MICROSOFT 365
ADMINISTRATION, BACKUP & DATA PROCESSING POLICY

Controller-to-Processor Access, Backup & Administration Arrangements

---

Sible Hedingham Parish Council

and

Solve My Problem Ltd

Document Reference	SMP-SHPC-DPP-2026
Related Reference	SMP-SHPC-M365-2026 (Managed Service Agreement) SMP-SHPC-DPA-2026 (Data Processing Agreement)
Version	1.1
Date	01/05/2026
Review Date	01/05/2027
Classification	OFFICIAL
Prepared By	Solve My Problem Ltd
Approved By	Council Meeting

Contents

Contents 2
1. Introduction 4
2. Purpose and Scope 4
2.1 Purpose 4
2.2 Scope 5
3. Lawful Basis for Processing 5
3.1 Special Category Data 6
4. Roles and Responsibilities 6
4.1 Data Controller 6
4.2 Data Processor 6
4.3 Named Contacts 6
4.4 Council Responsibilities 7
4.5 Provider Responsibilities 7
5. Data Access and Processing Activities 8
5.1 M365 Global Administration 8
5.2 Privileged Access Controls 8
5.3 Backup Administration 8
5.4 FOI and GDPR Request Support 9
5.5 Backup Deletion Limitations 9
5.6 Incidental Access to Personal Data 9
6. Security Measures 9
6.1 Technical Measures – M365 Tenancy 10
6.2 Technical Measures – Backup Infrastructure 10
6.3 Technical Measures – Provider Systems 10
6.4 Organisational Measures 10
7. Data Storage and Retention 11
7.1 Location of Data 11
7.2 Retention 11
8. Data Subject Rights 12
9. Data Breach Management 12
10. Third-Party Service Providers and Sub-Processors 13
11. International Data Transfers 13
12. Data Protection Impact Assessment 14
13. Training and Awareness 14
14. Policy Review 14
15. Agreement and Signatures 15
Appendix A: Glossary of Terms 16

1. Introduction

This policy sets out the terms under which personal data and other information held within the Microsoft 365 (M365) environment of Sible Hedingham Parish Council (the "Council") may be accessed, processed, and stored by Solve My Problem Ltd (the "Provider") in the course of delivering M365 administration and backup services under the managed service agreement referenced SMP-SHPC-M365-2026.

This is a controller-to-processor arrangement: the Council acts as Data Controller and the Provider acts as Data Processor. This policy should be read alongside the Council's Data Security Policy, IT Policy, published privacy notices, and the Data Processing Agreement (SMP-SHPC-DPA-2026) between the Council and the Provider.

The Council is a public authority listed under Schedule 1, Part II, Paragraph 7(a) of the Freedom of Information Act 2000 and is subject to the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018, and the ICO's Section 46 Code of Practice on records management.

2. Purpose and Scope

2.1 Purpose

The purpose of this policy is to:

- Define the categories of data that the Provider may access in the course of service delivery
- Establish the lawful basis under which the Council processes personal data within its M365 environment
- Set out the obligations of both parties regarding the protection of personal data
- Ensure transparency for data subjects whose information may be processed
- Support the Council's compliance with its obligations under FOIA, UK GDPR, and the ICO Section 46 Code of Practice

2.2 Scope

This policy covers all data held within the Council's M365 tenancy and associated backup infrastructure. The Council's M365 environment currently comprises 14 user accounts (1 Clerk and 13 Councillors) using .gov.uk email addresses under the siblehedingham-pc.gov.uk domain. The data in scope includes:

- Exchange Online mailboxes (email content, calendars, contacts) for all accounts
- OneDrive for Business files and folders
- Microsoft Teams messages, channels, and associated files (if Option A licensing is selected)
- Shared mailboxes (e.g. clerk@, enquiries@siblehedingham-pc.gov.uk)
- Microsoft 365 audit logs, sign-in logs, and message trace data
- User account and directory information (Microsoft Entra ID)
- Cloud-to-cloud backup copies of all of the above, held in the Provider's backup infrastructure

