DATA PROTECTION POLICY

Introduction

The protection of individuals via the lawful, legitimate and responsible processing and use of their personal data is a fundamental human right. Individuals may have a varying degree of understanding or concern for the protection of their personal data, but Capernwray must respect their right to have control over their personal data and ensure it acts in full compliance with legislative and regulatory requirements at all times.

The General Data Protection Regulation ("**GDPR**"), as supplemented by the Data Protection Act 2018 ("**DPA**"), is the main piece of legislation that governs how Capernwray collects and processes personal data and protects employees against the misuse of personal data.

Purpose of this Policy

This Policy sets out how Capernwray will process the personal data of its staff, students, guests, visitors, suppliers and other third parties, and applies to all personal data that Capernwray processes, regardless of the format or media on which the data is stored.

Scope of this Policy

This Policy applies to all members of Capernwray staff (whether paid or not and includes trustees, voluntary workers and ambassadors and any other persons carrying out work on behalf of Capernwray which involves the handling of personal data) (hereafter "**you**" or "**your**").

You have a crucial role to play in ensuring that Capernwray maintains the trust and confidence of the individuals about whom Capernwray processes personal data (including its own staff), complying with Capernwray's legal obligations and protecting Capernwray's reputation. This Policy therefore sets out what Capernwray expects from you in this regard.

Compliance with this Policy is mandatory. Any breach of this Policy and any related policies and procedures may result in disciplinary action.

All members of staff must read, understand and comply with this Policy when processing personal data in the course of performing their tasks and must observe and comply with all controls, practices, protocols and training to ensure such compliance.

Our Data Protection Representative, Debbie Atkinson (Head of HR & Compliance) is responsible for overseeing the implementation and review of this Policy (and the related policies and procedures) and can be contacted as follows: privacy@capernwray.org Ext. 8007

If you do not feel confident in your knowledge or understanding of this Policy or you have any concerns, it is important that you raise this with your line manager or our Data Protection Representative as soon as possible.

The GDPR is based on a core set of principles that Capernwray must observe and comply with at all times from the moment that personal data is collected until the moment that personal data is archived, deleted or destroyed.

Capernwray must ensure that all personal data is:

1. processed lawfully, fairly and in a transparent manner;
2. collected only for specified, explicit and legitimate purposes;
3. accurate and where necessary kept up to date;
4. not kept in a form which permits identification of data subjects for longer than is necessary for the purposes for which the data is processed;
5. processed in a manner that ensures its security using appropriate technical and organisational measures to protect against unauthorised or unlawful processing and against accidental loss, destruction or damage.

Additionally Capernwray must ensure that:

1. personal data is not transferred outside of the EEA (which includes the use of any website or application that is hosted on servers located outside of EEA) to another country without appropriate safeguards being in place;
2. Capernwray allows data subjects to exercise their rights in relation to their personal data.

Capernwray is responsible for, and must be able to demonstrate compliance with, all of the above principles, as set out in more detail below.

Lawfulness, fairness and transparency

<u>Lawfulness and fairness</u>

In order to collect and process personal data for any specific purpose, Capernwray must always have a lawful basis for doing so. Without a lawful basis for processing, such processing will be unlawful and unfair and may also have an adverse impact on the affected data subjects. No data subject should be surprised to learn that their personal data has been collected, consulted, used or otherwise processed by Capernwray. Processing personal data will only be lawful where at least one of the following lawful bases applies:

1. The data subject has given their **consent** for one or more specific purposes;
2. The processing is necessary for the **performance of a contract** to which the data subject is a party (for instance a contract of employment or registration with Capernwray);
3. To comply with Capernwray's **legal obligations;**
4. To protect the **vital interests** of the data subject or another person (this will equate to a situation where the processing is necessary to protect the individual's life);
5. To perform tasks carried out in the public interest or the exercise of official authority;
6. To pursue Capernwray's **legitimate interests** where those interests are not outweighed by the interests and rights of data subjects.

Capernwray must identify and document the lawful basis relied upon by it in relation to the processing of personal data for each specific purpose or group of related purposes.

Consent as a lawful basis for processing

There is no hierarchy between the lawful bases for processing above, of which a data subject's consent is only one. Consent may not be the most appropriate lawful basis depending on the circumstances.

In order for a data subject's consent to be valid and provide a lawful basis for processing, it must be:

- specific (not given in respect of multiple unrelated purposes);
- informed (explained in plain and accessible language);
- unambiguous and given by a clear affirmative action (meaning opt-in: silence, inactivity or pre-ticked boxes will not be sufficient);
- separate and unbundled from any other terms and conditions provided to the data subject;
- freely and genuinely given (there must not be any imbalance in the relationship between Capernwray and the data subject and consent must not be a condition for the provision of any product or service).

A data subject must be able to withdraw their consent as easily as they gave it.

Once consent has been given, it will need to be updated where Capernwray wishes to process the personal data for a new purpose that is not compatible with the original purpose for which they were collected.

