DATA PROTECTION POLICY

Living Waters Christian Fellowship, Darnall (LWCF) is committed to protecting personal data and respecting the rights of the individuals 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.

In May 2018 data protection law changed as GDPR, General Data Protection Regulation, came into force. This law gives individuals more rights over how information about them is stored and used by organisations, including churches. In particular, organisations have to tell individuals what they are doing with the information they are storing and using.

The GDPR requires personal data to be processed in a manner that ensures its security. This includes protection against unauthorised or unlawful processing and against accidental loss, destruction or damage. It requires that appropriate technical or organisational measures are used.

Therefore, LWCF must:

- only collect information that we need for a specific purpose;
- keep it secure;
- ensure it is relevant and up to date;
- only hold as much as we need, and only for as long as we need it; and allow you, the data subject of the information, to see it on request.

Good information handling is a core responsibility of the church, and it provides a range of benefits. Living Waters can enhance our local reputation, increase community and member confidence, by making sure personal information is accurate, relevant and safe.

The information we supply about the processing of personal data must be:

- concise, transparent, intelligible and easily accessible;
- written in clear and plain language, particularly if addressed to a child; or vulnerable adult with awareness disabilities

Living Waters Christian Fellowship, Darnall - Data Protection Policy

Introduction

1. UK legislation applies to all personal data regardless of the size of the organisation.

   In the full text of GDPR there are 99 articles setting out the rights of individuals and obligations placed on organisations covered by the regulation. These include allowing people to have easier access to the data companies and organisations hold about them, a new fines regime and a clear responsibility for organisations to obtain the consent of people they collect information about.

2. The principles are based upon:

   - The right of an individual (data subject) to know what data is being held about them and to check its accuracy; and
   - The concept that an individual's personal information should be used only for the specific purposes for which it is expressly held by an organisation and not disclosed to those who are not authorised to hold it.
   - It is the responsibility of the organisation to know what data it holds and to safeguard it**.**

3. Personal data relates to a living individual (or business entity) that can be identified from that data directly (or from that data plus other information in your possession). Identification can be by the information alone or in conjunction with any other information in the data controller's possession or which the data controller is likely to come into such possession.

4. GDPR requires, **Living Waters Christian Fellowship, Darnall**, as an organisation to:
   Notify all individuals (data subjects) that have personal data held by us, either in hard copy or electronic format, of:

      - Our Data Protection Policy by means of the "***Data Privacy Notice***" and
      - The nature of personal data held by us and their access to it by means of the "***Data Privacy Notice***"
      - Obtain the data subject's consent to hold such of their personal data that we currently hold (in either hard copy or electronic format) under the terms of the "Data Protection Policy" as set out here.
      - Draw the individual's attention to the availability and access of this policy document either on the website or in hard copy or electronic format by means of the "***Data Privacy Notice***". This should assist their full understanding of their personal rights relating to their personal data held by Living Waters Christian Fellowship, Darnall.

5. The GDPR puts an onus on an organisation to attend to its ethos to data protection in **that it must now show <u>how</u> it complies, not just that it complies.** It applies to data controllers and data processors and employees and volunteers alike.

6. **This new accountability principle requires demonstration of compliance**. It introduces a mandatory requirement to conduct a risk or a Privacy Impact Assessment (PIAs) where the processing of data is likely to significantly impact on the rights and freedoms of the data subject.

7. On a basic level some activities involve handling personal data. It is the organisation's responsibility to keep such information secure and ensure that individual's rights are respected.

8. Personal information can be:
   - Factual (e.g. Name, address or date of birth), or it can be
   - Opinion (e.g. performance appraisal), or
   - Statement of intention about them or
   - Online identifiers (e.g. computer IP addresses)

9. New rights include the right to "data erasure" and "data portability". A requirement to notify any relevant body or data subject of data breaches within 72 hours of becoming aware of the breach. Notification will not be necessary if the breach is unlikely to risk the rights and freedoms of the relevant data subjects.

