DATA PROCESSING AGREEMENT

Under Article 28 of the UK General Data Protection Regulation

---

Between

Sible Hedingham Parish Council

(Data Controller)

and

Solve My Problem Ltd

(Data Processor)

Document Reference	SMP-SHPC-DPA-2026
Related References	SMP-SHPC-M365-2026 (Managed Service Agreement) SMP-SHPC-DPP-2026 (M365 Administration, Backup & Data Processing Policy)
Version	1.1
Date	01/05/2026
Classification	OFFICIAL

1. Parties and Definitions

1.1 Parties

This Data Processing Agreement ("DPA") is entered into between **Sible Hedingham Parish Council** of Sible Hedingham Parish Council Office, 75 Swan Street, Sible Hedingham, Essex CO9 3HT (the "Controller") and **Solve My Problem Ltd** of Colleygate, Dunmow Road, Rayne, CM77 6RZ (the "Processor").

This DPA is supplemental to and forms part of the managed service agreement between the parties referenced SMP-SHPC-M365-2026 (the "Principal Agreement").

1.2 Definitions

In this DPA, unless the context otherwise requires:

- "Data Protection Legislation" means the UK GDPR (Regulation (EU) 2016/679 as it forms part of retained EU law), the Data Protection Act 2018, and any subordinate legislation made under them, as amended from time to time.
- "Personal Data", "Data Subject", "Processing", "Personal Data Breach", and "Supervisory Authority" have the meanings given to them in the UK GDPR.
- "Services" means the Microsoft 365 administration, backup, migration, and ongoing managed services provided by the Processor under the Principal Agreement.

2. Scope and Purpose of Processing

2.1 Subject Matter and Duration

The Processor shall process Personal Data on behalf of the Controller for the duration of the Principal Agreement and for such further period as is necessary to return or delete all Personal Data in accordance with this DPA.

2.2 Nature and Purpose of Processing

The Processor processes Personal Data for the purpose of providing the Services, which include:

- Microsoft 365 tenant administration (account creation, licence management, security configuration, troubleshooting)
- Cloud-to-cloud backup of M365 data, including email, OneDrive, calendar, and Teams where licensed/applicable, three times daily
- Backup verification, including review of email subjects, file names, or limited content to confirm backup integrity
- Searching and retrieving data from backup archives for FOI requests, DSAR responses, and erasure requests
- Email migration from the previous provider (Cloud Next) during Year 1
- Security configuration and ongoing maintenance in line with the UK Government Secure Configuration Blueprint and NCSC Cyber Essentials
- Password resets, MFA support, and general account management

2.3 Types of Personal Data

The Personal Data processed includes:

- Names, email addresses, and contact details of councillors, the Clerk, and their correspondents
- Email content and attachments (which may include correspondence with members of the public)
- Calendar entries and meeting invitations
- Files stored in OneDrive for Business
- Teams messages and files (if applicable)
- Account credentials and authentication data (managed within Microsoft Entra ID)
- Audit logs and sign-in records

2.4 Categories of Data Subjects

Data subjects include:

- Councillors and the Clerk of Sible Hedingham Parish Council
- Members of the public who correspond with the Council by email
- Third parties (suppliers, other organisations, agencies) who correspond with the Council
- Any individual whose personal data appears in documents, files, or correspondence held in the M365 environment

3. Obligations of the Processor

The Processor shall:

3.1 Documented Instructions

Process Personal Data only on the documented instructions of the Controller, as set out in this DPA and the M365 Administration, Backup & Data Processing Policy (SMP-SHPC-DPP-2026), unless required to do so by law. If the Processor is required by law to process Personal Data otherwise than on the Controller's instructions, the Processor shall inform the Controller of this legal requirement before processing (unless the law prohibits such notification on important grounds of public interest).

3.2 Confidentiality

Ensure that all personnel authorised to process Personal Data have committed to confidentiality obligations or are under an appropriate statutory obligation of confidentiality.

3.3 Security

Implement and maintain appropriate technical and organisational measures to ensure a level of security appropriate to the risk, as detailed in Section 6 of the M365 Administration, Backup & Data Processing Policy. These measures include as a minimum:

- Multi-factor authentication on all accounts used to access Council data
- Encryption of data in transit (TLS 1.2+) and at rest (AES-256 or equivalent)
- Access restricted to named, authorised personnel on a need-to-know basis
- Endpoint protection on all devices used to access the Council's M365 tenancy
- Regular review and patching of systems

3.4 Sub-Processing

Not engage another processor (sub-processor) without the prior specific written authorisation of the Controller. Where authorised, the Processor shall impose the same data protection obligations as set out in this DPA on the sub-processor by way of a contract. The Processor remains fully liable to the Controller for the performance of the sub-processor's obligations.

The currently authorised third-party service providers and sub-processors are listed in Section 10 of the M365 Administration, Backup & Data Processing Policy. The Processor shall inform the Controller of any intended changes and give the Controller the opportunity to object.

3.5 Data Subject Rights

Assist the Controller, taking into account the nature of the processing, in fulfilling the Controller's obligations to respond to Data Subject requests exercising their rights under Chapter III of the UK GDPR. This includes searching backup archives, providing copies of data, and deleting data from backups where technically feasible and instructed by the Controller.

