Council will establish and maintain the security and confidentiality of information held within its care and how it will ensure the lawful and correct treatment of personal data.
1.3 An up-to-date copy of this Policy shall be maintained on Clymping Parish Council's website.

2. Purpose

2.1 The purpose of this Policy is to ensure that as far as is reasonable practicable:

- The public and all users of the Council's information systems are confident of the confidentiality, integrity, and availability of the information used and produced
- Business damage and interruption caused by security incidents are minimised
- All legislative and regulatory requirements are met
- The Council's ICT equipment and facilities are used responsibly, securely and with integrity at all times

3. Scope

3.1 This policy applies to all information held by employees, Councillors and to any individual /organisation under contract to the Council.
3.2 All Councillors and employees of Clymping Parish Council have a legal responsibility to maintain the confidentiality, integrity and security of data held.
3.3 This policy applies throughout the lifecycle of the information, from creation, storage, use and disposal. It applies to all information including:

- Information stored electronically on databases or applications e.g. e-mail
- Information stored on computers, laptops or removable media such memory sticks.
- All paper records
- Spoken, including face-to-face, voicemail and recorded conversation

4. Legal and Regulatory Requirements

4.1 The Data Protection Act 1998 (DPA) and General Data Protection Regulations 2018 (GDPR) sets out high standards for the handling of personal information and protecting individuals' rights to privacy. It also regulates the ways in which personal information can be collected, handled and used.
4.2 The Parish Council fully endorsees and adheres to the principles of data protection as detailed in the DPA 1998 and the GDPR 2018. To this end, the Parish Council will ensure that personal data will be:-

- processed fairly and lawfully
- obtained only for lawful and specific purpose(s)
- adequate, relevant and not excessive in relation to the purpose for which it was collected
- accurate and where necessary kept up to date

- kept for no longer than is necessary for the purpose for which it was collected
- processed in accordance with the rights of the data subjects
- kept securely

5. Email communication

5.1 Email accounts provided by Clymping Parish Council are for official communication only.

5.2 Emails should be professional and respectful in tone. Confidential or sensitive information must not be sent via email unless it is encrypted.

5.3 Be cautious with attachments and links to avoid phishing and malware. Verify the source before opening any attachments or clicking on links.

5.4 Every authority must have a generic email account hosted on an authority owned domain, for example clerk@abcparishcouncil.gov.uk or clerk@abcparishcouncil.org.uk.

6. Information Security

6.1 The Parish Council will ensure that all information whether stored electronically or as paper records will be stored securely to ensure that:

- only authorised people can access, alter, disclose or destroy any personal data
- Councillors and employees of the Parish Council only act within the scope of their authority
- if personal data is accidentally lost, altered or destroyed, it can be recovered to prevent any damage or distress to the individuals concerned.
- All personal information held by the Parish Council will be kept in a secure location and not available for public access.
- All data stored on a computer will be password protected.

7. Policy Review

Clymping Parish Council will review this policy as is necessary and appropriate, and at a minimum on an annual basis.