Kenn Parish Council

IT and Digital Compliance Policy

1, Purpose and Scope.

1.1 This policy sets out how Kenn Parish Council (the Council) will manage its digital operations, data handling, and IT systems to ensure they are legal, secure, and accessible.

1.2 It applies to:

- All Councillors, and employees acting on behalf of the Council.
- All IT equipment, software, services, websites, cloud storage, communications And data used or processed for Council purposes.
- Use of both Council owned and personal devices when used for council business.

2, Legal and Regulatory Requirements.

2.1 The Council is subject to, but not limited to, the following legislation and regulations:

- The UK General Data Protection Regulation (UK GDPR) and Data Protection Act 2018
- The Freedom of Information Act 2000
- The Public Sector Bodies (Website and Mobile Applications) No 2 Accessibility Regulations 2018.
- Web Content Accessibility Guidelines (WCAG) 2.2 AA standard.
- The Transparency Code for Smaller Authorities.

2.2 The Council acts as both Data Controller and, where processing is delegated, data processer.

3, Email and Official Communication.

3.1 Users must only use the official email account on a domain owned by the Council. Which is **Kennparishcouncil.gov.uk** for Council business. This ensures that the service is Secure and backed up. Other email services such as Gmail or Hotmail or those belonging to private companies must not be used for Council business.

3.2 All official publications, correspondence and records must use Council owned email and Domains.

3.3 Emails must not be routinely forwarded to personal accounts.

3.4 council email addresses are for council use only, and not for private communications.

4, Data Protection and Managing Personal Data

4.1 The Council will only process personal data where there is a lawful basis under UK GDPR.

4.2 Personal data shall be

- Collected for specified explicit and legitimate purposes.
- Adequate relevant and limited to what is necessary.
- Accurate and kept up to date.
- Stored Securely.
- Kept no longer than necessary.
- Processed to ensure appropriate security.

4.3 Risk assessments will be undertaken for data processing tasks involving sensitive data, large volumes, or third party processing.

4.4 Where personal devices are used for Council business, they must be secured (passwords, encryption, antivirus).

4.5 Data breaches must be reported under the Councils data breach policy and statutory Requirements.

5, Council Website

5.1 The Council website must be hosted by a reputable web hosting company based in the UK And use the official Kennparishcouncil.gov.uk domain. This ensures that the service is secure and backed up.

5.2 The Council website must comply with WCAG 2.2 AA standards.

5.3 The Council website must publish all documents under the transparency Code, (agendas, minutes, accounts, governance statements, audit reports, councillor responsibilities).

5.4 An Accessibility statement must be published, explaining compliance status, Known issues, and contact details for accessible versions.

5.5 Regular reviews of the website must be conducted to ensure compliance and accuracy.

6, Security Management

6.1 Council owned laptops shall have anti-virus software and firewalls installed, and software shall Be regularly updated so it is current and supported by the manufacturer.

6.2 Users must use strong, unique passwords to protect council IT services and information, and Not share these with anyone else.

6.3 Passwords must not be stored or written down in insecure locations.

6.4 Councillors are only to store Council data on their device in a password protected Location and ensure that data is secure and backed up.

6.5 Council equipment changes require authorisation.

6.6 Access control must be used on group meeting channels (Zoom, Team's) to ensure that users only have read and update access to information that is required to fulfil their role.

6.7 Personal devices used for Council business must only be used where they do not pose a Security risk to Council data, and where stored on the device cannot be accessed by other Users. The operating system and other software on such devices should be kept up to date And supported by the manufacturer.

7, Social Media

7.1 Social Media includes blogs, social network sites such as Facebook, X, Instagram, Tic Tok, Multimedia or user generated sites such as You Tube.

7.2 Only designated employees may operate the Council controlled social media sites.

7.3 All social media posts must be lawful. (No publication of sensitive personal data, defamatory statements, or confidential information).

7.4 All communications must be professional following the Nolan principles and reflect Council values.

8, Training, Responsibility and Review

8.1 The clerk is responsible for ensuring compliance with this policy.

8.2 Training will be provided to all users in all areas including data protection, cybersecurity, and social media.

8.3 This policy will be reviewed annually or upon legislative or technical change.

9, Incidents, Compliance and Audits

9.1 All users are to report suspected breaches of security and suspected incidents of noncompliance with this policy to the clerk immediately.

9.2 The clerk will initiate an appropriate investigation of breaches and incidents.

9.3 Breaches of the policy may result in disciplinary action against employees or councillors, and reporting to the District authority monitoring officer for councillors.

9.4 The Council will periodically perform compliance audits.

10,

10.1 All software used by the council will be properly licenced and purchased.

10.2 All software used by the Council will be obtained from reputable sources.

11, Hardware

11.1 Council computer equipment is provided for Council use only.

11.2 Council computer and other electronic devices should be always treated with care and kept clean.

11.3 All Council computers and electronic equipment must be stored safely and securely when not in use.

11.4 An inventory of all council computers and electronic equipment should be maintained.

12, Authorities and References

- Data Protection Act 2018
- Freedom of information Act 2000
- Public Sector Bodies (websites and Mobile Applications) (No2) Accessibility regulations 2018
- Transparency Code for Smaller Authorities
- The Practitioners guide 2025 (assertion 10)