DATA PROTECTION POLICY

Introduction

Protecting personal data is a fundamental human right. At Capernwray, we respect individuals' rights to control their personal information and ensure we meet all legal requirements for data protection.

The United Kingdom General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 (DPA) are the main laws we follow for handling personal data. We're also monitoring proposed changes, like the Data Protection and Digital Information Bill and the Data (Use and Access) Bill, which could update these rules and may lead to future updates to this policy.

Purpose of This Policy

This policy explains how Capernwray processes personal data belonging to its staff, students, guests, visitors, suppliers, and other third parties. It applies to all personal data Capernwray processes, regardless of format or storage medium.

Scope of This Policy

This policy applies to all Capernwray staff, including trustees, volunteers, ambassadors, and anyone else handling personal data on behalf of Capernwray.

Compliance with this policy is mandatory. Breaches may result in disciplinary action.

Our Data Protection Representative oversees this policy. If you have questions or concerns, contact them at **privacy@capernwray.org** or Ext. 8037

Key Data Protection Principles

Capernwray follows these key principles for processing personal data:

1. Process data lawfully, fairly, and transparently.
2. Collect data for specified, explicit, and legitimate purposes.
3. Ensure data is accurate and kept up to date.
4. Retain data only for as long as necessary.
5. Protect data using appropriate technical and organisational measures.
6. Transfer data outside the UK only when safeguards are in place.
7. Ensure people can use their rights over their personal data.

Lawfulness, fairness and transparency

Lawfulness and Fairness

Capernwray can only collect and use personal data for lawful reasons. Without a lawful reason, processing the data would be unfair and unlawful and could harm the individuals involved.

People should never be surprised to learn how Capernwray uses their personal data. Capernwray will always record and explain the lawful reason for each specific use of personal data.

We will only process personal data when at least one of the following lawful reasons applies:

1. Consent: The individual has given clear permission for a specific purpose.
2. Contract: The processing is necessary for a contract the individual is part of, such as an employment agreement or registration.
3. Legal Obligation: The processing is required to meet legal responsibilities.
4. Vital Interests: The processing is essential to protect someone's life.
5. Public Interest: The processing is needed to perform a task in the public interest.
6. Legitimate Interests: The processing is for Capernwray's legitimate purposes, as long as these don't override the individual's rights.

Consent as a Lawful Basis
Consent is one option for processing data, but it is not always the best choice. It is used when no other lawful reason fits the situation. To be valid, consent must:

- Be specific to a clear purpose.
- Be informed, with the person understanding what they are agreeing to.
- Be unambiguous, requiring an active choice (e.g., ticking a box or signing a form).
- Be separate from other agreements, like terms and conditions.
- Be freely given, with no pressure or imbalance of power between Capernwray and the individual.

People must be able to withdraw consent just as easily as they give it. If consent is needed for a new purpose not covered by the original consent, Capernwray will explain the new use and ask for consent again.

When Explicit Consent is Required
Explicit consent is required for certain situations, such as:

1. Using sensitive personal data (e.g., health, ethnicity, or religious beliefs).
2. Automated decision-making, like profiling that significantly affects an individual.
3. Transferring personal data outside the UK when no other legal reason applies**.**

Certain types of sensitive personal data are subject to additional protection under the GDPR. These are listed under Article 9 of the GDPR as "special categories" of personal data. The special categories are:

1. Racial or ethnic origin.
2. Political opinions.
3. Religious or philosophical beliefs.
4. Trade union membership.
5. Genetic or biometric data.

6. Health information.
7. Details about a person's sex life or sexual orientation.

Capernwray will usually rely on other legal reasons, like legitimate interest or public health requirements, instead of explicit consent for these categories.

How We Collect Data
Most of the personal data Capernwray uses comes directly from the forms people fill out, such as:

- Contact forms.
- Booking or registration forms.
- Event participation forms
- Content download or lead capture forms

When processing sensitive data, Capernwray may rely on:

1. Explicit Consent: When people clearly agree to the use of their data.
2. Public Interest: When necessary for public health or similar reasons.
3. Legal Obligations: To meet legal or employment responsibilities (e.g., ensuring safety or preventing discrimination).

