RAYNE PARISH COUNCIL PERSONAL DEVICE AGREEMENT

1. **Purpose and scope**

   Rayne Parish Council (The Parish Council) is committed to protecting personal data in compliance with the General Data Protection Regulation (GDPR) and other applicable data protection laws. This policy outlines the measures and controls in place to ensure the secure handling of personal data communicated through personal electronic devices. All councilors have to use personal electronic devices to access the business of the Parish Council. By signing this agreement, councilors acknowledge the risks associated with the use of privately owned devices for Council purposes and consents to Council controls and technical enhancements designed to protect the Council and its information, networks and data. It is current policy that only the Clerk is issued with a laptop to undertake Council business.

2. **Definitions**

   2.1 **Personal Data** refers to any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, by reference to an identifier such as a name, an identification number, location data, an online identifier, or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person.

   2.2 **Device -** this includes but is not limited to a Personal Computer, laptop, tablet or smart phone.

   2.3 **Use of data covered –** accessing, viewing, storing or otherwise processing data to include (without limitation):

   - Correspondence
   - Reports
   - Documents
   - Manuals
   - Council Policies
   - Electronic or printed information
   - Voicemail
   - Photographs

3. **Requirements**

   All Councilors and staff shall comply with the following requirements -

   3.1 You must access council information only via a secure server or a Virtual Private Network (VPN) to ensure data encryption and protection against unauthorized access.

   Examples being a secure work place network or if you are accessing the information from a home network you will ensure that the home network security functions are enabled.

3.2 Your device must be protected by up-to-date anti-virus and anti-malware software to prevent security breaches. You must not access council information using public Wi-Fi services unless connected through a secure VPN to mitigate the risk of data interception, for example those provided by restaurants, due to the lack of security.

3.3 You must use your parish council email account exclusively for council business and ensure it is protected with strong, unique passwords and/or two-factor authentication (2FA), and ensure the email account is kept secure so that council personal information is not disclosed to any unauthorized third party

3.4 You must not send any council personal information to any unauthorized person thus it may not be sent to anyone other than Councilors, the Clerk or an authorized third party contracted to the Parish Council (e.g. payroll provider).

3.5 To ensure that no unauthorized third party may access personal information your device must be password protected

3.6 You should take care that when accessing or communicating personal data no 'eavesdropping' from unauthorized third parties occurs

3.7 To ensure adequate security, council information must not be stored using unauthorized file-sharing solutions. Only the Council's approved Cloud-based sharing system, which complies with GDPR requirements, should be used.

4. Incident Reporting

4.1 In compliance with GDPR reporting requirements, any data breach or loss of data must be reported immediately, and no later than within 24 hours, to the Data Protection Officer or the Clerk. This enables timely reporting to the relevant supervisory authority and affected individuals, if necessary. For example, if council information is stored on a laptop which was stolen this would need to be reported.

5. Data Retention and Disposal

5.1 The Document Retention and Disposal Policy adopted by the Parish Council applies equally to electronic data. All electronic data must be managed and disposed of in strict accordance with this policy to ensure compliance with data protection regulations and to prevent unauthorized access.

6. Device Disposal

6.1 Any disposal of an electronic device must be conducted securely, following the Council's approved data destruction procedures, to ensure that personal information cannot be accessed or retrieved. This includes physical destruction or certified data wiping methods.

6.2 You are aware that when your association/employment with the parish council ends, access to Council data, emails, etc. will be removed remotely.

7. Password Management

7.1 You are required to change your passwords for email, website, and cloud access every 6 months. Passwords must be strong, unique, and comply with the Council's password policy, which includes the use of a password manager for secure storage.

7.2 As the protection of our data is paramount, any Councilor or employee who does not sign this document will not be granted extension permission to access Parish Council data and emails via personal devices. Access will be via the Web Based application only. This does not hinder your ability to be a Councilor or an employee or receive all parish council data, just the way it is received.

Training and Awareness: Regular training sessions should be conducted to ensure all councillors and staff are aware of the latest data protection practices and the importance of compliance.

Policy Review: The policy should be reviewed more frequently, at least bi-annually, to ensure it remains up-to-date with evolving data protection laws and technological advancements.

I confirm that I have read this document and will comply with the requirements as set out above

Signed……..

Dated……