The United Reformed Church

South Western Synod

Moderator: Revd Ruth Whitehead

Taunton URC
18 Paul Street
Taunton
Somerset TA1 3PF

01823 275470
synodoffice@urcsouthwest.org.uk
www.urcsouthwest.org.uk

The United Reformed Church (South Western Synod) Incorporated

Data Protection Policy

Introduction

The United Reformed Church (South Western Synod) Incorporated is committed to protecting all of the information which we process concerning the people we support and work with, and to respecting people's rights around how their information is handled. This policy explains our responsibilities and how we will meet them.

*A glossary of terms highlighted in **bold** will be found in Schedule 1at the end of this document.*

Section A – What this policy is for

1. Policy statement

1.1 The United Reformed Church (South Western Synod) Incorporated (The Synod) is committed to protecting **personal data** and respecting the rights of our **data subjects,** namely the people whose **personal data** we collect and use. We value the personal information entrusted to us and we respect that trust, by complying with all relevant laws, and adopting good practice.

We **process** personal data to enable us to:

a) administer records of Synod members, officers and committee members;
a) provide an annual directory (The South Western Synod Year Book);

b) administer records of Board and sub-committee members;

c) manage or supervise ministerial candidates and provide lay and ministerial training;**

d) provide pastoral support for ministers, students and others connected with the United Reformed Church;

e) maintain and update records of office holders at local churches, and Synod representatives;

f) recruit, support and manage employees and volunteers;

g) arrange or manage training, and training records;

h) arrange meetings or conferences;

i) safeguard children, young people and adults at risk;

j) maintain our financial accounts and records (including the processing of gift aid);

k) make grants;

l) pay expenses;

m) fundraise and promote the interests of the United Reformed Church, including online and via social media;

n) manage our properties (including, purchases, sales, lettings, hiring, licenses and leases);

o) maintain the security of property and premises;

p) liaise with contractors;

q) maintain records including minutes of meetings

r) provide news and information about events, activities and services in the Synod, in local churches and in the wider world;

s) enable the Synod to engage with churches, charities and community groups

t) enable the Synod to provide voluntary services for the benefit of the public in the South Western province;

u) provide contact details of officers and others with specific responsibilities (eg Disclosure & Barring Service signatories) to the Synod office and Church House. This enables the national administration of the United Reformed Church;

v) respond effectively to correspondence, enquiries and to handle any complaints.

**Ministers should also refer to the Privacy Policy for Ministers and Church Related Community Workers, available from the Ministries Department at Church House.

1.2 This policy has been approved by the Synod Trust Officers, as has the appointment of the Moderator to act as Data Controller for the purposes of the General Data Protection Regulations 2016. The Moderator is responsible for ensuring that we comply with all our legal obligations and sets out the legal rules that apply whenever we obtain, store or use personal data.

1.3 This policy will be reviewed on an annual basis.

2. Why this policy is important

2.1 We are committed to protecting personal data from misuse, and from being shared without consent, whether through poor security or careless work practices. We want the information we process to be accurate, and to avoid the upset or harm which might be caused to people through any form of poor practice or breach of General Data Protection Regulations.

2.2 This policy sets out the measures we are committed to taking as an organisation and, what each of us will do to ensure we comply with the relevant legislation.

2.3 In particular, we will make sure that all personal data is:

a) processed lawfully, fairly and in a transparent manner;

b) processed for specified, explicit and legitimate purposes and not in a manner that is incompatible with those purposes;

c) adequate, relevant and limited to what is necessary for the purposes for which it is being processed;

d) accurate and, where necessary, up to date;

e) not kept longer than necessary for the purposes for which it is being processed

f) processed in a secure manner, by using appropriate technical and organisational means;

g) processed in keeping with the rights of data subjects regarding their personal data.