10. There are hefty financial penalties for severe breaches and non-compliance. Accordingly, we will have to institute an awareness and training programme for those involved in church activities which include either church members or community outsiders. We must introduce and maintain within the wider church an ethos of caring about such data and its safety.

11. There are 3 key focal points that need to be addressed:
    - Children (requiring written Parental consent) and Vulnerable Adults which must be handled in a clear and sensitive manner;
    - Employees (requiring written consent as it is an amendment of their contract of employment);
    - General membership - nearly everybody else involved in church activities

    Each group will receive its own relevant version of the Data Privacy Notice and Consent document. See attachments.

Data Protection Policy
(Full Version)

Contents

1. Personal data
2. Data Controller
3. How do we process personal data?
4. What is the legal basis for processing personal data?
5. Sharing personal data
6. How long do we keep data?
7. Security of personal data
8. Keeping records of our data processing
9. Individual's rights - "Your rights and your personal data"
10. Further processing
11. Data protection impact assessments
12. Dealing with data protection breaches
13. Subject Access Requests (SARs)
14. Managing the Personal Information held
15. Contact Details

Schedule 1 – Definitions and useful terms

Schedule 2 – The Data Operational Hierarchy

Schedule 3 –UK version GDPR Exemptions

Living Waters, Darnall - Data Protection Policy

1. Personal data

Personal data relates to a living individual who can be identified from that data. Identification can be by the information alone or in conjunction with any other information in the data controller's possession or likely to come into such possession. The processing of personal data is governed by the General Data Protection Regulation (the 'GDPR').

2. Data Controller

The Trustees of Living Waters Christian Fellowship, Darnall ("LWCF") are ultimately responsible as the Data Controller; but the day to day responsibility rests with the Operational Data Controller and in turn those individuals (the external Data Processors and LWCF staff and volunteers) responsible for the direct input and thereby maintaining a responsibility to the Data Controller through the Operational Data Controller.

This means that LWCF decide how personal data is processed and for what purposes. See Schedule 2 for the data operational hierarchy.

The trustees must ensure that LWCF has sufficient staff, volunteers and skills to discharge our obligations under the GDPR.

3. How do we process personal data?

LWCF complies with its obligations under the GDPR by keeping personal data up to date; by storing and destroying it securely; by not collecting or retaining excessive amounts of data; by protecting personal data from loss, misuse, unauthorised access and disclosure and by ensuring that appropriate technical measures are in place to protect personal data.

We use personal data for the following purposes;

- Provide you with news and information about events and activities at the church
- Provide appropriate pastoral care
- Maintain communication between individuals and departments of the church
- Administer membership records
- Maintain financial accounts and records
- Fundraise and promote the interests of the church
- Manage our volunteer workforce
- Keep children and vulnerable adults safe

4. What is the legal basis for processing personal data?

Processing is carried out by a not-for-profit body with a religious aim provided: -

- the processing relates only to members or former members (or those who have regular contact with it in connection with those purposes); and
- there is no disclosure to a third party without consent or legal requirement; or
- Processing is necessary for carrying out obligations under employment, recruitment and management of volunteers, social security or social protection law, or a collective agreement; or
- Explicit consent of the data subject has been given.

5. Sharing personal data

Personal data will be treated as strictly confidential and will only be used within the designated purposes in section 3, and within the restrictions described in section 4.

We will only share personal data with third parties

- With the data subject's consent
- or if so required by law

6. How long do we keep data?

We retain data on the following basis:

Record Type	Retention Period
Membership data	Indefinitely
Contacts and friends of the church	12 months after last contact
Youth contacts	12 months after last contact
Foodbank, community projects	12 months after last contact
Gift Aid declarations	Indefinite
Gift aid claims	7 years after the relevant tax year
Registers of marriage	Indefinite
Registers of baptisms	Indefinite
Photographs and videos church events	Indefinite
Personal data relating to events for which Information is gathered	Disposed of immediately after the event unless retention is required because of an incident

7. Security of personal data

LWCF 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.

