Arlingham Parish Council

Created: December 2021
Adopted: January 2022
Reviewed: February 2025
Next Review: February 2026

DATA PROTECTION POLICY

1. Purpose

Arlingham Parish Council (The Council) are committed to being transparent about how it collects and uses personal data in accordance with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 (DPA 2018), whilst also complying with the Freedom of Information Act 2000.

The Council is registered as a data controller with the Information Commissioner's Office (ICO).

The Council has appointed Arlingham Parish Council Clerk as the person with responsibility for data protection compliance within The Council. Questions about this policy, or requests for further information, should be directed to the Clerk.

2. Scope

This policy applies to anyone who has access to and/or is a user of The Council's ICT systems including staff, councillors, volunteers, visitors, contractors, and other community users.

This policy applies to all personal data, regardless of whether it is in paper or electronic format.

The Council will ensure that information is not kept for longer than is necessary and will retain the minimum amount of information that it requires to carry out its functions, adhering to any legal or statutory requirements.

The Council's Privacy Notice is available on our website at www.arlingham.co.uk.

3. Data Protection Responsibilities and Principles

The Council complies with the seven key data protection principles the UK GDPR sets out:

- Lawfulness, fairness and transparency;
- Purpose limitation;
- Data minimisation;
- Accuracy;
- Storage limitation;
- Integrity and confidentiality (security);
- Accountability.

All staff/councillors are responsible for:

- Familiarising themselves with and complying with this policy;
- Taking care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse at all times. All staff should adopt the approach that they should treat the personal data of others with the same care with which they would treat their own;
- Storing, transporting and transferring data using encryption and secure password protected devices;
- Deleting data in line with this policy and the retention schedule.

4. Rights of Individuals

In all aspects of its work The Council will ensure that the rights of its data subject are protected by all practicable measures. Subject to exceptions, the rights of the data subject as defined in law are:

- **The right to be informed** – The Council advises individuals how it will use their data through our Privacy Notice and other documentation such as consent forms where appropriate;
- **The right of access** – An individual is entitled to the following when they make a data subject access request (DSAR)
    - Confirmation that their data is being processed;
    - Access to their personal data;
    - Other supplementary information which largely corresponds to the information that should be provided in the Privacy Notice.

  The Council must respond to such a request within 30 days unless the request is complex, in which case it may be extended by a further 60 days;
- **The right to rectification** – Individuals have the right to rectify information that they think is inaccurate or incomplete. The Council has a duty to investigate any such claims and rectify the information where appropriate within 30 days, unless an extension of up to a further 60 days can be justified;
- **The right to erasure** – The right for an individual to request that their data is erased when there is no compelling reason for their data to be processed, though this is not absolute. This is applicable:
    - When original purpose for the personal data is no longer necessary or the data itself is no longer necessary for the purpose;
    - When the individual no longer consents;
    - If the individual objects to their data being processed and there is no legitimate reason to override this objection;
    - If the data being processed relates to the offer of information society services to a child;
    - If the data is ever processed in breach of data protection regulations (i.e. UK GDPR);
    - There is a legal obligation to erase the data.
- **The right to restrict processing** – Individuals have the right to restrict the use of their information, but The Council are still permitted to store the personal data. An individual may make a request for restriction and The Council have 30 days to respond;
- **The right to data portability** – Individuals have a right to make a request in relation to data which is held electronically for it to be transferred to another organisation or to themselves where they have provided either directly;
- **The right to object** – Individuals have a right to object in relation to the processing of data for:
    - A task carried out in the public interest;
    - For the exercise of official authority;
    - For their legitimate interests;
    - For scientific, historical research or statistical purposes;
    - For direct marketing purposes.
- **The rights related to automated decision making.** It is noted that The Council do not undertake this type of processing of personal data.

5. Processing Personal Data

The Council will process personal data (that is not classed as special categories of personal data) for one or more of the following reasons:

- The data subject has given consent to the processing of his or her personal data for one or more specific purpose;
- It is necessary for the performance of a contract, e.g., your contract of employment (or services); and/or
- It is necessary to comply with any legal obligation; and/or
- It is necessary for the council's legitimate interests (or for the legitimate interests of a third party), unless there is a good reason to protect your personal data which overrides those legitimate interests; and/or
- It is necessary to protect the vital interests of a data subject or another person; and/or
- It is necessary for the performance if a task carried out in the public interest or in the exercise of official authority vested in the controller.