3 How this policy applies to you, and what you need to know

3.1 Whether you are an officer, trustee, committee member, employee or volunteer of the United Reformed Church (South Western Synod) Incorporated, whenever you process personal information on behalf of the Synod, you are required to fully comply with this policy. If you think that you have accidentally breached the policy, it is important that you contact our Data Protection Lead (The Moderator as Data Controller) immediately so that prompt action can be taken to try and limit the impact of the breach.

Anyone who breaches the Data Protection Policy may be subject to disciplinary action, and where that individual has breached the policy intentionally, recklessly, or for personal benefit they may also be liable to prosecution or to regulatory action.

3.2 As a line manager of the Synod: You are required to make sure that any data-processing activities for which you are responsible, follow the rules set out in this Data Protection Policy.

3.3 As a data subject of the Synod: We will handle your personal information in line with this policy.

3.4 As an appointed **data processor**/contractor: Companies who are appointed by us as a data processor are required to comply with this policy under their contract with us. Any breach of the policy will be taken seriously and could lead to the Synod taking contract enforcement action against the company, or terminating the contract. Data processors have direct obligations under the General Data Protection Regulation 2016 [the GDPR], primarily to only process data on instructions from the controller (us) and to implement appropriate technical and organisational measures to ensure a level of security which is appropriate to the risk involved.

3.5 The Moderator of the South Western Synod as Data Protection Lead is responsible for:

a) advising the Synod, its members and employees about their legal obligations under data protection law:
b) monitoring compliance with data protection law;
c) dealing with data security breaches and
d) Managing the development of this policy.

Any questions about this policy or any concerns that the policy has not been followed should be referred to the Moderator at moderator@urcsouthwest.org.uk. (We have resolved not to designate a Data Protection Officer as this is not required under article 37.1 of the GDPR).

3.6 Before you collect or handle any personal data as part of your work (paid or otherwise) for the Synod, it is important that you take the time to read this policy carefully and understand what is required of you, as well as the organisation's responsibilities when we process data.

3.7 Our procedures will be in line with the terms of this policy, but if you are unsure about whether any of your processing activities might breach this policy you must first speak to the Data Protection Lead.

4. Training and guidance

4.1 We will provide general training at least annually for all Synod staff to raise awareness of their obligations and our responsibilities, as well as to outline the law.

4.2 We may also issue procedures, guidance or instructions from time to time. Line managers must ensure that the employees whom they manage understand the implications of GDPR on their work.

Section B – Our data protection responsibilities

5. What personal information do we process?

5.1 In the course of our work, we may collect and process information (personal data) about many different people (data subjects). This includes data we receive straight from an individual, for example, where they complete forms or contact us. We may also receive information about data subjects from other sources including, for example, previous employers, referees, estate agents, conveyancers, complainants, witnesses, or other church bodies.

5.2 We process personal data in both electronic and paper form, and all such data is protected under data protection law. The personal data we process can include, but is not restricted to information such as:

a) names and contact details;
b) further details of directors;
c) personnel records of employees;
d) records of complaints;
e) records of financial transactions including rent arrears;
f) contracts and correspondence.

5.3 In some cases, we hold types of information referred to as **"special category"** data in the GDPR. This personal data will only be processed under strict conditions as set out in the GDPR .

5.4 We will only process or hold data relating to criminal proceedings or offences, or allegations of offences:

a) for the purposes of recruitment;
b) if the data is required by our insurers;
c) if there is an overarching safeguarding requirement to process this data for the protection of children and adults who may be put at risk.

This processing will only ever be carried out on advice from the Synod Safeguarding Advisor or the Ministries Team of the United Reformed Church.

5.5 Other data may also be considered 'sensitive' such as bank details, but will not be subject to the same legal protection as 'special category' data as set out in the GDPR.

6. How we will process personal data.

6.1 Making sure processing is fair and lawful

We will process all data fairly and lawfully by ensuring our processing activities meet one or more of the legal bases, as listed below, and are carried out in a transparent manner. This means we will provide people with an explanation of how and why we process their personal data including any data provided by other parties.

