ALBURY PARISH COUNCIL

Serving Farley Green, Brook, Little London & Newlands Corner

Data Protection Policy

1. **Introduction**

   Albury Parish Council needs to gather and use certain information about individuals. These can include parishioners, suppliers, business contacts, employees and other people the organization has a relationship with or may need to contact.

   This policy describes how this personal data must be collected, handled and stored to meet the Parish Council's data protection standards – and to comply with the law.

2. **Why this policy exists**

   This data protection policy ensures that Albury Parish Council:

   - Complies with data protection law and follows good practice.
   - Protects the rights of staff, parishioners and partners.
   - Is open about how it stores and processes individuals' data.
   - Protects itself from the risks of a data breach.

3. **Data Protection Law**

   The Data Protection Act 2018 and UK GDPR describe how organisations must collect, handle and store personal information. These rules apply regardless of whether data is stored electronically, on paper or on other materials.

   To comply with the law, personal information must be collected and used fairly, stored safely and not disclosed unlawfully.

   The Data Protection Act is underpinned by eight important principles. These say that personal data must:

   - Be processed fairly and lawfully.
   - Be obtained only for specific, lawful purposes.
   - Be adequate, relevant and not excessive.
   - Be accurate and kept up to date.
   - Not be held for any longer than necessary.
   - Processed in accordance with the rights of data subjects.
   - Be protected in appropriate ways.
   - Not be transferred outside the European Economic Area (EEA) unless that country or territory also ensures an adequate level of protection.

   UK GDPR also outlines seven principles of data protection, which explain that the data controller must:

   - Ensure lawful, fair, and transparent processing.

- Specify clear, legitimate purposes.
- Collect only necessary data.
- Maintain accurate, up-to-date information.
- Limit data storage duration.
- Protect data integrity and confidentiality.
- Demonstrate accountability and compliance.

4. **Scope**

This policy applies to:

- Albury Parish Council.
- All staff, councillors and volunteers of Albury Parish Council.
- All contractors, suppliers and other people working on behalf of Albury Parish Council.

It applies to all data that the council and its bodies hold relating to identifiable individuals, even if that information technically falls outside of the Data Protection Act 1998 or UK GDPR. This can include:

- Names of individuals.
- Postal addresses.
- Email addresses.
- Telephone numbers.
- Any other information relating to individuals.

5. **Data Protection Risks**

This policy helps to protect Albury Parish Council from some very real data security risks, including:

- **Breaches of confidentiality:** for instance, information being given out inappropriately.
- **Failing to offer choice:** for instance, all individuals should be free to choose how the company uses data relating to them.
- **Reputational damage:** for instance, the company could suffer if hackers successfully gained access to sensitive data.

6. **Responsibilities**

Everyone who works with or for Albury Parish Council has some responsibility for ensuring data is collected, stored and handled appropriately.

- **Councillors** are ultimately responsible for ensuring that Albury Parish Council meets its legal obligations.
- **The Data Protection Officer** is responsible for:
  i. Keeping councillors updated about data protection responsibilities, risks, and issues.
  ii. Reviewing all data protection procedures and related policies, in line with an agreed schedule.
  iii. Arranging data protection training and advice for the people covered by this policy.
  iv. Handling data protection questions from anyone covered by this policy.
  v. Dealing with requests from individuals to see the data Albury Parish Council holds about them (also called subject access requests).

vi. Checking and approving any contracts or agreements with third parties that may handle the Parish Council's sensitive data.
vii. The Council is not required to appoint a statutory DPO but will elect one voluntarily at the Annual Meeting each year.

- **The Clerk** is responsible for:
  i. Ensuring all systems, services and equipment used for storing data meet acceptable security standards.
  ii. Performing regular checks and scans to ensure security hardware and software is functioning properly.
  iii. Evaluating any third-party services the Parish Council is considering using to store or process data. For instance, cloud computing services.

