Local Government for Langton Green, Speldhurst, Ashurst and Old Groombridge

WhatsApp Data Protection and Artificial Intelligence (AI) Usage Policies

1. Purpose

This policy sets out how Speldhurst Parish Council manages personal data when using WhatsApp for council business, ensuring compliance with the UK GDPR and Data Protection Act 2018.

2. Scope

This policy applies to all Councillors, officers, and staff who use WhatsApp for council-related communications.

3. Principles

- **Lawfulness, Fairness, and Transparency:** Personal data shared or discussed on WhatsApp must be processed lawfully, fairly, and transparently.
- **Purpose Limitation:** WhatsApp must only be used for legitimate council business.
- **Data Minimisation:** Only necessary personal data should be shared.
- **Accuracy:** Ensure information shared is accurate and up to date.
- **Storage Limitation:** Personal data must not be retained on WhatsApp longer than necessary.
- **Integrity and Confidentiality:** Appropriate security measures must be in place to protect data.

4. Use of WhatsApp

- WhatsApp may be used for informal, time-sensitive communications only.
- Formal council business, decisions, and records must be conducted and stored via official council channels (e.g., .gov.uk email, council systems).
- No sensitive or special category data (e.g., health, race, religion) should be shared via WhatsApp.
- Group membership must be controlled and reviewed regularly.

- Any message sent or received via WhatsApp that relates to council business is official information and may be subject to disclosure under FOIA, regardless of whether it was sent from a personal or council-owned device.

4. Business Information must be preserved

- Where a WhatsApp message includes information that:
  relates to council decisions,
  provides advice, instruction, or direction, or
  forms part of a discussion leading to an action,
- the user must **transfer the relevant content** (e.g., screenshot, text copy, file) to an approved council record-keeping system such as email, a document repository, or council minutes.

Routine Deletion

- Routine deletion of messages is permitted only when:
  the messages are transitory or purely administrative (e.g., confirming attendance),
  any business-critical information has been captured elsewhere, and
  there is no ongoing FOI request involving the content.

5. FOI Requests and legal obligations

FOI Holds

- Upon receipt of an FOI request:
  All potentially relevant WhatsApp messages must be preserved immediately.
  Users must not delete, edit, or otherwise remove any information that may fall within the scope of the request.

Legal Warning

- Deleting information after an FOI request has been received may constitute a criminal offence under Section 77 of the Freedom of Information Act 2000.

Duty to Assist

- All councillors and staff must cooperate fully in supplying any WhatsApp messages relevant to an FOI request, internal review, audit, or legal requirement.

6. Data Security

- Devices used for WhatsApp must be secured with passwords or biometrics.
- WhatsApp must be kept updated to the latest version.
- Chats containing personal data must be deleted when no longer needed.
- If a device is lost or stolen, the Clerk must be informed immediately.

7. Data Subject Rights

• Individuals have the right to access, rectify, or request deletion of their personal data.

• Any data subject request received via WhatsApp must be referred to the Clerk or Data Protection Officer.

8. Breach Management

Any suspected data breach involving WhatsApp must be reported to the Clerk immediately. The council will record, investigate, and, if necessary, report breaches in line with its Data Breach Policy.

9. Training and Awareness

All users must receive training on this policy and data protection principles.

10. Review

This policy will be reviewed annually or when there are significant changes to legislation or council practice.

Artificial Intelligence (AI) Usage Policy

1. Purpose

This policy sets out how Artificial Intelligence (AI) tools may be used by Speldhurst Parish Council in a safe, lawful, and responsible manner. The aim is to allow staff and councillors to benefit from AI where appropriate, while ensuring that personal data, protected information, and Parish Council data are handled in line with existing data protection and governance policies.

AI is not treated as a special or exceptional category of technology; rather, it is subject to the same standards of data protection, confidentiality, and accountability that already apply to all information handling within the Parish Council.

2. Scope

This policy applies to:

- All Parish Council staff, councillors, contractors, and volunteers
- Any use of AI tools in connection with Parish Council business, whether on Council-owned or personal devices

3. Key Principles

The following principles underpin all use of AI within the Parish Council:

- **Data protection first**: Personal data, sensitive data, or protected information must never be shared with AI systems unless they are specifically designed to protect such information and have been formally approved by the Finance & Governance Committee.
- **Minimum risk approach**: Until clearer external compliance and regulatory guidance is available, the Parish Council will take a cautious and conservative approach to AI adoption.
- **Consistency with existing policies**: AI use must comply with existing policies, including (but not limited to) data protection, information security, confidentiality, and acceptable use policies.
- **Human accountability**: AI tools may assist with tasks, but responsibility for decisions, outputs, and actions always rests with the human user.

4. Approved and Safe Use of AI

4.1 Approved Systems

At present, the only AI systems approved for use with Parish Council information are:

- **Microsoft 365 AI features**, as provided under the Parish Council's paid Microsoft 365 subscription. These tools do not use Council data to train public AI models.

In the future, other systems (for example, GovAssist) may be approved for handling Parish Council data, but only following formal assessment and approval by the Finance & Governance Committee.

4.2 Use of Public AI Tools

Public or third-party AI tools (such as ChatGPT or similar services) may only be used under the following strict conditions:

- No personal data, sensitive data, or protected information is shared
- No information is provided that could identify the Parish Council, its staff, councillors, residents, suppliers, or partners
- Queries must be framed in **broad, generic terms only**, with no identifiable link back to Parish Council business

This allows limited and flexible use of public AI tools for general research, drafting assistance, or problem-solving, while ensuring that Parish Council data is not exposed.

5. Prohibited Use

The following uses of AI are strictly prohibited:

- Entering personal data, special category data, or confidential Parish Council information into any AI system that has not been approved by Finance & Governance
- Using AI tools to make automated decisions about individuals
- Relying on AI outputs without appropriate human review and judgement
- Circumventing existing data handling or approval processes by using AI

6. Data Protection and Confidentiality

All use of AI must comply with:

- UK GDPR and Data Protection Act requirements
- Parish Council data protection and information security policies

Users must assume that information entered into unapproved AI tools could be stored, reused, or disclosed beyond the Parish Council's control.

7. Training and Awareness

Staff and councillors are expected to:

- Familiarise themselves with this policy before using AI tools for Parish Council business
- Seek guidance from the Clerk or Finance & Governance Committee if unsure whether a particular use is permitted

8. Review and Updates

This policy will be reviewed periodically, particularly as national guidance, regulatory expectations, and approved AI tools evolve. Updates will be approved by the Parish Council or the Finance & Governance Committee as appropriate.