6.2 Our legal basis for processing personal data.

We will act lawfully by only processing personal data under one of the following legal conditions, as listed in Article 6 of the GDPR:

a) processing is necessary for a contract with the data subject;

b) the processing is necessary for us to comply with a legal obligation;

c) processing is necessary to protect someone's life (this is called vital interests, and is likely to arise only in the case of a medical emergency);

d) processing is necessary for us to perform a task in the public interest, and the task has a clear basis in law;

e) processing is necessary for legitimate interests pursued by the Synod or another organisation, unless these are overridden by the interests, rights and freedoms of the data subject.

f) If none of the other legal conditions apply, the processing will be conducted lawfully through us seeking the clear consent of the data subject.

6.3 Our legal use of 'special category' data.

We will act lawfully by only processing 'special category' personal data when, in addition to the conditions above, one of the extra conditions, as listed in Article 9 of the GDPR, is met. These conditions include where:

a) processing is necessary for carrying out our obligations under employment and social security and social protection law;

b) processing is necessary for safeguarding the vital interests (in emergency, life or death situations) of an individual and the data subject is incapable of giving consent;

c) processing is carried out in the course of our legitimate activities and only relates to our members or persons we are in regular contact with in connection with our purposes;

d) processing is necessary for pursuing legal claims;

e) If none of the other legal conditions apply, the processing will be conducted lawfully through us seeking the explicit consent of the data subject.

6.4 Before deciding which condition should be relied upon, we may refer to the original text of the GDPR as well as any relevant guidance, and seek legal advice as required.

Informing individuals when we use their data.

6.5 When personal data is collected directly from an individual, we will ensure that they understand why we are asking for this data, the way/s it will be processed, and the legal basis on which we are relying for processing. We will make sure the individual is fully informed on who we are, how to contact us, and how to access our **Privacy Notice**. We will explain any consequences of not providing data if this will impact on the service we wish to provide or prevent us from entering into a contract or fulfilling a legal obligation. We will inform the individual of any information which will need to be shared, why, and with whom, including if the third party is outside of the European Union.

6.6 If data is collected from another source, rather than directly from the data subject, we will provide the data subject with confirmation of the data received together with the information set out above at 6.5.

We will provide this notification within 1 month of us receiving the data, unless any legal exemption applies. If we use the data to communicate with the data subject, we will clearly explain how we came about their contact details and any other information passed to us.

If we plan to pass the data onto someone else outside of the Synod, we will give the data subject this information before we pass on the data, and will seek their express consent, unless any legal exemption applies.

7. When consent is needed to process data.

7.1 Where none of the other legal conditions apply to the processing, we will seek consent from the data subject. When doing this we will clearly set out what we are asking consent for, why we are collecting the data and how we plan to use it. Consent will be restricted to each process we seek consent for and we will only ask for consent when the data subject has a real choice whether or not to provide us with their data.

7.2 Consent, once given, can be withdrawn at any time in which case data processing will stop, unless legal requirements dictate otherwise. Data subjects will be informed of their right to withdraw consent and it will be as easy to withdraw consent as it is to give consent.

8. Processing for specified purposes

We will only process personal data for the specific purposes explained in our privacy notices (summarised in section 0) or for other purposes specifically permitted by law. We will explain those other purposes to data subjects as set out in section 6, unless there are lawful reasons for not doing so.

9. Data will be adequate, relevant and not excessive

We will only collect and use personal data that is needed for the specific purposes described above (which will normally be explained to the data subjects in privacy notices). We will not collect more than is needed to achieve those purposes.

10. Accurate data

We will make sure that personal data held is accurate and up to date. The accuracy of personal data will be checked at the point of collection and at appropriate future times.

11. Keeping data and destroying it

We will keep personal data only for as long as is necessary for the purposes for which it was collected. We will maintain appropriate retention periods for specific records, and these will be incorporated into our Privacy Notice.

