

Community Watchmen Ministries (CWM)

DATA PROTECTION POLICY 2026-2027

Revision Date: September 2026

Review Date: September 2027

Contents

	Page
1. Introduction	3
Context	3
Aims	3
Scope	4
2. Roles and Responsibilities	4
All personnel	4
Data Protection Lead (DPL)	4
CWM Data Controller	5
Leadership Team	5
3. Training and Guidance	5
4. CWM's Data Protection Responsibilities	6
What personal data do we process?	6
Making sure processing is fair and lawful	6
How can we legally use personal data?	6
What must we tell individuals before we use their data?	7
When we need consent to process data	7
Processing for specified purposes	7
Accurate data	7
Keeping and destroying data	7
Security of personal data	8
Keeping records of our data processing	8
5. Working with Data Subjects	8
Data subjects' rights	8
6. Managing Change & Risks	9
Data protection impact assessments (DPIAs)	9
Dealing with data protection breaches	9
Glossary of terms	11
Information Commissioners Office (ICO)	13
Registration	13
Contact Details	13
Additional Supporting Documents	13

1. Introduction

Context

Data protection at Community Watchmen Ministries (CWM) is about ensuring people can trust it to use their data fairly and responsibly. The UK data protection regime is set out in the Data (Use and Access) Act 2025 (DUAA 2025) and Data Protection Act 2018 (DPA 2018), along with the UK General Data Protection Regulation (UK GDPR) (which also forms part of UK law). It takes a flexible, risk-based approach which puts the onus on CWM to think about and justify how and why it uses data.

The Information Commissioners Office (ICO) regulates data protection in the UK. They offer advice and guidance, promote good practice, carry out audits, consider complaints, monitor compliance and take enforcement action where appropriate.

This Policy has been documented giving consideration to and in compliance with the following legislation and guidance:

Title	Body
DUAA 2025	UK Government
DPA 2018	UK Government
UK GDPR	UK Government
Guidance for organisations	ICO

Aims

The aim of this policy is to set out the governing principles that ensure CWM meets its obligations under the law and adopts good practice when processing personal data. In particular, it ensures that CWM will keep the following UK GDPR key principles at the heart of its approach to processing data:

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

It also ensures that CWM upholds the following rights of those whose data it processes:

- The right to be informed

- The right of access
- The right to rectification
- The right to erasure
- The right to restrict processing
- The right to data portability
- The right to object
- Rights in relation to automated decision making and profiling.

Scope

This policy applies to:

- all CWM staff/volunteers (personnel).
- all activities or ministries that operate under CWM.

This is not a legal document. It does not confer rights nor override any legal or statutory obligations.

2. Roles and Responsibilities

All personnel

All personnel are defined as volunteers, including the leadership team who work for Community Watchmen Ministries in any ministry or activity of the charity.

Before CWM personnel collect or handle any personal data as part of their work, it is important that they take the time to read this policy carefully and understand what is required of them, as well as the organisation's responsibilities when we process data.

All personnel are required to comply with this policy. If you think that you have accidentally breached the policy, it is important that you contact the CWM Data Protection Lead immediately so that we can take swift action to try to 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 as stated in CWM's Disciplinary Policy.

Data Protection Lead (DPL)

DPL act as the first point of contact regarding data protection issues for CWM. They manage requests and incidents regarding ministry data.

The DPL's role is to assist CWM to monitor internal compliance, inform and advise on its data protection obligations and act as a contact point for data subjects and the supervisory authority.

CWM must ensure that the DPL is involved, properly and in a timely manner, in all issues which relate to the protection of personal data.

CWM must support the DPL in performing their tasks by providing resources necessary to carry out those tasks and access to personal data and processing operations.

CWM must ensure that the DPL does not receive any instructions regarding the exercise of those tasks. They shall not be penalised by CWM for performing their tasks.

The DPL reports to the leadership team.

They liaise with and decide whether to pass on cases to ICO.