If The Council processes personal data (excluding special categories of personal data) in line with one of the above bases, it does not require consent. Otherwise, The Council is required to gain consent to process personal data. If The Council asks for consent to process personal data, then we will explain the reason for the request. And consent can be withdrawn later.

6. Impact Assessments

If processing is carried out which results in a high risk to rights and freedoms, The Council will carry out a Data Protection Impact Assessment (DPIA) to determine the necessity and proportionality of processing. This will include considering the purposes for which the activity is carried out, the risks for individuals and the measures that can be put in place to mitigate those risks. If the processing takes place which relies on legitimate interests as the legal basis then the Council would undertake a Legitimate Interests Assessment (LIA).

7. Data Breaches

The Council have robust measures in place to minimise and prevent data breaches from taking place. Should a breach of personal data occur The Council must take notes and keep evidence of that breach.

If individuals are aware of a data breach, please contact the Clerk or Chairman of The Council immediately and keep any evidence relating to the breach.

The Council will record all data breaches regardless of their effect and impact on the data subject. If The Council discovers that there has been a breach personal data that poses a high risk to the rights and freedoms of individuals, we will report it to the Information Commissioner within 72 hours of discovery.

Any employee who knowingly or recklessly contravenes any instruction contained in, or following from, this Policy may, depending on the circumstances of the case, have disciplinary actions, which could include dismissal, taken against them.

8. Retention and Destruction

Timeframes for retention of documents have been set using legislative requirements.

The attached Appendix 1 shows the minimum requirements for the retention of documents as determined by those officers responsible for the management of these particular documentation types.

Destruction of paper documents will be done by way of shredding and electronic destruction is under review.

9. Definitions

"Personal data" is any information that relates to a living individual who can be identified from that data (for example a name, photograph, video, email or postal address) on its own, or when combining it with other information which helps to identify a living individual. This personal data may include (but is not limited to):

- Name and address (including email address);
- Bank details;
- References;
- Employment history;
- Taxation and national insurance records;
- Bookings (halls etc);
- Complaints.

"Special categories of personal data" may include more sensitive information such as:

- Racial or ethnic origin;
- Political opinions;
- Religious or philosophical beliefs;
- Trade union membership;
- Health, sex life or sexual orientation;
- Genetic or biometric data.

"Criminal records data" means information about an individual's criminal convictions and offences, and information relating to criminal allegations and proceedings and will be treated in much the same way as ‘special category personal data’.

“Processing” is any use that is made of data, including collecting, recording, organising, consulting, storing, amending, disclosing or destroying it.

“Data subject” refers to any living individual whose personal data is collected, held or processed by The Council.

“Data controller” is the person responsible who determines the purposes for which and the means by which personal data is processed.

Appendix 1

Finance

Document	Retention Period
Financial Published Final Accounts	Indefinitely
Signed Audited Accounts	Indefinitely
Final Accounts working papers	5 years
Records of all accounting transactions	At least 5 years
Cash books (records of monies paid out and received)	6 years
Purchase orders	6 years
Invoices received	6 years
Payment vouchers (copy invoices)	6 years
BACS listings	6 years
Goods received notes, advice notes and delivery notes	3 years
Asset register	10 years
Financial Plan	Indefinitely
Budget estimates – detailed working papers and summaries	3 years
Bank statements (electronic or hard copies)	6 years
Banking records including cheques	6 years
Bank reconciliation	3 years
Grant/funding applications and claims	5 years
Precept forms	Indefinitely
Internal audit plans/reports	3 years
Payroll and tax information	6 years
Record of payments made to employees (wages)	6 years
Statutory end of year returns to Inland Revenue and Pensions Section	Indefinitely
VAT, Income Tax and National Insurance Records	6 years
Current and expired insurance contracts	6 years

Personnel

Unsuccessful application forms	6 months
Unsuccessful reference requests	1 year
Successful application forms and CVs	For duration of employment + 5 years
References received	For duration of employment + 5 years
Statutory sick records, pay, calculations, certificates etc	For duration of employment + 5 years
Annual leave records	For duration of employment + 5 years
Annual appraisal/assessment records	Current year and previous 2 years

Personnel files and training records	5 years after employment ceases
DPIs for Councillors	5 years after standing down

Corporate

Minutes and reports of ALL committee meetings and working groups	Indefinitely
Policies and procedures	Until updated or reviewed
Internal audit records	3 years
Questionnaire data	Indefinitely
All emails and correspondence	1 year
Warranties	10 years
Risk assessment forms	2 years
Approved minutes	Indefinitely
Draft/rough notes taken at meeting	Until minutes are approved
Electoral Role from District Council	Until updated