We will implement security measures which provide a level of security which is appropriate to the risks involved in the processing.

Measures will include technical and organisational security measures. In assessing what measures are the most appropriate we will take into account the following, and anything else that is relevant:

- The quality of the security measure;
- The costs of implementation;
- The nature, scope, context and purpose of processing;
- The risk (of varying likelihood and severity) to the rights and freedoms of data subjects; the risk which could result from a data breach.

Measures may include:

- Technical systems security;
- Measures to restrict or minimise access to data;
- Measures to ensure our systems and data remain available, or can be easily restored in the case of an incident;
- Physical security of information and of our premises, and
- Organisational measures, including policies, procedures, training and audits; regular testing and evaluating of the effectiveness of security measures

8. Keeping records of our data processing

To show how we comply with the law we will keep clear records of our processing activities and of the decisions we make concerning personal data (setting out our reasons for those decisions).

9. Individual Rights - "Your rights and your personal data "

Unless the data is subject to an exemption under the GDPR, you have rights with respect to your personal data.

Further information and advice about your rights can be obtained from the data protection regulator. See contact details below.

An outline of an individual's rights follows:

i) The right to be informed

You have the right to be provided with clear, transparent and easily understandable information about how we use your information and your rights. This is why we're providing you with the information in this Policy.

ii) The right of access

The right to request a copy of the personal data which Living Waters, Darnall holds about you (a Subject Access Request or 'SAR'). Also, the right to obtain access to your information (if we're processing it), and certain other information (similar to that provided in this Privacy Policy). This is so you're aware and can check that we're using your information in accordance with data protection law.

iii) The right to rectification

You are entitled to have your information corrected if it's inaccurate or incomplete.

iv) The right to erasure

This is also known as 'the right to be forgotten' and, in simple terms, enables you to request the deletion or removal of your information where there's no compelling reason for us to keep using it. This is not a general right to erasure; there are exceptions.

v) The right to restrict processing

You have rights to 'block' or suppress further use of your information. When processing is restricted, we can still store your information, but may not use it further. We keep lists of people who have asked for further use of their information to be 'blocked' to make sure the restriction is respected in future.

vi) The right to object to processing

You have the right to object to certain types of processing including processing for direct publicity and 'marketing' (i.e. If you no longer want to be contacted)

vii) The right to lodge a complaint

You have the right to lodge a complaint about the way we handle or process your personal data with the national data protection regulator.

viii) The right to withdraw consent

If you have given your consent to anything we do with your personal data, you have the right to withdraw your consent at any time (although if you do so it does not mean that anything we have done with your personal data with your consent up to that point is unlawful). This includes your right to withdraw consent to us using your personal data for publicity and 'marketing' purposes.

10. Further processing

If LWCF wishes to use an individual's personal data for a new purpose not covered by the Data Privacy Notice and this Data Protection Policy document, then we will provide them with a new notice explaining this new use prior to commencing the processing and setting out the relevant purposes and processing conditions. Where and whenever necessary we will seek an individual's prior consent to the new processing.

11. Data protection impact assessments

When LWCF is planning to carry out any data processing which is likely to result in a high risk we will carry out a Data Protection Impact Assessment (DPIA). These include situations when 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.

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

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

12. Dealing with data protection breaches

Where staff or volunteers or contractors working for us, think that this policy has not been followed, or data might have been breached or lost, this will be reported **immediately** to the Data Protection Officer, who will in turn immediately notify The Trustees collectively (the 'Data Controller) of the potential breach. LWCF will keep records of personal data breaches, even if we do not report them to the ICO.

The trustees will report all data breaches which are likely to result in a risk to any person, to the ICO. Reports will be made to the ICO within **72 hours** from when someone in the church becomes aware of the breach.

In situations where a personal data breach causes a high risk to any person, the trustees will (as well as reporting the breach to the ICO), 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.