3. Lawful Basis for Processing

The Council's use of Microsoft 365 administration and backup services is necessary to support its statutory functions, governance, record keeping, information security, and its ability to respond to FOIA and UK GDPR requests. The Council relies primarily on the following lawful bases for the processing of personal data within its M365 environment:

Lawful Basis	Application
Article 6(1)(e) – Public Task	Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the Council as a parish council. This is the Council's primary lawful basis for routine processing of personal data within its M365 environment.
Article 6(1)(c) – Legal Obligation	Processing is necessary for compliance with legal obligations including the Freedom of Information Act 2000, the UK GDPR, the Data Protection Act 2018, the ICO Section 46 Code of Practice, and the Council's records retention, audit, and statutory governance obligations.

The Provider acts as a processor and processes personal data only on the documented instructions of the Council, as set out in this policy and the Data Processing Agreement. The Provider does not determine the purposes or means of processing on its own account.

3.1 Special Category Data

Special category data may be encountered incidentally within Council correspondence, attachments, files, or records. The Provider shall not intentionally search for or process special category data except where necessary to provide the agreed services or where instructed by the Council.

The Council remains responsible for identifying and documenting any applicable Article 9 condition, Schedule 1 condition, and Appropriate Policy Document required under the Data Protection Act 2018 in relation to the Council's own processing activities.

4. Roles and Responsibilities

4.1 Data Controller

Sible Hedingham Parish Council is the Data Controller for all personal data held within its M365 environment. The Council determines the purposes and means of processing and retains ultimate responsibility for the data. The Clerk acts as the Council's primary point of contact for data protection matters.

4.2 Data Processor

Solve My Problem Ltd acts as a Data Processor when accessing or handling the Council's data in the course of delivering the agreed managed services. The Provider shall only process data on the documented instructions of the Council.

4.3 Named Contacts

The following contacts are nominated for the practical operation of this policy, including 24-hour breach notification:

Role	Contact
Council data protection contact	Clerk to the Council clerk@siblehedingham-pc.gov.uk 01787 462568
Provider data protection / security contact	Darren Casey, Solve My Problem Ltd admin@solvemyproblem.co.uk 01376 386724
Emergency / out-of-hours breach contact	Held by the Clerk and available to authorised Council officers

4.4 Council Responsibilities

- Maintain an up-to-date Record of Processing Activities (ROPA) that reflects data processing by the Provider
- Ensure that privacy notices published by the Council inform data subjects that an external managed service provider administers the M365 environment and backup infrastructure
- Identify and document any Article 9 condition, Schedule 1 condition, and Appropriate Policy Document required for the Council's own processing
- Review and approve the Provider's access levels on at least an annual basis
- Report any suspected data breaches to the Provider without undue delay
- Ensure councillors are aware that the Provider has administrative access to the M365 environment as described in this policy

4.5 Provider Responsibilities

- Process data only in accordance with the Council's documented instructions
- Maintain appropriate technical and organisational security measures (see Section 6)
- Not engage any sub-processor without prior written consent of the Council
- Assist the Council in responding to data subject access requests (DSARs) and erasure requests under Articles 15 and 17 of the UK GDPR
- Assist the Council in searching and retrieving emails from backup archives for Freedom of Information requests
- Notify the Council without undue delay (and in any event within 24 hours) upon becoming aware of a personal data breach
- Ensure that all personnel with access to Council data are subject to confidentiality obligations and have received appropriate data protection training
- On termination of the agreement, return or securely delete all Council data as directed by the Council

5. Data Access and Processing Activities

5.1 M365 Global Administration

The Provider holds Global Administrator access to the Council's M365 tenancy. This level of access is necessary to deliver the managed service and includes the ability to:

