Assertion 10

1. **Digital Security & Email: Mandatory use of council-owned domain email addresses rather than personal emails.**

The Parish Council has a .gov domain and all staff and Councillors are issued with a parish council email address. GDPR training annually reinforces the need to only use this account for Council business.

2. **Website Accessibility: Websites must meet WCAG 2.2 AA standards and display an up-to-date accessibility statement.**

The Council has reviewed its website for compliance with WCAG 2.2AA guidance and updated its Accessibility Statement.

3. **Data Protection Compliance: Active management of data, including data audits, risk assessments, and adherence to UK GDPR and the Data Protection Act 2018.**

The Council employs the services of Maureen Chaffe of Processmatters2 as External Data Protection Officer whose role is:

- to inform and advise about obligations to comply with the GDPR and other data protection laws.
- to monitor compliance with the GDPR and other data protection laws.
- to raise awareness of data protection issues, initial training of all staff and conducting one internal audit per annum.
- to advise on, and to monitor, data protection impact assessments.
- to cooperate with the supervisory authority; and
- to be a point of contact for supervisory authorities and for individuals whose data is processed (employees, customers etc).

The Council has a suite of policies which are updated annually and staff and Councillors undertake annual GDPR training.
A data audit has been undertaken and a data retention schedule and Privacy Policy created.

A Privacy Impact Assessment is mandated for all new projects which involve the collection of data. These are signed off by the External Data Protection Officer and any necessary amendments to the Privacy Policy and Retention Schedules are made.
A clear audit trail demonstrating proactive management of digital and data risk is provided by the IT support company and accessible upon request by the External DPO.

4. IT & Governance Policies: Adoption of specific policies, including a Data Protection Policy and an IT Policy regulating the use of equipment, to reduce cyber risks.

The Council has an IT Security Policy which is signed by all staff and Councillors. The IT supplier JNR Computers Ltd provides a layered security model which provides:

- Enterprise-grade protection normally seen only in much larger organisations:
- Advanced endpoint protection and real-time threat detection
- Professional email filtering to reduce phishing and impersonation risk
- Strong identity security using multi-factor authentication and conditional access
- Continuous cyber security monitoring and alerting
- Independent ("out of zone") Microsoft 365 backup with long-term retention

Microsoft 365 Backup ("Out of Zone")

Many councils now use the term "out of zone" to describe backups that are held separately from the live Microsoft 365 environment used day-to-day. In practical terms, this means council email and documents are copied into an independent backup environment, so they remain recoverable even if the live tenant is affected by an incident.

This separation strengthens governance and audit confidence. It supports the expectation that backups of digital records are performed regularly and secured, and it provides a clear internal-control measure that can be evidenced during review and audit.

- Separate backup environment (independent of the live Microsoft 365 tenant) for stronger resilience
- Recovery capability after accidental deletion, malicious deletion, ransomware, or account compromise
- Protection against wider service disruption that impacts access to Microsoft 365 (including regional outages)
- Long-term retention to protect historic council records

Recognised Standards and Public-Sector Credentials

JNR Computer Services operates to nationally recognised standards and is aligned with public-sector cyber security expectations. This provides additional assurance that your

chosen provider meets established best practice:

- Cyber Essentials certified, demonstrating independently assessed baseline cyber security controls
- Registered IT provider for Parish and Town Councils with the Department for Science, Innovation and Technology (DSIT)
- Alignment with public-sector digital governance and compliance expectations
- Supplier assurance suitable for audit and insurance purposes

Alignment with AGAR Assertion 10 and Audit Requirements

JNR's solution supports a positive response by providing:

- Documented IT and cyber security controls supporting risk management
- Managed monitoring, backup, and recovery arrangements evidencing internal control
- A secure Microsoft 365 environment configured and managed for governance and compliance
- A clear audit trail demonstrating proactive management of digital and data risk
- Independent certification and government-aligned registration supporting auditor assurance

Microsoft 365

Microsoft 365 is a powerful platform, but only when configured and managed correctly. JNR ensures that councils benefit from:

- Encryption of council data in transit and at rest
- Secure use of email, OneDrive, SharePoint, and Teams
- Rapid recovery from accidental deletion or ransomware incidents
- Data loss prevention controls to reduce human error
- UK and EU-aligned data residency and compliance requirements

5. Transparency Code: : Ongoing compliance with the Local Government Transparency Code 2015 is required, particularly for councils with expenditure exceeding £25,000.

The Parish Council has a Publication Scheme which sets out the classes of information routinely available, such as policies and procedures, minutes of meetings, annual reports and financial information. The Council uses the parish council website to make most of this information available.

The Parish Council publishes the financial information required of it under the Transparency Code.