Transparency
Capernwray is committed to being clear about how it collects and uses personal data. Any explanation we provide must be:

- Easy to find.
- Simple to understand.
- Written in plain language.

Capernwray's **Privacy Policy** explains how personal data is processed. All privacy notices must be reviewed by the Data Protection Representative to ensure they are up to date and accurate.

Purpose Limitation
Capernwray will only collect and use personal data for specific and clear purposes. If we need to use the data for a new purpose, we will inform the individual and, where required, ask for consent again.

Data Use for Staff
Capernwray collects personal data about staff primarily for:

- Recruitment, promotions, and training.
- Paying wages and calculating benefits, including pensions.
- Performance reviews and managing discipline.
- Meeting legal requirements, such as health and safety rules.

- Providing references for future employers or educational opportunities.

Examples of personal data Capernwray collects about staff include:

- Personal details, like name, address, and qualifications.
- Emergency contact information.
- Notes from meetings or appraisals.
- Salary, benefits, and bank details.
- Absence and sickness records.

Data Minimisation
Capernwray only collects data necessary for specific purposes. Staff must avoid collecting unnecessary information and ensure outdated or unnecessary data is securely deleted, destroyed or anonymised in line with Capernwray's Data Retention Policy.

Accuracy and Storage Limitation
Capernwray ensures that data is accurate, reviewed regularly, and kept up to date. If errors are identified, they are corrected or deleted. Data is retained only as long as needed for its purpose or legal requirements. See Capernwray's Data Retention Policy.

Security, Integrity, and Confidentiality

Security of personal data
Personal data is protected using appropriate technical and organisational measures. Staff must ensure:

1. Confidentiality: Only authorised individuals can access data.
2. Integrity: Data is accurate and used as intended.
3. Availability: Data is accessible to those who need it.

If enacted, the Cyber Security and Resilience Bill may require additional safeguards for critical systems and infrastructure.

Reporting Data Breaches
Any suspected data breach must be reported immediately to the Data Protection Representative Jayne Pugh (Director of Marketing & External Relations) to obtain advice and take all appropriate steps to preserve evidence relating to the breach.

If required, Capernwray will notify the ICO and affected individuals within legal timeframes.

Sharing Personal Data
You are not permitted to share personal data with third parties unless:

1. Capernwray has approved the data sharing in advance.
2. The data subject has been informed through a privacy notice or fair processing notice.

3. The third party is processing the data on Capernwray's behalf, and the following conditions are met:
    - Capernwray has conducted due diligence to ensure the third party complies with data protection laws.
    - A written agreement is in place with the third party, meeting the requirements of the UK GDPR, including obligations around confidentiality, security, and data use limitations.

Any unauthorised transfer of personal data would breach the principles of lawfulness, fairness, and transparency. If the breach involves a security failure, it may constitute a personal data breach.

Only share personal data with third parties or use online/cloud-based services for work-related purposes if you are sure all the above conditions are met. This includes verifying that Capernwray has approved any online service and complies with applicable data protection laws.

If you are unsure whether sharing personal data is appropriate, seek advice from the Data Protection Representative before proceeding.

Data Transfers Outside the UK
The UK GDPR restricts the transfer of personal data outside the UK or the European Economic Area (EEA) to ensure the data remains protected to the same standard. A 'transfer' includes sending, sharing, or accessing personal data in another country.

Personal data is only transferred outside the UK or EEA if one of the following conditions is met:

1. Adequate Protection: The country has been approved by the European Commission or the UK government as having strong data protection laws equivalent to those in the UK or EEA.
2. Appropriate Safeguards: Measures like binding corporate rules or standard contractual clauses are in place to ensure the data is protected.
3. Explicit Consent: The individual has been fully informed of any risks and has agreed to the transfer.
4. Necessary for a Contract: The transfer is needed to fulfil a contract with the individual (e.g., booking a retreat or holiday) or for steps requested by them before entering into a contract.
5. Public Interest or Vital Interests: The transfer is required for public interest, legal claims, or to protect someone's life when they cannot give consent.
6. Legitimate Interests: In limited cases, the transfer is essential for Capernwray's legitimate interests, provided it doesn't override the individual's rights.

