**AGAR Assertion 10 – IT and Digital Governance Report**

Produced by the Clerk – 5th March 2026

1. **Purpose of Report**

For the financial year 2025/26, Assertion 10 of the Annual Governance and Accountability Return (AGAR) requires the Council to confirm:

"The authority has taken steps to manage its risks and reviewed the adequacy of its system of internal control."

This report outlines the actions taken to ensure compliance with this requirement in respect of IT governance, digital infrastructure, data protection and transparency.

**2. IT Policy**

The Parish Council adopted a new IT Policy in November 2025. This policy will be updated again (in April or May 2026) in line with the latest template issued by the National Association of Local Councils (NALC).

The revised policy:

- Mandates use of council-owned email accounts for official business
- Sets expectations for password security and device usage
- Clarifies responsibilities regarding data protection and cyber security
- Supports compliance with GDPR and FOI obligations

Council approval of the updated policy is recommended. It is also recommended that there is no further use of personal emails as from the **30th April 2026.** The Clerk will only circulate council business to council-owned email addresses from 1st May 2026.

**3. Data Audit**

A full Data Audit was completed on 3rd March 2026. The audit identifies the types of data held, storage locations, access controls, retention periods and any required actions.

The data audit will be reviewed annually.

**4. Website and Digital Infrastructure**

The Council:

- Owns and controls its website domain and official email accounts
- Uses authority-owned email addresses for council business
- Maintains an up-to-date Publication Scheme
- Routinely publishes financial information via the website and newsletter (Finance tab, agenda and minutes tabs on the website)

**5. Website Accessibility**

The Council website was last tested against Web Content Accessibility Guidelines (WCAG) 2.2 AA on 24th February 2026. Testing was carried out using recognised accessibility evaluation tools and an Accessibility Statement is published on the website https://warsop-pc.gov.uk/accessibility-statement/

Test carried out on 24th February (AIM Score 9.4 / 10) at:
https://wave.webaim.org/report#/warsop-pc.gov.uk

## 6. Data Protection & GDPR

The Clerk acts as the Council's Data Protection Officer. The GDPR Policy, Data Breach Policy and GDPR Risk assessment were last updated in January 2026. The Council maintains Data Protection policies, privacy notices, Subject Access Request procedures and data breach procedures.

To further strengthen compliance, the Clerk will aim to attend GDPR refresher training during 2026.

## 7. Transparency & Publication Requirements

The Council has adopted the ICO Model Publication Scheme (renewed again March 2026) and publishes financial information in accordance with the Transparency Code for Smaller Authorities. AGAR, budgets, payments and governance documents are published on the website.

## 8. Digital Infrastructure & Risk Management Report

The Council has a consolidated Digital Infrastructure & Risk Management Report – see Annex 1.

- IT asset register
- Backup arrangements
- Cyber security measures
- Accessibility review schedule
- Data audit review cycle

## 9. Conclusion and Recommendations

The Clerk is satisfied that the Council has taken appropriate steps to manage digital and governance risks. Council is asked to:

1. Note the contents of this report

2. Approve an updated IT Policy as soon as possible (based on the new NALC model) to replace the existing IT Policy

3. Confirm satisfaction with digital governance arrangements in terms with the SAPPP 2025 guidelines for Assertion 10 compliance.

**Extract from SMALLER AUTHORITIES PROPER PRACTICES PANEL - PRACTIONERS' GUIDE 2025**

5.117.Data protection and security - Using authority-owned email accounts ensures that sensitive information is handled in a controlled environment with appropriate security measures. This aligns with GDPR principles such as data minimisation, integrity and confidentiality.

5.118. Accountability and transparency - authority-owned email accounts provide a clear record of communications, which is essential for transparency and accountability.

This helps in maintaining an audit trail and ensures all authority-related communications are accessible for review if needed.

5.119. Consistency, trust and professionalism - it is best practice to use .gov.uk domains for smaller authorities' emails and websites (excluding parish meetings). This helps maintain a consistent and professional image for the authority and ensures all communications are easily identifiable as coming from the authority. This is increasingly important as cyber scams are on the rise. For support on setting up a gov.uk domain for your smaller authority you can follow the guidance on moving your parish council to a .gov.uk domain. .org is second best option – confirmed as acceptable

5.120. Having authority-owned email accounts also makes Data Subject Access and

Freedom of Information Requests easier to manage.

5.121. Compliance with policies - All authorities should have an IT policy that mandates the use of authority-owned email accounts for official business. These policies are designed to ensure that all communications are conducted in a manner that is consistent with the authority's standards and legal obligations

5.122. IT Policies - An IT policy prevents misunderstandings when using IT equipment for authority business and makes sure that there can be no excuses for anyone in your authority not protecting their data or working safely. If your authority does not have a policy, you might like to use this IT policy template. It is important to personalise the template for the specific use of your authority and add links to guidance where needed.