The DPL may fulfil other tasks and duties. CWM must ensure that any such tasks and duties do not result in a conflict of interests.

CWM Data Controller

The Data Controller is responsible for:

- assisting the DPL with their responsibilities under this policy.
- supporting CWM volunteers with their responsibilities under this policy, where appropriate.

Leadership Team

The Leadership Team are required to make sure that any procedures that involve personal data, which they are responsible for, follow the rules set out in this Data Protection Policy.

3. Training and Guidance

CWM will provide general training at the point of induction and thereafter at least two yearly for all personnel to raise awareness of their obligations and responsibilities, as well as to outline the law.

CWM may also issue procedures, guidance, or instructions from time to time.

The leadership team must set aside time to look together at the implications for their work.

4. CWM's Data Protection Responsibilities

What personal data do we process?

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 the person it is about, for example, where they complete forms or contact us.

We process personal data in both electronic and paper form and all this data is protected under data protection law. The personal data we process can include information such as names, contact details and banking details.

We **DO NOT** hold types of information that are called "special categories" of data stated in the UK GDPR 2018.

Making sure processing is fair and lawful

Processing of personal data will only be fair and lawful when there is a lawful basis for processing the data and when the processing is transparent. This means CWM will provide people with an explanation of how and why it processes their personal data at the point data is collected from them, as well as when data is collected about them from other sources.

How can we legally use personal data?

Processing of personal data is only lawful if one of these lawful bases, as listed in Article 6 of the UK GDPR, is met:

a) the processing is necessary for a contract with the data subject
b) the processing is necessary for us to comply with a legal obligation
c) the processing is necessary to protect someone's life (this is called "vital interests")
d) the processing is necessary for us to perform a task in the public interest, and the task has a clear basis in law
e) the processing is necessary for legitimate interests pursued by CWM 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 only be lawful if the data subject has given their clear consent

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

What must we tell individuals before we use their data?

If personal data is collected directly from the individual, CWM will inform them about its identity/contact details and those of the Data Protection Lead, the reasons for processing the data, explaining our legitimate interests, who the data will be shared with, how long the data will be stored and the data subjects' rights.

This information is commonly referred to as a 'Privacy Notice'.

This information will be given at the time when the personal data is collected.

When we need consent to process data

Where none of the other legal conditions apply to the processing, and we are required to get consent from the data subject, we will clearly set out what we are asking consent for, including why we are collecting the data and how we plan to use it. Consent will be specific to each process we are requesting 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.

Consent can, however, be withdrawn at any time and if withdrawn, the processing will stop. 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.

Processing for specified purposes

CWM will only process personal data for the specific purposes explained in its privacy notices or for other purposes specifically permitted by law. CWM will only collect and use personal data that is needed for those specific purposes. CWM will not collect more than is needed to achieve those purposes. CWM will not collect any personal data "just in case" it might be useful later.

Accurate data

We will make sure that personal data held is accurate and, where appropriate, kept up to date. The accuracy of personal data will be checked at the point of collection and at appropriate points later on.

Keeping and destroying data

We will not keep personal data longer than is necessary for the purposes that it was collected for. We will comply with official guidance issued about retention periods for specific records.

Information about how long we will keep records for can be found in our Data Retention Schedule.

Security of personal data

CWM 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.

The security measures implemented will 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 CWM will take into account the following, and anything else that is relevant:

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

Measures may include:

a) technical systems security
b) measures to restrict or minimise access to data
c) measures to ensure our 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 testing and evaluating of the effectiveness of security measures

Keeping records of our data processing

To show how we comply with article 30 of the UK GDPR, 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).

5. Working with Data Subjects

Data subjects' rights

CWM will process personal data in line with data subjects' rights, including their:

a) right of access - to ask CWM for copies of their personal information

b) right to rectification - to ask CWM to rectify or complete personal information they think is inaccurate or incomplete
c) right to erasure - to ask CWM to erase their personal information in certain circumstances
d) right to restriction of processing - to ask CWM to restrict the processing of their personal information in certain circumstances
e) right to object to processing - to object to the processing of their personal information in certain circumstances

We DO NOT share or transfer personal data to outside organisations under any circumstances.