13. Subject Access Requests (SARs)

Individuals can request information verbally or in writing. Such requests are SARs. To better police the LWCF system we should request that it in writing to the Operational Data Controller.

Individuals have the right to obtain:

- confirmation that you are processing their data; *
- access to their personal data; and
- other supplementary information – this largely corresponds to the information that you should provide in a privacy notice.

Individuals also have the right to:

- receive copy of the personal information that we hold;
- have personal data rectified if it is inaccurate or completed if it is incomplete;
- to be forgotten and can request the erasure of personal data when certain criteria are met;
- to block or restrict the processing of their personal data;
- to data portability allowing individuals to obtain and reuse their personal data for their own purposes across different services.

LWCF's response to SARs

Responses should be both timely and considered. In certain cases, it may be appropriate to refuse the request after considering all the circumstances.

Time Limit

- must provide the information without delay and at least within one calendar month of receiving it. This can be extended by a further two months for complex or numerous requests (in which case CBC must inform the individual and give an explanation). It is good practice to make a note on the record of whether the request or data is under dispute and why or the reason for the delay

- calculate the time limit from the day after receiving the request (whether the day after is a working day or not) until the corresponding calendar date in the next month. A calendar month ends on the corresponding date of the next month (e.g. 2 January to

2 February); unless that date does not exist in which case it is the last day of the next month (e.g. 31 January to 28 February).
If the corresponding date falls on a weekend or a public holiday, you have until the next working day to respond (e.g. receive a request on 30 March and the time limit starts from the next day (31 March). As there is no equivalent date in April, we have until 30 April to respond. However, if 30 April falls on a weekend, or is a public holiday, we have until the end of the next working day to respond).
This means that the legal deadline will vary from 28 days to 31 days depending on the month. For practical purposes if a consistent number of days is required (e.g. for a computer system), it may be helpful to adopt a 28-day period to ensure compliance as this is always within a calendar month.

Verification

Naturally under data security measures LWCF must verify the identity of the person making the request, using "reasonable means". If we have shared the personal data with other organisations (for example other controllers and processors) LWCF must inform them of the request where possible.

Response format

If the request is made electronically, you should provide the information in a commonly used electronic format.

14. Managing the personal information held

When processing personal data within the IT system LWCF needs to recognise the risks involved and take appropriate technical and organisational measures to secure the data.

LWCF should regularly review the information it processes or stores to identify when it needs to take action (e.g. correct inaccurate records). "Records" management policies, with rules for creating and keeping records (including emails) might help.

Conducting regular data quality reviews of systems and manual records LWCF holds will help to ensure the information continues to be adequate for the purposes it is processed for. The data quality checks to provide assurances on the accuracy of data inputted by staff and volunteers alike

Any data accuracy issues identified should be communicated as lessons learned to staff and volunteers through ongoing awareness campaigns and internal training

15. Contact Details

To exercise all relevant rights, queries of complaints please in the first instance contact the Operational Data Controller at livingwatersdarnall@outlook.com heading the email as “Data Protection Policy”

The Information Commissioners Office can be contacted:

Telephone: 0303 123 1113, or

Email https://ico.org.uk/global/contact-us/email/

or Postal mail or in person at:

The Information Commissioner's Office;

Wycliffe House,
Water Lane,
Wilmslow,
Cheshire.
SK9 5AF.

Schedule 1 – Definitions and useful terms

The following terms are used throughout this policy and have their legal meaning as set out within the GDPR. The GDPR definitions are further explained below:

Data controller

The data controller means 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.

However, if you are a controller, you are not relieved of your obligations where a processor is involved – the GDPR places further obligations on you to ensure your contracts with processors comply with the GDPR.

Data processors

Data processors include any 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. This definition will include the data processors' own staff (note that staff of data processors may also be data subjects).

This does not include LWCF staff or volunteers acting as such (data handlers/ inputters) and not as third parties in their own right as "suppliers" to LWCF.

If you are a processor, the GDPR places specific legal obligations on you; for example, you are required to maintain records of personal data and processing activities. You will have legal liability if you are responsible for a breach.

