



Appleton Parish Council

Appleton Parish Hall, Dudlow Green Road, Appleton, WA4 5EQ
Telephone 01925 268153 Email clerk@appletonparish.gov.uk

Data Protection Policy

Adopted by Appleton Parish Council by resolution on 20 October 2025 and will be reviewed periodically thereafter.

Reviewed: 21 April 2026 (8)

1. Introduction

This Data Protection Policy has been prepared to ensure that all councillors, Employees and Volunteers, who have access to and/or handle personal data associated with Appleton Parish Council (the Council), are aware of the current data protection regulations requirements. Furthermore, this policy also aims to make sure that the data subjects themselves are aware of their rights.

This policy also sets out the Council's commitment to protecting personal data and how the Council will implement that commitment.

This policy applies to all councillors, employees and volunteers working with the Council.

This policy is based upon the requirements of:-

Data Protection Act (DPA) 2018.

General Data Protection Regulation UK (GDPR) 2021.

Data Use and Access Act (DUAA) 2025.

2. Definitions

2.1. Personal Data

Personal data is information about individuals that enables them to be identified. This could include their name, address, place of work, contact information, other types of personal information, etcetera. This information could be located and stored in physical or IT based record systems.

2.2 Data handlers

Data Handlers means all Appleton Parish Councillors, Council employees and Volunteers working with The Council who are authorised to process, store or handle personal data information.

2.3 Data Controller

The Parish Council is the Data Controller. The Council decides what personal information it will hold and for how long it will be used or retained. It is the Data Controller's responsibility to establish practices and policies in line with the requirements of the Act.

The Proper Officer (The Clerk) will act as the nominated officer for data protection.

2.4 Information Commissioner's Office (ICO)

The Information Commissioner's Office (ICO) is the UK's independent regulatory office for data protection and freedom of information.

2.5 Data Protection Officer (DPO)

The Data Protection Officer (DPO) is the person or persons who ensure that laws protecting personal data are being implemented within an organisation.

Parish Councils are not required to appoint a Data Protection Officer because they are not considered to be public authorities for the purposes of GDPR under the Data Protection Act 2018.

3. Appleton Parish Council is Committed to: -

- Ensuring that the Council complies with the data protection principles as set out in the current UK data protection legislation.
- Ensuring that personal data is collected only for the specified purpose and that it will be used fairly and lawfully.
- Processing personal data only in order to meet the operational needs of the Council, or to fulfil legal requirements.
- Taking steps to ensure that personal data is up to date and accurate.
- Establishing appropriate retention periods for personal data.
- Ensuring that data subject's rights including access, rectification, erasure and data portability, can be appropriately exercised.
- Providing adequate security measures to protect personal data.
- Ensuring that a nominated officer is responsible for data protection compliance and provides a point of contact for all data protection issues.
- Ensuring that all staff are made aware of good practice regarding data protection.
- Providing adequate training for all staff responsible for personal data.
- Ensuring that everyone handling personal data knows where to find further guidance.
- Detecting, reporting and managing personal data breaches in accordance with legal requirements.
- Ensuring that queries regarding data protection, both internal and external to the Council's activities, are dealt with effectively and promptly.
- Regularly reviewing data protection procedures and guidelines within the Council.

4. The seven principles of the Data Protection Act 2018 (DPA)

4.1. Lawfulness, fairness and transparency

Personal data must be collected and processed lawfully, fairly and transparently and individuals must be told about its collection and use.

4.2. Purpose limitation

Personal data must be collected only for specified, explicit and legitimate purposes and not further processed or used in a way that is incompatible with those purposes.

4.3. Data minimisation

Personal data must be adequate, relevant and limited only to what is necessary for the processing purpose.

4.4. Accuracy

Personal data must be accurate and where necessary, kept up to date. Inaccurate or incomplete data must be corrected or deleted.

4.5. Storage limitation

Personal data must not be kept for longer than is necessary for the purposes for which it is processed.

4.6. Integrity and confidentiality

Personal data must be processed in a manner that ensures appropriate security, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage.

4.7. Accountability

The controller or processor is responsible for complying with these principles and must be able to demonstrate compliance.

5. Data Handlers Responsibilities

All Data Handlers are responsible for the safeguarding of any personal data that they come into contact with whilst carrying out their duties on behalf of Appleton Parish Council.

All Data Handlers are responsible for maintaining the confidentiality of information supplied by the public, unless the subject has given permission otherwise.

6. Storage of data

Appleton Parish Council recognises its responsibilities when it takes personal details about people. This information will be kept within the Parish Council's facilities and is not available for public access. This personal data shall be stored by the Parish Council within secure, password protected, office computer(s).

Retention of documents will be in accordance with the Parish Council's Retention Policy..

7. Subject Access Requests (SARs)

Appleton Parish Council is aware that people have the right to access any personal information that is held about them. These Subject Access Requests (SARs) must be submitted writing using hard copy or email. In some cases the Council may need to verify the requestor's identity, or a third party's authorisation, before the request can be processed. The Council will inform the requester if there is a need for the verification together with details of the documents that the Council require to achieve this.

8. Data Breaches

GDPR defines a personal data breach as "a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure of or access to, personal data".

Data breaches could include: -

- Access by an unauthorised third party
- Deliberate or accidental action by a data handler
- Sending personal data to an incorrect recipient
- Computer devices containing personal data being lost or stolen
- Alteration of personal data without permission
- Loss of availability of personal data

9. Reporting a Data Breach

If and when a Data Handler becomes aware of a data breach that may result in a risk to the rights and freedoms of the individual, the breach must be: -

- Reported to the Information Commissioner's Office (ICO) without delay and in any event within 72 hours of having become aware of the breach.
- Reported to affected individuals without undue delay
- Reported to the Parish Clerk or the Chair of the Council as soon as possible.

If the data breach is thought to be high-risk, affected individuals must be informed directly, explaining the breach and the steps being taken too mitigate it.

The ICO can be contacted at: -

<https://ico.org.uk/fororganisations/report-a-breach>