- Create and remove user accounts when councillors join or leave the Council
- Manage licences, passwords, and multi-factor authentication for all 14 accounts
- Configure and maintain Exchange Online, OneDrive, SharePoint, and Teams
- Configure and maintain security settings including MFA enforcement, audit logging, legacy authentication blocking, anti-malware and anti-phishing protection, external forwarding rules, and external sharing settings
- Monitor service health and review audit logs, sign-in logs, and message trace
- Respond to security incidents and perform troubleshooting
- Apply configuration changes in line with the UK Government Secure Configuration Blueprint for Microsoft 365 and NCSC Cyber Essentials guidance

5.2 Privileged Access Controls

Privileged administrator access shall be restricted to named Provider personnel and protected by multi-factor authentication. Where technically available, privileged access shall be reviewed periodically and removed when no longer required. Administrative actions may be reviewed through Microsoft 365 audit logs where necessary, and the Council retains the right to request a list of personnel with administrative access at any time.

5.3 Backup Administration

The Provider operates and manages an independent cloud-to-cloud backup service covering all 14 user accounts. This backup is separate from Microsoft's native retention features and provides:

- Automatic backup of email, OneDrive files, and calendar data three times per day
- Long-term retention (configurable, minimum 1 year)
- Searchable backup archives enabling retrieval of individual emails, files, or calendar items
- UK-based data storage for backup data, in line with the backup vendor's service terms

As part of routine backup verification, the Provider periodically checks backup integrity. This may involve viewing email subjects, file names, folder structures, or limited content to confirm that backups are running correctly and that data can be restored. This verification is essential to ensure the Council can meet its obligations under UK GDPR Article 32 regarding the ability to restore availability and access to personal data in the event of a physical or technical incident.

Restore operations are performed at the Council's request (for example, for FOI responses, GDPR requests, or recovery from accidental deletion) or as part of agreed verification procedures.

5.4 FOI and GDPR Request Support

As part of the managed service, the Provider will search and retrieve emails from backup archives in response to:

- Freedom of Information requests received by the Council
- Data subject access requests under Article 15 of the UK GDPR
- Erasure requests under Article 17 of the UK GDPR, including confirmation of deletion from backup where technically feasible

Support for FOI, DSAR and erasure requests will be provided in accordance with the managed service agreement. Where requests exceed the included support allowance, additional charges may apply as set out in that agreement.

5.5 Backup Deletion Limitations

Where immediate deletion from immutable or point-in-time backup sets is not technically possible, the Provider shall ensure the data is not restored into live systems except where legally required or expressly instructed by the Council, and that it expires in accordance with the applicable backup retention period. The Provider shall confirm to the Council in writing that this limitation has been applied where relevant to an erasure request.

5.6 Incidental Access to Personal Data

In the course of the above activities, the Provider may encounter personal data including but not limited to names, email addresses, correspondence content, attachments, and council business records. The Provider shall:

- Treat all such data as confidential
- Access data only to the extent necessary to perform the agreed services
- Not copy, extract, or disclose data for any purpose outside the scope of this agreement
- Immediately notify the Council if content is encountered that suggests safeguarding concerns or criminal activity, in line with applicable legal obligations

6. Security Measures

The Provider shall maintain the following technical and organisational measures, aligned with the UK Government Secure Configuration Blueprint for Microsoft 365 ("Good" tier), NCSC Cyber Essentials requirements, and the Council's Data Security Policy and IT Policy.

6.1 Technical Measures – M365 Tenancy

- Multi-factor authentication (MFA) enforced on all accounts via security defaults
- Legacy authentication protocols blocked
- Audit logging enabled for all mailboxes
- Anti-malware and anti-phishing protection configured (Exchange Online Protection)
- External email forwarding rules blocked
- Secure external sharing settings for OneDrive and SharePoint
- TLS 1.2 encryption for email in transit
- DMARC, DKIM, and SPF configured for the siblehedingham-pc.gov.uk domain

6.2 Technical Measures – Backup Infrastructure

- Encryption of backup data in transit (TLS 1.2 or above) and at rest (AES-256 or equivalent)
- Backup data stored separately from the M365 production environment
- Access to backup infrastructure restricted to authorised Provider personnel only
- Immutability features applied where available to protect against ransomware and accidental deletion