5.123. Website accessibility - Where a smaller authority is subject to the requirements of website accessibility it does not have to buy a new website to comply with accessibility law if it places a disproportionate burden on the authority. At a minimum all authorities' websites must include an accessibility statement on their website and keep it under regular review. This statement should include reasons for not meeting accessibility requirements, ways to source alternative copies of non-accessible documents and a point of contact.

5.124. Data Protection - To ensure compliance with data protection regulations, smaller authorities must:

• Appoint a Data Protection officer to oversee data protection and ensure

compliance with GDPR.

• Conduct regular data audits to identify what personal data is held, how it is

used and make sure it is processed lawfully.

• Implement a Data Protection policy on data handling, storage and sharing.

• Provide regular training to ensure all staff and members are trained on data protection principles and practices.

• Secure data using appropriate technical and organisational measures to protect personal data from breaches.

5.125. The Freedom of Information Act places a duty on every public authority to adopt and maintain a publication scheme which details the publication of information by the authority and is approved by the Information Commissioner; adoption of the Information Commissioners Office model publication scheme meets this requirement.

5.126. In addition to this the Transparency Code for Smaller Authorities requires parish councils, internal drainage boards, charter trustees and port health authorities with an annual turnover not exceeding £25,000 to publish certain information set out in the code. This enables local electors and local taxpayers to access relevant information about the authority's accounts and governance.

5.127. Smaller Authorities with total turnover or expenditure greater than £25,000 should as best practice comply with the Local Government Transparency Code 2015; the government believes that in principle all data held and managed by local authorities should be made available to the public unless there are specific sensitivities to doing so.

5.128. Monitoring an authority's compliance with the relevant transparency code is not part of the external auditor's limited assurance review of the AGAR. It would however be expected that internal auditors would review this control area.

Annex 1 – Digital Infrastructure

**Digital Infrastructure & Risk Management Report**

## Report Details

**Organisation:** Warsop Parish Council

**Report Owner:** Jade Wilson, Clerk

**Reporting Period:** April 2026-March 2027

**Date Prepared:** 4th March 2026

**Next Review Date:** March 2027

## IT Asset Register

| Asset Type | Quantity | Owner | Location/Hosting | Criticality | Last Reviewed |
|---|---|---|---|---|---|
| Website | 2 | WPC | Parish Online & JKE Web Design | High | 26/02/2026 |
| 4G/5G Wifi Router | 1 | WPC | Onecom | Medium | 26/02/2026 |
| | | | | | |

## Backup & Disaster Recovery

| System/Data | Backup Method | Frequency | Storage Location | Encryption | Retention | Last Tested |
|---|---|---|---|---|---|---|
| Website | Host/Parish Online | Nightly | Host web servers | 2 Factor Authentication | Ongoing | 24/02/2026 |
| Email | Parish Online (Zoho) | Nightly | Host web servers | 2 Factor Authentication | As long as required | 24/02/2026 |
| | | | | | | |

## Cyber Security Measures

| | |
|---|---|
| Information Security Policy in place | Yes |
| Multi-Factor Authentication enabled | Yes, where required |
| Endpoint protection deployed | Yes |
| Firewall/network security | Yes – Windows Defender |

| | |
|---|---|
| Email security & anti-phishing | Yes |
| Patch management process | Yes  regular updates to plugins and websites etc. |
| Vulnerability scanning | Yes |
| Security awareness training | No – to be reviewed. |

## Accessibility Review Schedule

| System/Service | Review Type | Frequency | Last Review | Next Review | Owner |
|---|---|---|---|---|---|
| Website Accessibility Features | Practical test | 12 months | 24/02/26 | 02/27 | WPC |

## Data Audit Review Cycle

| Audit Type | Scope | Frequency | Last Completed | Next Due | Responsible |
|---|---|---|---|---|---|
| Access Control Review | User permissions for Website, Emails, and Bank Account | Every 12 months | December 2025 | May 2026 | Jade Wilson (Clerk) |
| Data Retention Review | A check of the data held and shared with partners | Every 12 months | February 2026 | 2027 | Jade Wilson (Clerk) |

## Digital Risk Register

| Risk ID | Description | Likelihood | Impact | Mitigation | Owner | Review Date |
|---|---|---|---|---|---|---|
| VIR01 | Virus attack on personal devices | Low | High | Update personal devices with latest operating system updates | Jade Wilson , Clerk | 02/2027 |
| VIR02 | Virus or hacking attack on council website(s) | Medium | High | Update plugins regularly, use security, and remove unused third-party content. | WPC | 02/2027 |