Data subjects

Data subjects include **all** living individuals who we hold or otherwise process personal data about. A data subject does not need to be a UK national or resident. All data subjects have legal rights in relation to their personal information. Data subjects that we are likely to hold personal data about include:

a. Our church members and the church congregation
b. People we care for and support
c. People who participate in our projects and events
d. Volunteers

e. Trustees
f. Tenants/Hirers
g. Consultants/individuals who are our contractors or employees working for them;
h. Advisers and representatives of other organisations
i. Donors/supporters
j. Enquirers
k. Friends and family
l. Complainants

ICO means the Information Commissioners Office.

This 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. Contact details are in clause 15 of the policy document.

Personal data

Personal data means any information relating to a natural person (living person) who is either identified or is identifiable. A natural person must be an individual and cannot be a company or a public body. Representatives of companies or public bodies would, however, be natural persons.

Personal data is limited to information about **living individuals** and does not cover deceased people.

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

Privacy Notice means the information given to data subjects which explains how we process their data and for what purposes.

Format

Hard Copy means in either paper, photocopy or other such media state.

Electronic Copy means in either computer, email, voicemail, Facebook, twitter or other such media format.

Processing

Processing is very widely defined and includes any activity that involves the data. It includes obtaining, recording or holding the data, or carrying out any operation or set of operations on the data 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 of clear, moving or stills images of living individuals is also a processing activity of Living Waters Christian Fellowship.

Special categories of data (as identified in the GDPR) include 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 GDPR does not apply to certain activities including processing covered by the Law Enforcement Directive, processing for national security purposes and processing carried out by individuals purely for personal/household activities.

Schedule 2 – Data Operational Hierarchy

1. Data Controller	Trustees have joint and several responsibilities A designated Trustee will act as the operational data controller representing the Trustees
2. Data Processor	These are EXTERNAL processors of our data. They will be nominated by team or activity leaders for appointment by the Trustees to the roles individually specified and overseen by operational data controller.
3. Team or Activity Leaders	Each team or activity leader is also to be considered for appointment as a lead processor/ data champion Have the data role of ensuring that none of the data relating to their sphere of activity is removed from the church premises without the proper signed authorisation of both the operational data controller.
4. Employees and Volunteers	Have the responsibility of applying due care and attention to their duties with regard to all data. Sensible consideration must be given for the requesting or supplying of data in respect of the degree of confidentiality invoked.

Schedule 3 – UK version GDPR Exemptions

What exemptions does the UK version of GDPR permit?

EU Article 23 enables Member States to introduce exemptions to the GDPR in certain situations.

Member States can introduce exemptions from the GDPR's transparency obligations and individual rights, but only where the restriction respects the essence of the individual's fundamental rights and freedoms and is a necessary and proportionate measure in a democratic society to safeguard:

- national security;
- defence;
- public security;
- the prevention, investigation, detection or prosecution of criminal offences;
- other important public interests, in particular economic or financial interests, including budgetary and taxation matters, public health and security;
- the protection of judicial independence and proceedings;
- breaches of ethics in regulated professions;
- monitoring, inspection or regulatory functions connected to the exercise of official authority regarding security, defence, other important public interests or crime/ethics prevention; the protection of the individual, or the rights and freedoms of others; or the enforcement of civil law matters.

The UK version of GDPR does not apply to certain activities including processing covered by the Law Enforcement Directive, processing for national security purposes and processing carried out by individuals purely for personal/household activities

What about other Member State derogations or exemptions?
(Derogation = An exemption from or relaxation of a rule of law)

Chapter IX provides that Member States can provide exemptions, derogations, conditions or rules in relation to specific processing activities.

These include processing that relates to:

- freedom of expression and freedom of information;
- public access to official documents;
- national identification numbers;
- processing of employee data;

- processing for archiving purposes and for scientific or historical research and statistical purposes;
- secrecy obligations; and
- **churches and religious associations**.