If any CWM personnel receive any request from a data subject that relates or could relate to their data protection rights, this will be passed on to the CWM Data Protection Lead immediately.

CWM will act on all valid requests as soon as possible, and at the latest within one calendar month, unless there is reason to, and it is lawful to extend the timescale. This can be extended by up to two months in some circumstances.

6. Managing Change & Risks

Data protection impact assessments (DPIAs)

When we are planning to carry out any data processing which is likely to result in a high risk, we will carry out a 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.'

Dealing with data protection breaches

Where CWM personnel think that this policy has not been followed, or data might have been breached, this will be reported immediately to a Data Protection Lead.

CWM will keep records of personal data breaches, even if we do not report them to the ICO, this information with be kept secure.

CWM 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 CWM becomes aware of the breach.

In situations where a personal data breach causes a high risk to any person, we 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.

Glossary of terms

Data breach

A personal data breach is when a breach of security affects the confidentiality, integrity or availability of personal data. This could happen when personal data is accidentally or unlawfully:

- lost or destroyed;
- made unavailable;
- altered; or
- disclosed to or accessed by an unauthorised individual.

Data controller

The natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data. The charity, Community Watchmen Ministries, is data controller for ministries and activities that operate under this charity.

Data processing

Any operation which is performed on personal data, such as collecting, recording, using, storing, altering, disclosing or destroying.

Data processor

A natural or legal person, public authority, agency or other body which processes personal data on behalf of a controller. In doing so, they serve the controller's interests rather than their own.

Data Protection Act 2018 (DPA 2018)

The DPA 2018 sets out the framework for data protection law in the UK. It updates and replaces the Data Protection Act 1998, and came into effect on 25 May 2018. It sits alongside the UK GDPR.

Data protection impact assessment (DPIA)

A DPIA is a risk assessment that provides a way to systematically and comprehensively analyse data processing activities and helps identify and minimise data protection risks. It is a legal requirement in some circumstances.

Data Protection Lead (DPL)

CWM has a member of personnel designated as the DPL. They act as the first point of contact regarding data protection issues for CWM ministry. They manage requests and incidents regarding local data. They liaise with and decide whether to pass on cases to the ICO.

Data subject

The individual to whom the personal data relates.

CWM personnel

All personnel are defined as volunteers, including the leadership team who work for Community Watchmen Ministries in any ministry or activity of the charity.

UK General Data Protection Regulation (UK GDPR)

The UK GDPR sets out the key principles, rights and obligations for most processing of personal data and came into effect on 25 May 2018.

Information Commissioners Office (ICO)

The UK's independent supervisory authority set up to uphold information rights in the public interest, promoting openness by public bodies and data privacy for individuals. The ICO regulates data protection in the UK. They offer advice and guidance, promote good practice, carry out audits, consider complaints, monitor compliance and take enforcement action where appropriate.

Personal data

Any information relating to an identified or identifiable natural (living) person.

Special category data

Personal data that needs more protection because it is sensitive. This includes data about an individual's racial or ethnic origin; political opinions; religious or similar (e.g. philosophical) beliefs; trade union membership; health (including physical and mental health, and the provision of health care services); genetic data; biometric data; sexual life and sexual orientation.

Information Commissioners Office (ICO)

Registration

Organisation Name: Community Watchmen Ministries

Do not need to be registered as CWM do not have any paid employees.

Contact Details

Data Controller: Susan J Sinclair - Director of CWM

Data Protection Lead (DPL)

Name: Jackie Johnson

Email: [redacted] cwmprayer@me.com

Mobile No: [redacted]

Signed by or on behalf of the Leadership Team

Signature: 

Name: Susan J Sinclair

Designation: Director of CWM

Date of Signing:

12/9/26.

Additional Supporting Documents

Data Retention Schedule
Privacy Policy
Code of Conduct
Disciplinary Policy