6.3 Technical Measures – Provider Systems

- Multi-factor authentication on all Provider accounts used to access Council data
- Endpoint protection and device management on all systems used to access the Council's M365 tenancy
- Regular vulnerability scanning and patching

6.4 Organisational Measures

- Confidentiality obligations and data protection training for all Provider staff with access to Council data
- Access restricted to named, authorised personnel only
- Documented processes for granting, reviewing, and revoking access
- Incident response and breach notification procedures

7. Data Storage and Retention

7.1 Location of Data

The Council requires UK data residency for Council customer data at rest where available under the relevant Microsoft 365 and backup service terms. The Provider shall not intentionally configure backup storage outside the United Kingdom without the Council's prior written consent.

Microsoft 365 production data is hosted by Microsoft within Microsoft's global cloud infrastructure. Microsoft provides workload-specific data residency commitments for UK tenancies; the precise scope of UK data residency depends on the service, product terms, and any associated metadata, support, or diagnostic processing carried out by Microsoft.

Cloud-to-cloud backup data held by the Provider is stored in UK-based data centres operated by the backup service provider, in line with that vendor's service terms.

Any international transfer of personal data shall be subject to appropriate safeguards under Chapter V of the UK GDPR.

7.2 Retention

Backup data shall be retained in accordance with the Council's adopted records retention schedule. The default backup retention periods are:

Data Type	Backup Retention Period
Exchange Online (email, calendar, contacts)	12 months
OneDrive for Business files	12 months
Microsoft Teams (if applicable)	12 months
Shared mailboxes	12 months

These periods shall be reviewed against the Council's adopted retention schedule and the ICO Section 46 Code of Practice. The Provider will adjust backup retention settings as instructed by the Council.

Upon termination of the managed service agreement, backup data shall be securely deleted using methods that render the data unrecoverable, and the Provider shall confirm deletion in writing within 30 days of the effective termination date, subject to the limitations in Section 5.5.

8. Data Subject Rights

Data subjects retain all rights afforded to them under Chapter III of the UK GDPR, including the rights of access (Article 15), rectification (Article 16), erasure (Article 17), restriction (Article 18), portability (Article 20), and objection (Article 21).

Where the Council receives a data subject rights request that requires action within the Provider's systems, the Provider shall:

- Respond to the Council's instruction within 5 working days
- Search backup archives and provide results as required
- Delete specific emails or data from backup archives where erasure is required and technically feasible
- Maintain audit trails of any data searched, accessed, restored, or deleted as part of such requests

9. Data Breach Management

In the event of a personal data breach (as defined by Article 4(12) UK GDPR):

- The Provider shall notify the Council (via the Clerk) within 24 hours of becoming aware of the breach, using the contact details in Section 4.3
- The notification shall include: the nature of the breach, categories and approximate number of data subjects affected, likely consequences, and measures taken or proposed to mitigate the breach
- The Council, as Data Controller, shall determine whether notification to the Information Commissioner's Office (ICO) is required under Article 33 (within 72 hours of awareness) and whether affected data subjects must be informed under Article 34
- The Provider shall cooperate fully with the Council's investigation and provide all information and access reasonably required
- Both parties shall maintain a written record of all personal data breaches, including the facts, effects, and remedial action taken

10. Third-Party Service Providers and Sub-Processors

The Provider shall not engage any sub-processor to process Council data without the prior written authorisation of the Council. The following third-party service providers are relevant to the Services at the date of this policy:

Provider	Role	Data Location
Microsoft Corporation	Provides the Microsoft 365 platform used by the Council. Depending on the licensing and contractual route, Microsoft may act as a processor directly to the Council and/or as a sub-processor in relation to services procured through the Provider.	Microsoft global cloud, with UK data residency commitments where applicable under Microsoft's service terms
Afi.ai	Cloud-to-cloud backup software and storage for all M365 data, operated by the Provider as a sub-processor.	UK data centres

The parties shall maintain an up-to-date list of relevant third-party service providers and sub-processors. The Provider shall ensure that any sub-processor it engages is bound by data protection obligations no less onerous than those set out in this policy and the Data Processing Agreement, and shall inform the Council of any intended changes to sub-processors and give the Council the opportunity to object.

