ASSERTION 10 – HOLBROOK PARISH COUNCIL

Including:

1. Data Map
2. AGAR Assertion 10 Summary
3. Data-Flow Description
4. Data-Protection Risk Register

In order to comply with WCAG 2.2 AA, All content uses:

- Clear hierarchical headings
- Short sentences
- Plain English
- No tables
- No colour-dependent meaning
- No special characters that screen readers struggle with
- Bullet points instead of complex layouts
- Consistent structure

1. DATA MAP - ACCESSIBLE VERSION

Section A: Governance and Administration

Councillor Contact Details

- Data held: Names, addresses, email addresses, phone numbers
- Purpose: Meeting administration and statutory notices
- Lawful basis: evidence and support for councillor role
- Storage: Council email system and secure cloud folder
- Access: Clerk and Chair
- Retention: Duration of term plus one year
- Risks: Data leakage
- Controls: Council email domain, access controls

Register of Interests

- Data held: DPI forms – held electronically by HPC and Babergh DC
- Purpose: Transparency

- Lawful basis: Legal obligation
- Storage: Website/District Council and clerk's secure folder
- Access: Clerk and public
- Retention: As required by Monitoring Officer
- Risks: Over-publication
- Controls: Redaction of sensitive data and accessibility checks

Section B: Staffing and HR

Employee Records

- Data held: Contracts, payroll information, appraisals
- Purpose: Employment management
- Lawful basis: Contract
- Storage: Secure HR folder
- Access: Clerk and Chairman
- Retention: 3 years after employment ends
- Risks: Unauthorised access
- Controls: Encryption and restricted access

Section C: Finance and Payments

Supplier Details

- Data held: Names, addresses, bank details
- Purpose: Payments and financial administration
- Lawful basis: Contract and management of PC functions
- Storage: Accounting software and online banking portal
- Access: Clerk/Bank signatories
- Retention: Seven years
- Risks: Fraud or unauthorised access
- Controls: Multi-factor authentication and audit trail

Grant Applications

- Data held: Contact details and project information

- Purpose: Awarding grants
- Lawful basis: Public task
- Storage: Secure cloud folder
- Access: Clerk and Councillors
- Retention: Seven years
- Risks: Over-sharing
- Controls: Redaction before publication

Section D: Communications and Engagement

Mailing Lists

- Data held: Names and email addresses
- Purpose: Sending letters, important information and updates
- Lawful basis: Consent
- Storage: Parish Council email account
- Access: Clerk
- Retention: Until consent withdrawn
- Risks: Spam complaints
- Controls: BCC for circular emails other than Councillors

Section E: IT Systems and Infrastructure

Council Email System

- Data processed: All council correspondence
- Risks: Loss, theft, personal devices used for council work
- Controls: Council-owned domain, multi-factor authentication, IT policy

Website

- Data processed: Published documents
- Risks: Accessibility issues and hacking
- Controls: WCAG 2.2 AA compliance, regular updates

Cloud Storage

- Data processed: Governance and finance files

- Risks: Unauthorised access
- Controls: permissions review

Councillor Devices

- Data processed: Emails, agendas, documents
- Risks: Mixing personal and council data
- Controls: Encryption and regular GDPR information and updates

2. AGAR ASSERTION 10 SUMMARY

Parish Council: **Holbrook Parish Council**

AGAR Year: 2025-2026

Assertion 10: Compliance with GDPR and the Data Protection Act 2018

Summary of Evidence

- A full data map has been completed
- Lawful bases identified for all processing activities
- Storage locations reviewed and documented
- Access controls in place, including multi-factor authentication and encryption
- Retention schedule adopted and followed
- Privacy notices updated and published
- Data processing agreements in place with all relevant providers
- Security measures implemented including updates, password policy and Backups
- Data breach procedure documented and reviewed
- Councillors have received regular (at least annual) GDPR refresher Information

This summary forms part of the council's AGAR evidence pack.

3. DATA-FLOW DESCRIPTION

Resident to Council Contact Flow

- Resident submits a message to Council
- Message is sent to the clerk's email and sensitive data redacted/removed if forwarded to councillors for consideration/decision making

- Information is stored in secure cloud storage
- Data is retained or deleted according to policy

Supplier Payment Flow

- Supplier submits invoice
- Clerk receives invoice by email
- Information is entered into accounting software
- Payment is made through the bank portal
- Records are retained for audit

Councillor Document Flow

- Councillor sends or receives documents via council email
- Documents are stored in cloud storage
- Some documents may be published if required for transparency purposes.

Employee HR Flow

- Employee provides HR documents
- Clerk stores documents in encrypted HR folder
- Payroll provider processes salary
- HMRC receives required information

4. DATA-PROTECTION RISK REGISTER

Risk: Councillors using personal email for council business

- Likelihood: Medium
- Impact: High
- Controls: Mandatory council email domain and training
- Residual risk: Low

Risk: Loss of HR data

- Likelihood: Low
- Impact: High
- Controls: Encrypted folder and restricted access
- Residual risk: Low

Risk: Supplier bank details exposed

- Likelihood: Low
- Impact: High
- Controls: Multi-factor authentication and audit trail
- Residual risk: Low

Risk: Over-publication of personal data in minutes

- Likelihood: Medium
- Impact: Medium
- Controls: Redaction & GDPR policy, and clerk/council review of practices
- Residual risk: Low

Risk: Data breach not reported in time

- Likelihood: Low
- Impact: High
- Controls: Breach procedure, policies and training
- Residual risk: Low

Risk: Cloud storage misconfigured

- Likelihood: Low
- Impact: High
- Controls: Permissions review
- Residual risk: Low

Further information is contained in the following policies which are reviewed at least annually:

GDPR & Information Management
Document Retention
Information Security
IT Policy
Publication Scheme
Privacy Notices
Accessibility Statement