12. Security of personal data

12.1 We will use appropriate measures to keep personal data secure at all points of the processing. Keeping data secure includes protecting it from unauthorised or unlawful processing, or from accidental loss, destruction or damage, and as such, information will only be shared within the Synod on a need-to-know basis.

12.2 All security measures will be tailored to effectively meet the degree of risk involved in the processing and will include both technical and procedural measures. These will be assessed based on, amongst other things:

a) the quality of the security measure;
b) implementation costs;
c) the nature, scope, context and purpose of processing;
d) the degree of risk to the rights and freedoms of data subjects;
e) the potential risk/s which could result from a data breach.

12.3 Appropriate security measures may include:

a) technical systems security;
b) measures to restrict or minimise access to data;
c) measures to ensure systems and data remain available, or can be easily restored in the case of an incident;
d) physical security of information and of our premises;
e) organisational measures, including policies, procedures, training and audits;
f) regular evaluation and review of the effectiveness of security measures.

13. Keeping records of our data processing

For transparency and legal purposes we will keep clear records of our processing activities by way of a data mapping audit, which will be reviewed annually. We will note any changes made concerning data-processing explaining why these decision have been made.

Section C – Working with people we process data about (data subjects)

14 Data subjects' rights

14.1 We will process personal data in line with data subjects' rights, including their right to:

a) request access to any of their personal data held by us (known as a Subject Access Request);

b) ask to have inaccurate personal data changed;

c) restrict processing, in certain circumstances;

d) object to processing, in certain circumstances, including preventing the use of their data for direct marketing;

e) receive any data requested in a format portability, which means to receive their data, or some of their data, in a format that can be easily used by another person (including the data subject themselves) or organisation;

f) not be subject to automated decisions, in certain circumstances; and

g) withdraw consent when we are relying on consent to process their data.

14.2 If a colleague receives any request from a data subject that relates or could relate to their data protection rights, this will be forwarded to our Data Protection Lead immediately.

14.3 We will act on all valid requests as soon as possible, and at the latest within one calendar month, unless we have reason to, and can lawfully extend the timescale. This can be extended by up to two months in some circumstances.

14.4 All data activities relating to subjects' rights will be provided free of charge.

14.5 Any information provided to data subjects will be concise and transparent, using clear and plain language.

15. Direct marketing

15.1 We will comply with the rules set out in the GDPR, the Privacy and Electronic Communications (EC Directive) Regulations 2003 [PECR] and any laws which may amend or replace the regulations around **direct marketing**. This applies to all forms of contact with individuals.

15.2 Any direct marketing material that we send will identify the United Reformed Church South Western Synod Incorporated as the sender and will include an option to opt out of receiving similar communications in the future, which will be actioned on receipt.

Section D – working with other organisations & transferring data

16. Sharing information with other organisations

16.1 Unless there is a legal exemption, we will only share personal data when we have a legitimate basis to do so and we have informed the data subject that this might happen via our Privacy Notice.

16.2 We will keep records of information shared with third parties, which will include any legal exemptions and why they have applied. We will follow the **Information Commissioner's Office** statutory ***Data Sharing Code of Practice*** (or any replacement code of practice) when sharing personal data with other data controllers. Legal advice will be sought as required.

17. Data processors

17.1 Before appointing a contractor to process personal data on our behalf we will carry out due diligence checks. These will ensure the contractor has appropriate technical and organisational measures to comply with the data protection legislation including data security and the rights of data subjects. We will only appoint contractors who can meet these criteria.

17.2 Any such appointments will be in writing using wording requiring legal compliance from the contractor. We will monitor processing activities and contract-compliance.

18 Transferring personal data outside the European Union (EU)

18.1 We will only transfer personal data outside the EU where permitted by GDPR. This includes storage on a "cloud" based service where the servers are located outside the EU.

18.2 We will only transfer data outside the EU where it is permitted by one of the conditions for non-EU transfers in the GDPR.