Before any data is transferred outside the UK or EEA, you must ensure:

- One of the above conditions applies.

- Capernwray has approved the transfer.

If you're unsure whether a transfer meets these conditions, contact the Data Protection Representative for advice.

Data Subject Rights
Under the UK GDPR and related legislation, individuals (referred to as 'data subjects') have several rights regarding their personal data. These include:

1. Right to Withdraw Consent: If we are using consent as the basis for processing, individuals can withdraw it at any time, for any reason.
2. Right to Be Informed: Individuals must be told how their data is collected, used, and processed. Our privacy notices explain this.
3. Right of Access: Individuals can ask for a copy of their personal data and information about how we use it.
4. Right to Rectification: Individuals can request corrections to inaccurate data or additions to incomplete data.
5. Right to Erasure (Right to Be Forgotten): Individuals can ask us to delete their data if:
    - It's no longer needed.
    - They withdraw consent.
    - They object to processing.
    - The processing was unlawful.
    - The data must be deleted to meet a legal obligation.
    - The data was collected from a child under 13.
6. Right to Restrict Processing: Individuals can ask us to limit the use of their data if:
    - They believe it's inaccurate.
    - Processing is unlawful but they prefer restriction instead of deletion.
    - The data is no longer needed but must be kept for legal claims.
    - They object to processing while we assess their request.
7. Right to Data Portability: In some cases, individuals can ask for their data in a digital format that can be easily transferred to another organisation.
8. Right to Object: Individuals can object to processing if it is based on legitimate interests or performed for marketing purposes.
9. Right to Object to Automated Decisions: Individuals can object to decisions made entirely by automated systems that significantly impact them and can request human review.
10. Right to Be Notified of Data Breaches: If a breach risks their rights or freedoms, individuals must be informed promptly.
11. Right to Complain: If individuals are unhappy with how their data is handled, they can make a complaint to the Information Commissioner's Office (ICO) or another relevant authority.

How to Handle Requests

- When a data subject makes a request, verify their identity before acting.

- Be cautious of third parties attempting to access data without authorisation.
- Forward all requests to the Data Protection Representative immediately, even if you're unsure if it qualifies.
- Capernwray will usually respond to requests within one month.

Accessing Your Personal Data as an Employee
Employees have the right to access personal data held about them, but this right is exercised through a formal process. Employees cannot bypass the process and directly access their data. All requests must go through the designated channel to comply with data protection laws and safeguard confidentiality.

Here's how it works:

1. Formal Request Required: Employees must submit a Subject Access Request (SAR) to access their personal data. This ensures the organisation has a record of the request and can verify the employee's identity.
2. Verification: The organisation must confirm the identity of the employee making the request to prevent unauthorised access to data.
3. Response Time: Once the request is received, the organisation has one month to respond, although this can be extended by up to two months for complex or multiple requests.
4. Facilitated by a Designated Person: The organisation's Data Protection Representative or another authorised individual is responsible for managing and fulfilling SARs, ensuring the process is lawful and documented.

Fees
In most cases, requests are free. However, a reasonable fee may apply if the request is excessive or repetitive.

Research Exemption
Some data subject rights do not apply when personal data is used for research purposes, provided:

1. Technical and organisational safeguards (e.g., data minimisation or pseudonymisation) are in place.
2. Processing does not cause significant harm or distress to individuals.
3. The research does not involve decisions about individuals (unless ethically approved for medical purposes).
4. Following usual rights would prevent or seriously affect the research.

If these conditions are met, the following apply:

    - Data collected for other purposes can be used for research and kept indefinitely.
    - Individuals do not have the right to access or change data if research results will be anonymised.
    - Rights to rectification, erasure, restriction, and objection do not apply.

