Redditch Assemblies of God

Date Protection Policy

Redditch Assemblies of God Church needs to gather and use certain information about individuals. This can include clients, contacts, employees and other people the organisation 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 organisation's data protection standards and to comply with the law.

This data management policy ensures Redditch Assemblies of God Church;

- complies with data protection law and follows good practice
- protects the rights of clients, staff and members
- is transparent about how it stores and processes individuals' data
- protects itself from the risks of a data breach

Data protection law

The UK General Data Protection Regulation (GDPR) applies in the UK. It outlines that personal data must be:

1. Processed lawfully, fairly and in a transparent manner in relation to individuals.
2. Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes. Further processing for archiving purposes in the public interest, scientific or historical research or statistical purposes shall not be considered to be incompatible with the initial purposes.
3. Adequate, relevant and limited to what's necessary in relation to the purposes for which they're processed.
4. Accurate and, where necessary, kept up to date.
5. Protected—Every reasonable step must be taken to ensure that inaccurate personal data, having regard to the purposes for which they're processed, is erased or rectified without delay.
6. Kept in a form that permits identification of data subjects for no longer than is necessary, and for the purposes for which the personal data is processed (personal).
7. Stored for longer periods. For example, the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes. This will also be subject to implementation of the appropriate technical and organisational measures required by UK GDPR in order to safeguard the rights and freedoms of individuals.
8. Processed in a manner that ensures appropriate security of personal data. This includes protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

9. Managed by a controller responsible for, and be able to demonstrate, compliance with the principles.

People and responsibilities

Everyone at Redditch Assemblies of God Church contributes to compliance with UK GDPR. Key decision-makers must understand the requirements and accountability of the organisation to prioritise and support the implementation of compliance.

Data Protection Officer (DPO), the person responsible for fulfilling the tasks of the DPO in respect of Redditch Assemblies of God Church is (Elaine Palmer-Taylor). They are responsible for leading on compliance with the regulations.

These responsibilities should include (but are not necessarily limited to):

1. Inform and advise the organisation and its employees about their obligations to comply with UK GDPR and other data protection laws
2. Monitor compliance with UK GDPR and other data protection laws – including managing internal data protection activities, advising on data protection impact assessments, training staff and conducting internal audits
3. Be the first point of contact for supervisory authorities and for individuals whose data is processed (employees, members)
4. Keeping the board updated about data protection issues and risks.
5. Documenting, maintaining and developing the organisation’s data protection policy and related procedures, in line with agreed schedule.
6. Embedding ongoing privacy measures into policies and day-to-day activities, throughout the organisation. The policies themselves will stand as proof of compliance.
7. Dealing with subject access requests, deletion requests and queries from clients, stakeholders and data subjects about data protection related matters.
8. Checking and approving contracts or agreements with third parties that may handle the organisation's sensitive data.
9. Ensuring all systems, services and equipment used for storing data meet acceptable security standards.
10. Performing regular checks and scans to ensure security hardware and software are functioning properly.
11. Evaluating any third party services the company is considering using to store or process data, to ensure their compliance with obligations under the regulations.
12. Developing privacy notices to reflect a lawful basis for fair processing, ensuring that intended uses are clearly articulated. This will also ensure that data subjects understand how they can give or withdraw consent, or exercise their rights in relation to the company's use of their data.

13. Ensuring that audience development, marketing, fundraising and all other initiatives involving processing personal information and/or contacting individuals abide by the UK GDPR principles.

Scope of personal information to be processed

1. The scope of the data we may process:

    - names of individuals
    - postal addresses of individuals
    - email addresses and other contact information
    - marriage, baptismal, dedications and funeral
    - membership information i.e. gift aid, tithing and donations
    - Accident
    - Payroll

    Any other information deemed necessary for legal reuirements and the smooth running of the church.

2. Where the data is collected from and stored?

    The data is stored electronically on designated PC's but mainly on software on the cloud.

3. Consideration is made to ensure that the data is accurate. We check accuracy, duplication and completeness of data. We only keep data that is relevant to the purpose, not excessive, up-to-date and not kept for longer than is necessary.

4. Details of any sensitive special categories of personal information?

    Is restricted and used only for the intended purpose.

Uses and conditions for processing

- intended purpose for that processing
- data to be processed
- the lawful basis for processing
- plan for how these conditions for processing are supported

Consent

In cases where we rely on consent as the lawful condition for processing, we will review the processes and systems to make sure that consent is freely and unambiguously given for specific purposes, and that we can evidence an affirmative action on the part of the data subject to have indicated consent, and such that data subjects can reasonably understand who is using their personal information, what information, and for what purposes, and using which communications channels. We will demonstrate how and when consent was obtained upon request. Our practices and systems will communicate an individual's right to withdraw consent at any time.

Where 'legitimate interest' is the lawful condition for processing, evidence will be given of the process by which the rights and freedoms of the individual have been weighed against the

interests of the company, and how consideration/mitigation of the outcomes of the process have been made.

Data Sharing

Data will be kept within the organisation. If we intend to share any personal information with a third-party organisation, prior notice will be given and consent obtained.

Where other lawful conditions for processing are relied upon for data sharing, these will be described beforehand.

Security measures

The measures that are in place to protect the personal information stored.

- Measures have been put in place to leverage technology to require or ensure compliance. Such as, restricting and protecting access to the data to those people for whom it is necessary to perform the processing. Security software and firewalls, encryption, and the use of secure Virtual Private Networks (VPN), log-in restricted access.

The procedural and organisational policy measures;

- protocols for safe transfer of data in transit
- protocols for password management
- data back-up

Data breaches;

- If a data breach is identified, the DPO will notify the ICO and suggested take the necessary advise to manage the breach.

Subject access requests

All individuals who are the subject of data held by your organisation are entitled to:

- ask what information the company holds about them and why
- ask how to gain access to it
- be informed how to keep it up to date
- be informed how the company is meeting its data protection obligations

The timeframe for processing the SAR will align with legal requirements unless otherwise notified of delays.

The right to be forgotten

In certain circumstances, subjects have the right to be deleted from your database. The organisation will evaluate the individual's right to be deleted and comply unless there is a

legal basis to retain certain information. The following example is a guide and is not an exhaustive list of legal information that should be kept.

- **Accident Records:** Minimum of 3 years since the last entry, or if it involves a child until they reach 21.
- **Income Tax and NI:** Minimum of 3 years from the end of the financial year to which they relate.
- **Maternity and Paternity:** Minimum of 3 years from the end of the tax year in which the leave ends.
- **Salary and Pay:** Minimum of 6 years.
- **Working Time:** 2 years.

Privacy notices

Redditch Assemblies of God Church aims to ensure that individuals are aware that their data is being processed, and that they understand:

- who is processing their data
- what data is involved
- the purpose for processing that data
- the outcomes of data processing
- how to exercise their rights

The company has a privacy statement, setting out how data relating to these individuals is used by the company.

The privacy statement can be viewed on redditchaog.org.uk.

Ongoing documentation of measures to ensure compliance

Meeting the obligations of the UK GDPR to ensure compliance will be an ongoing process. Redditch Assemblies of God Church implements the following ongoing measures:

- maintain documentation/evidence of the privacy measures implemented and records of compliance
- regularly test the privacy measures implemented and maintain records of the testing and outcomes
- use the results of testing, other audits, or metrics to demonstrate both existing and continuous compliance improvement efforts
- keep records showing training of employees on privacy and data protection matters

POLICY DATED: 13/08/2024

REVIEW DATE: *August 2026*