7. **General Guidelines**

- The only people able to access data covered by this policy should be those who need it for their work.
- Data should not be shared informally.
- Albury Parish Council will ensure that its employees have access to training to help them understand their responsibilities when handling data.
- Employees should keep all data secure, by taking sensible precautions and following the guidelines below.
- In particular, strong passwords should be used (minimum length of 12 characters, including uppercase letters, lowercase letters, numbers, and special characters) and they should never be shared.
- Personal data should not be disclosed to unauthorized people, either within the company or externally.
- Data should be regularly reviewed and updated if it is found to be out of date. If no longer required, it should be deleted and disposed of securely.

8. Data Storage

These rules describe how and where data should be safely stored.

9. **Paper Storage**

When data is stored on paper it should be kept in a secure place where unauthorised people cannot see it.

These guidelines also apply to data that is usually stored electronically but has been printed out for some reason.

- When not required, the paper or files should be kept in a locked drawer or filing cabinet.
- Employees should ensure paper and printouts are not left where unauthorized people could see them, eg: on a printer.
- Data printouts should be shredded and disposed of securely when no longer required.

10. Electronic Storage

When data is stored electronically it must be protected from unauthorised access, accidental deletion, and malicious hacking attempts:

- Data should be protected by strong passwords (as above) that are changed regularly and never shared.

- If data is stored on removable media these should be kept locked away securely when not being used.
- Data should only be stored on designated drives and servers and should only be uploaded to an approved cloud computing service.
- Servers containing personal data should be sited in a secure location.
- Data should be backed up frequently (daily backups recommended). These backups should be tested regularly (monthly testing recommended).
- All servers and computers containing data should be protected by approved security software and a firewall.

11. Data Use

- When working with personal data, employees should ensure that the screens of their computers are locked when left unattended.
- Personal data should not be shared informally. In particular, it should never be sent by email.
- Data must be encrypted before being transferred electronically (e.g. via secure transfer tools)
- Personal data should never be transferred outside the European Economic Area unless that country or territory also ensures an adequate level of protection under UK GDPR requirements.

12. Data Accuracy

The law requires Albury Parish Council to take reasonable steps to ensure data is kept accurate and up to date.

- Data will be kept in as few places as necessary.
- Every opportunity should be taken to ensure data is updated.
- Albury Parish Council will make it easy for data subjects to update the information it holds on them, e.g., via the Parish Council website.
- Data should be updated as inaccuracies are discovered.

13. Subject Access Requests

All individuals who are the subject of personal data held by Albury Parish Council are entitled to:

- Ask what information the council holds about them and why.
- Ask how to gain access to it.
- Be informed about how to keep it up to date.
- Be informed how the parish council is meeting its data protection obligations

A request from an individual for this information is a Subject Access Request.

Subject Access Requests should be made by email, addressed to the data controller.

The data controller will aim to provide the relevant data within one month.

The data controller will always verify the identity of anyone making a Subject Access Request before giving information, by one of the following methods:

1. **Email Requests for Disclosure:**

Step 1: Email Verification:

- **Match Email Address:** Verify that the request is coming from the same email address that is on the record.
- **Check Previous Correspondence:** Review previous email interactions to confirm the requester's identity.

Step 2: Additional Verification (if necessary):

- **Document Verification:** Request a copy of a government-issued ID (e.g. passport, driver's licence) or a recent utility bill that matches the address on record (if applicable).

Step 3: Confirmation

- **Email Confirmation:** Send a confirmation email to the requester's registered email address, acknowledging receipt of the DSAR and outlining the next steps.

2. Phone Requests for Disclosure:

Step 1: Initial Verification:

- **Call Verification:** Call the phone number on record and ask the requester to verify specific details (e.g., address).

Step 2: Additional Verification (if necessary):

- **Document Verification:** Request a copy of a government-issued ID (e.g. passport, driver's licence) or a recent utility bill that matches the address on record (if applicable).

Step 3: Confirmation

- **Phone Confirmation:** Confirm the details over the phone and inform the requester of the next steps. Follow up with an email or letter confirmation.