Section E – Managing change & risks

19. Data protection impact assessments

19.1 Whenever we carry out data processing activity with a high risk, we will first carry out a Data Protection Impact Assessment (DPIA). This includes where we process data relating to vulnerable people, trawling of data from public profiles, using new technology, and transferring data outside the EU. Any decision not to conduct a DPIA will be recorded.

19.2 We may also conduct a DPIA in other cases when we consider it appropriate to do so. If we are unable to mitigate high risk we will consult with the ICO.

19.3 DPIAs will be conducted in accordance with the ICO's Code of Practice ***Conducting privacy impact assessments***.

20. Dealing with data protection breaches

20.1 We will promote a culture of honesty and integrity so that any person processing data in connection with Synod purposes will report immediately, to the Data Protection Lead, any actual or potential breach of this policy.

20.2 We will keep records of personal data breaches, even if we do not report them to the ICO.

20.3 We will report all data breaches which are likely to result in risk to any person, to the ICO. Reports will be made to the ICO within **72 hours** from the breach becoming known.

20.4 In situations where a personal data breach causes a serious risk to any person, we will additionally inform data subjects whose information is affected, without undue delay. This can include situations where, for example, bank account details are lost, or an email containing sensitive information is sent to the wrong recipient. Informing data subjects can enable them to take steps to protect themselves and/or to exercise their rights

Schedule 1 – Definitions and useful terms

The following terms are used in this policy and are defined as set out within the GDPR.

Data controller. Any person, company, authority or other body who (or which) determines the means for processing personal data and the purposes for which it is processed. It does not matter if the decisions are made alone or jointly with others.

The data controller is responsible for the personal data which is processed and the way in which it is processed. We are the data controller of data which we process.

Data processors. Individuals or organisations which process personal data on our behalf and on our instructions e.g. an external organisation which provides secure waste disposal for us.

Data subjects. All living individuals about whom we hold or process personal data. Data subjects have legal rights in relation to their personal information. Data subjects that we are likely to hold personal data about include:

a) trustees, subcommittee members and other volunteers;
b) our employees, their next of kin, and former employees;
c) consultants/individuals who are our contractors or employees working for them;
d) tenants;
e) grantees, debtors, creditors and those with whom we have financial transactions;
f) complainants;
g) supporters;
h) enquirers;
i) ministers and local church officers; and
j) advisers and representatives of other organisations.

Direct Marketing. Communication (by any means) of any advertising or marketing material which is directed, or addressed, to individuals. "Marketing" does not need to be selling anything, or be advertising a commercial product. It includes contact made by organisations to individuals for the purposes of promoting the organisation's aims.

ICO. The Information Commissioner's Office, which is the UK's regulatory body responsible for ensuring that we comply with our legal data protection duties. The ICO produces guidance on how to implement data protection law and can take regulatory action where a breach occurs.

Personal data. Any information relating to a living person who is either identified or is identifiable. This is an individual not a company or a public body. Representatives of companies or public bodies would, however, be natural persons. Personal data can be factual (for example, a name, address or date of birth) or it can be an opinion about that person, their actions and behaviour.

Privacy notice. The written statement made available to data subjects which explains how we process their data and for what purposes.

Processing. Widely defined to include any activity that involves the data. It includes obtaining, recording or holding the data, or carrying out any data processing including organising, amending, retrieving, using, disclosing, erasing or destroying it. Processing can also include transferring personal data to third parties, listening to a recorded message (e.g. on voicemail) or viewing personal data on a screen or in a paper document which forms part of a structured filing system. Viewing clear photographs or moving images of living individuals is also a processing activity.

Special categories of data. This information about a person's:

a) Racial or ethnic origin;

b) Political opinions;

c) Religious or similar (e.g. philosophical) beliefs;

d) Trade union membership;

e) Health (including physical and mental health, and the provision of health care services);

f) Genetic data;

g) Biometric data;

h) Sexual life and sexual orientation.

The United Reformed Church (South Western Synod) Incorporated is a Registered Charity, No 275364.