Accountability and Compliance

Capernwray is responsible for following data protection laws and must be able to prove it. This is called the accountability principle under the UK GDPR. To meet this responsibility, Capernwray ensures the following:

1. Appointing a Data Protection Representative:
    - Capernwray has a qualified Data Protection Representative who is given the resources and support needed to oversee compliance.
2. Building Data Protection into Processes:
    - When deciding how to use personal data, Capernwray applies technical and organisational safeguards to ensure compliance with data protection principles at every stage.
3. Limiting Data Use by Default:
   Capernwray ensures only the data that is absolutely necessary for a specific purpose is collected, stored, and accessed. This includes limiting:
    - The type and amount of data.
    - How long it's kept.
    - Who can access it.
4. Assessing and Managing Risks:
    - If a planned activity poses a high risk to individuals' rights (such as processing sensitive data), Capernwray carries out a Data Protection Impact Assessment (DPIA) to identify and reduce risks.
5. Embedding Data Protection into Documents and Policies:
    - Data protection requirements are integrated into Capernwray's internal documents, privacy notices, and fair processing notices.
6. Staff Training:
    - All staff members are trained regularly on data protection laws, Capernwray's policies, and best practices. Training completion is recorded for accountability.
7. Testing and Reviewing Safeguards:
    - Capernwray regularly checks its data protection measures to ensure they are effective and updates them as needed. This includes periodic reviews of policies, procedures, and technical systems.

Proposed legislation may require additional documentation and reporting for specific data uses.

Data Protection Impact Assessment (DPIA)

A Data Protection Impact Assessment (DPIA) is required for activities that are likely to pose high risks to individuals' personal data, such as using new technologies or large-scale processing.
A DPIA must:

1. Describe the purpose, nature, and scope of the processing.
2. Assess whether the processing is necessary and proportionate.
3. Identify risks to individuals.
4. Outline measures to reduce or remove those risks.

DPIAs must be reviewed and approved by the Data Protection Representative before proceeding.

Direct Marketing

Capernwray is committed to conducting direct marketing activities in compliance with the UK General Data Protection Regulation (UK GDPR) and the Privacy and Electronic Communications Regulations (PECR). We recognise that direct marketing encompasses any communication promoting our services, including emails, SMS, telephone calls, and postal mail.

Under the UK GDPR, we must have a valid lawful basis for processing personal data for direct marketing purposes. The two most applicable bases are:

1. **Consent:** We obtain explicit consent from individuals before sending direct marketing communications, ensuring that consent is freely given, specific, informed, and unambiguous.

2. **Legitimate Interests:** In certain circumstances, we may rely on legitimate interests as our lawful basis for processing personal data for direct marketing. This is permissible when our interests are not overridden by the individual's rights and freedoms. We conduct a Legitimate Interests Assessment (LIA) to ensure compliance.

Electronic Marketing Communications

For electronic marketing communications (e.g., email and SMS), Capernwray complies with the Privacy and Electronic Communications Regulations (PECR). We require prior consent for most marketing activities unless the 'soft opt-in' applies.

The **soft opt-in** allows Capernwray to send marketing messages about similar products or services to individuals who have previously engaged with us. This applies when:

1. We obtained the individual's contact details during the purchase or negotiation of a teaching course, holiday, retreat, event or taster session.
    - For example, if someone booked a holiday or attended a taster session, we may send them information about upcoming retreats or other relevant offers.
2. We provide a simple, free way to opt out of marketing**.**
    - At the time we collect their contact details, individuals are informed of their right to opt-out.
    - Every marketing message includes a clear and free method to unsubscribe, such as a link in emails or instructions for SMS messages.

Capernwray will never use the soft opt-in to market unrelated products or services. We respect individuals' preferences and will immediately stop sending marketing communications if they opt-out.

Right to Object
Individuals have the absolute right to object to direct marketing at any time. On receiving an objection, we will promptly cease processing personal data for direct marketing purposes.

Proposed Reforms
We are aware of proposed reforms that may affect consent requirements and the use of legitimate interests for marketing. We are committed to monitoring these developments and will update our policies and practices to ensure ongoing compliance.

Complaints Procedure

We take data protection complaints seriously. If you have concerns, contact the Data Protection Representative at privacy@capernwray.org.

If unresolved, complaints can be escalated to the Information Commissioner's Office (ICO) via their website or by calling 0303 123 1113.

Review Schedule

This policy is reviewed biennially or sooner if legal changes require updates.
Last Reviewed: November 2024
Next Review Due: November 2026

.