3. Written Requests for Disclosure:

Step 1: Email Verification:

- **Match Address:** Verify that the request is coming from the same postal address that is on record.
- **Check Previous Correspondence:** Review previous interactions to confirm the requester's identity.

Step 2: Additional Verification (if necessary):

- **Document Verification:** Request a copy of a government-issued ID (e.g. passport, driver's licence) or a recent utility bill that matches the address on record (if applicable).

Step 3: Confirmation

- **Letter Confirmation:** Send a confirmation letter to the requester's registered postal address, acknowledging receipt of the DSAR and outlining the next steps.

4. Other DSARs (Erasure and Recification).

Step 1: Initial Verification:

- **Verify Identity:** Use one of the above methods (email, phone, written) to verify the requester's identity.

Step 2: Additional Verification:

- **Document Verification:** Request a copy of a government-issued ID or a recent utility bill that matches that address on record (if applicable).

Step 3: Confirmation

- **Confirmation Communication:** Send a confirmation via email, phone, or letter to acknowledge receipt of the DSAR and outline the next steps.

14. Disclosing data for other reasons

- In certain circumstances, the Data Protection Act allows personal data to be disclosed to law enforcement agencies without the consent of the data subject.

- Under these circumstances, Albury Parish Council will disclose the requested data. The data controller will ensure the request is legitimate.

15. Data Retention Schedule

Annual Review and Erasure:

- **Review Cycle:** All data categories will be reviewed annually at the next meeting after the end of the financial year.
- **Erasure:** Data that is no longer required will be securely deleted or destroyed.

Categories of Data and Retention Period:

- **Name of Individuals:** Retained for 5 years.
- **Postal Addresses:** Retained for 5 years.
- **Email Addresses:** Retained for 5 years.
- **Telephone Numbers:** Retained for 5 years.
- **Other Information Relating to Individual:** Retained for 5 years.

Procedures for Secure Deletion and Destruction:

- **Electronic Data:** Use secure deletion software to permanently erase data.

- **Paper Data:** Shred documents and dispose of them securely.

16. **Data Protection Impact Assessments**

Annual Meeting of the Council:

- **Regular Assessment:** Conduct regular data protection impact assessments (DPIAs) at the Annual Meeting of the Council.

Evaluating New Processing Activity:

- **Procedure:** Evaluate any new data processing activities to ensure compliance with data protection laws.

Regular Review Cycle:

- **Review Cycle:** Establish a regular review cycle for all data processing activities.

17. **Data Processing Agreements**

Detailed Requirements:

- **Agreements:** Ensure all data processing agreements include detailed requirements for data protection.

Due Diligence Procedures:

- **Selecting Processors:** Conduct due diligence procedures when selecting data processors to ensure they meet data protection standards.

Monitoring and Audit Requirements:

- **Monitoring:** Regularly monitor data processors to ensure compliance.
- **Audits:** Conduct audits of data processors to verify their compliance with data protection agreements.

18. **Data Protection Training**

Mandatory Training

- **Training for All Staff and Councillors:** Establish mandatory data protection training for all staff and councillors.

Training Frequency:

- **Bi-Annual Refreshers:** Set a minimum training frequency of bi-annual refreshers.

Training Verification and Documentation:

- **Verification:** Verify that all staff and councillors have completed the training.
- **Documentation:** Maintain documentation of all training activities.

19. Providing Information

Albury parish Council aims to ensure that individuals are aware that their data is being processed and that they understand:

- How the data is being used.
- How to exercise their rights.

To these ends, Albury Parish Council has a privacy statement setting out how data relating to individuals is used by the authority.

This is available on request and is also available on the Parish Council's website:

www.alburyparishcouncil.gov.uk

20. Review

All policies of the Parish Council are reviewed annually, or sooner if required by changes in legislation or council operation.

21. Contact Information

For any questions or concerns regarding this policy or our co-option practices, please contact us using these details:

CJ Bishop-Wright

1 Mint Cottages

Park Road

Banstead

Surrey

SM7 3DS

clerk@alburyparishcouncil.gov.uk

07856 010 600