11. International Data Transfers

The Council requires UK data residency for Council customer data at rest where available under the relevant service terms. The Provider shall not intentionally configure storage of Council data outside the United Kingdom without the Council's prior written consent.

Where international transfers occur as part of the underlying platform services (for example, Microsoft's global support, telemetry, or diagnostic processing), the Provider shall ensure that the relevant transfer mechanism under Chapter V of the UK GDPR is in place under the platform provider's service terms.

Should a transfer of Council data outside the UK become necessary for any other reason, the Provider shall not proceed without the prior written consent of the Council and shall ensure an appropriate transfer mechanism is in place, such as the UK International Data Transfer Agreement (IDTA).

12. Data Protection Impact Assessment

The Council has conducted a DPIA screening assessment for this arrangement. Given the nature and volume of data processed by a parish council of 14 users, the Council has concluded that a full DPIA is not required at this time because:

- The processing does not involve large-scale systematic monitoring of publicly accessible areas
- The processing does not involve automated decision-making with legal or significant effects
- The volume of personal data processed is proportionate to the size and function of the Council
- Appropriate safeguards are in place as described in this policy

If the nature of processing changes significantly, the Council shall review whether a full DPIA is required.

13. Training and Awareness

- The Provider shall ensure all staff who may access Council data receive appropriate data protection training upon appointment and at least annually thereafter
- The Council shall ensure that councillors and the Clerk are aware that the Provider administers the M365 environment and has the access described in this policy
- The Council shall include reference to this arrangement in its published privacy notices
- This policy shall be published on the Council's website

14. Policy Review

This policy shall be reviewed at least annually, or sooner if:

- There is a change in applicable legislation or ICO guidance
- There is a significant change to the managed services provided (for example, a licensing tier change)
- A data breach or near-miss occurs that highlights a policy gap
- The Council or Provider undergoes organisational change
- Local government reorganisation or changes to the Council's statutory, governance, IT, or records management arrangements affect the services covered by this policy

Amendments require the agreement of both parties and approval by Full Council.

15. Agreement and Signatures

By signing below, both parties confirm that they have read, understood, and agree to comply with this policy.

On behalf of Sible Hedingham Parish Council:

Name:	
Role:	
Signature:	
Date:	

On behalf of Solve My Problem Ltd:

Name:	
Role:	
Signature:	
Date:	

Appendix A: Glossary of Terms

Term	Definition
Appropriate Policy Document	A document required under the Data Protection Act 2018 when relying on certain Schedule 1 conditions for processing special category data, explaining the procedures for compliance and retention.
Data Controller	The entity that determines the purposes and means of processing personal data (Sible Hedingham Parish Council).
Data Processor	The entity that processes personal data on behalf of the Controller (Solve My Problem Ltd).
DPA	Data Processing Agreement – a contract required under Article 28 UK GDPR between Controller and Processor.
DPIA	Data Protection Impact Assessment – a risk assessment under Article 35 UK GDPR for high-risk processing.
DSAR	Data Subject Access Request – a request from an individual under Article 15 UK GDPR.
FOIA	Freedom of Information Act 2000 – under which the Council is a listed public authority.
ICO	Information Commissioner's Office – the UK's independent data protection authority.
M365	Microsoft 365 – the cloud productivity suite including Exchange Online, OneDrive, SharePoint, and Teams.
MFA	Multi-Factor Authentication – requiring two or more verification factors to access a system.
ROPA	Record of Processing Activities – the register required under Article 30 UK GDPR.
UK GDPR	The UK General Data Protection Regulation, as incorporated into UK law by the Data Protection Act 2018 and the European Union (Withdrawal) Act 2018.