3.6 Security and Breach Assistance

Assist the Controller in ensuring compliance with the Controller's obligations under Articles 32 to 36 of the UK GDPR (security of processing, notification of breaches to the supervisory authority and data subjects, and data protection impact assessments), considering the nature of processing and the information available to the Processor.

3.7 Breach Notification

Notify the Controller without undue delay, and in any event within 24 hours, after becoming aware of a Personal Data Breach. The notification shall include:

- A description of the nature of the breach, including where possible the categories and approximate number of Data Subjects and Personal Data records affected
- The name and contact details of the Processor's point of contact
- A description of the likely consequences of the breach
- A description of the measures taken or proposed to address the breach, including measures to mitigate possible adverse effects

3.8 Deletion or Return of Data

At the choice of the Controller, delete or return all Personal Data to the Controller after the end of the provision of Services, and delete existing copies unless UK law requires storage of the Personal Data. The Processor shall confirm deletion in writing within 30 days of the effective termination date. Where immediate deletion from immutable or point-in-time backup sets is not technically possible, the Processor shall ensure the data is not restored into live systems except where legally required or expressly instructed by the Controller, and that it expires in accordance with the applicable backup retention period.

3.9 Audits and Inspections

Make available to the Controller all information necessary to demonstrate compliance with the obligations laid down in Article 28 of the UK GDPR, and allow for and contribute to audits, including inspections, conducted by the Controller or an auditor mandated by the Controller. The Processor shall immediately inform the Controller if, in the Processor's opinion, an instruction from the Controller infringes the Data Protection Legislation.

4. International Transfers

The Processor shall not intentionally configure storage of Council Personal Data outside the United Kingdom without the prior written consent of the Controller. Backup data shall be stored in UK data centres in line with the backup vendor's service terms.

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

If any other transfer becomes necessary, the Processor shall ensure that one of the transfer mechanisms set out in Chapter V of the UK GDPR is in place before any transfer occurs and shall provide evidence of this to the Controller.

5. Obligations of the Controller

The Controller shall:

- Ensure it has a lawful basis for processing Personal Data and for instructing the Processor to process on its behalf
- Provide documented instructions to the Processor regarding the processing of Personal Data
- Ensure that relevant privacy notices inform Data Subjects of this processing arrangement
- Identify and document any 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
- Notify the Processor without undue delay of any data subject rights request or complaint that may require action by the Processor
- Comply with its obligations under the Data Protection Legislation, including maintaining a Record of Processing Activities

6. Liability

Each party shall be liable for its own acts and omissions in relation to the Data Protection Legislation. Nothing in this DPA limits or excludes either party's liability for breaches of the Data Protection Legislation that are attributable to that party's own acts or omissions.

The Processor's total aggregate liability arising under or in connection with this DPA shall be subject to any limitations of liability set out in the Principal Agreement.

7. Term and Termination

This DPA shall commence on the date of signature and shall continue for the duration of the Principal Agreement. Upon termination of the Principal Agreement, the provisions of this DPA that relate to the return or deletion of Personal Data (Clause 3.8) and audit rights (Clause 3.9) shall continue to apply until all Personal Data has been returned or deleted as confirmed in writing.

Either party may terminate this DPA immediately by written notice if the other party commits a material breach of this DPA which is not remedied within 30 days of written notice specifying the breach.

8. General Provisions

8.1 Governing Law

This DPA shall be governed by and construed in accordance with the laws of England and Wales. The courts of England and Wales shall have exclusive jurisdiction to settle any dispute arising out of or in connection with this DPA.

8.2 Precedence

In the event of any conflict between this DPA and the Principal Agreement, this DPA shall prevail to the extent of the conflict insofar as it relates to the processing of Personal Data.

8.3 Amendments

No amendment to this DPA shall be effective unless it is in writing and signed by both parties.

8.4 Entire Agreement

This DPA, together with the Principal Agreement and the M365 Administration, Backup & Data Processing Policy, constitutes the entire agreement between the parties in relation to the processing of Personal Data.

9. Signatures

Signed by the duly authorised representatives of the parties:

On behalf of Sible Hedingham Parish Council (Controller):

Name:	
Role:	
Signature:	
Date:	

On behalf of Solve My Problem Ltd (Processor):

Name:	
Role:	
Signature:	
Date:	

Annex 1: Details of Processing

Item	Detail
Controller	Sible Hedingham Parish Council
Processor	Solve My Problem Ltd
Subject Matter	Microsoft 365 administration, cloud-to-cloud backup, email migration, and ongoing managed services for the Council's M365 tenancy.
Duration	For the term of the managed service agreement (SMP-SHPC-M365-2026), initial term 12 months, then rolling monthly with 30 days' notice.
Nature of Processing	Storage, backup, retrieval, search, deletion, administrative access, security configuration, and email migration.
Purpose of Processing	To provide managed M365 services enabling the Council to meet its obligations under FOIA, UK GDPR, and the ICO Section 46 Code of Practice.
Types of Personal Data	Names, email addresses, contact details, email content and attachments, calendar entries, OneDrive files, Teams messages (if applicable), account credentials, audit logs.
Categories of Data Subjects	Councillors and Clerk, members of the public, third-party correspondents (suppliers, agencies, organisations).
Authorised Sub-Processors	Afi.ai (cloud-to-cloud backup, UK data centres). Microsoft Corporation provides the underlying M365 platform and may act as a processor directly to the Council and/or as a sub-processor depending on the licensing route.