Unless Capernwray is able to rely on another lawful basis for processing, a higher standard of explicit consent (where there can be no doubt that consent has been obtained, for example a signed document or a Yes/No option accompanied by clear consent wording) will usually be required to process special categories of personal data, for automated decision-making and for transferring personal data outside of the EEA.

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. Personal data revealing racial or ethnic origin;
2. Political opinions;
3. Religious or philosophical beliefs;
4. Trade union membership;
5. Genetic data and biometric data processed for the purpose of uniquely identifying a natural person;
6. Data concerning health;
7. Data concerning a natural person's sex life or sexual orientation.

Where Capernwray needs to process **special categories of personal data**, it will generally rely on another lawful basis that does not require explicit consent.

The vast majority of the information Capernwray holds is obtained directly from our forms that students, guests or visitors have filled in (such as contact forms, booking forms, registration forms and events forms).

To the extent we process **special categories of personal data**, in addition to pursuing our legitimate interest in fulfilling the purposes set out below, we have obtained the data subject's explicit consent, or it may be necessary for reasons of public interest in the area of public health:

- Communicating with students, guests, alumni, and current and potential supporters with updates and news;
- Providing benefits and services to students, guests, alumni and supporters;
- Furthering our charitable mission (which includes fundraising and securing the support of volunteers);
- Enabling us to achieve our strategic and operational goals;
- To help support the NHS Test and Trace service by holding personal information for individuals who have accessed, visited or used Capernwray facilities or events.

The most appropriate condition for employment purposes is that the processing is necessary to enable Capernwray to meet its legal obligations (for example, to ensure health and safety or to avoid unlawful discrimination).

Transparency

Capernwray is required to ensure that any information provided by Capernwray to data subjects about how their personal data will be processed is concise, easily accessible, easy to understand and written in plain language. Where Capernwray has not been transparent about how it processes personal data, this will call the lawfulness and fairness of the processing into question.

Capernwray can demonstrate transparency through its Privacy Policy.

All privacy notices and fair processing notices should be reviewed by our Data Protection Representative, Debbie Atkinson (Head of HR & Compliance).

Purpose Limitation

Capernwray must only collect and process personal data for specified, explicit and legitimate purposes that have been communicated to data subjects **before** the personal data has been collected.

Capernwray must ensure that it does not process any personal data obtained for one or more specific purposes for a new purpose that is not compatible with the original purpose. Where Capernwray intends to do so, it must inform the data subjects **before** using their personal data for the new purpose and, where the lawful basis relied upon for the original purpose was consent, obtain such consent again.

Personal Data held in relation to staff

Personal data relating to Capernwray staff may be collected primarily for the purposes of:

- recruitment, promotion, training, redeployment and/or career development;
- administration and payment of wages;
- calculation of certain benefits including pensions;
- disciplinary or performance management purposes;
- performance review;
- recording of communication with employees and their representatives;

- compliance with legislation;
- provision of references to financial institutions, to facilitate entry onto educational courses and/or to assist future potential employers; and
- staffing levels and career planning.

Capernwray considers that the following personal data falls within the categories set out above:

- personal details including name, address, age, status and qualifications. Where specific monitoring systems are in place, ethnic origin and nationality will also be deemed as relevant;
- references and CVs;
- emergency contact details;
- notes on discussions between management and the employee;
- appraisals and documents relating to grievance, discipline, promotion, demotion or termination of employment;
- training records;
- salary, benefits and bank/building society details; and
- absence and sickness information.

Data minimisation

The personal data that Capernwray collects and processes must be adequate, relevant and limited to what is necessary in relation to the purposes for which it is to be processed.

You must only process personal data when necessary for the performance of your duties and tasks and not for any other purposes. Accessing personal data that you are not authorised to access, or that you have no reason to access, may result in disciplinary action and in certain circumstances, may constitute a criminal offence.

You may only collect personal data as required for the performance of your duties and tasks and should not ask a data subject to provide more personal data than is strictly necessary for the intended purposes.

You must ensure that when personal data is no longer needed for the specific purposes for which they were collected, that such personal data is deleted, destroyed or anonymised.
You must observe and comply with Capernwray's Data Retention Policy.

Accuracy

The personal data that Capernwray collects and processes must be accurate and, where necessary, kept up-to-date and must be corrected or deleted without delay when Capernwray discovers, or is notified, that the data is inaccurate.

You must ensure that you update all relevant records if you become aware that any personal data is inaccurate. Where appropriate, any inaccurate or out-of-date records should be deleted or destroyed.

In order to ensure Capernwray's files are accurate and up to date, and so that Capernwray is able to contact you or, in the case of an emergency, another designated person, you must notify Capernwray as soon as possible of any change in your personal details (e.g., change of name, address; telephone number; loss of driving licence where relevant; next of kin details, etc.). These records will be stored in your personnel file.

Storage limitation

The personal data that Capernwray collects and processes must not be kept in a form that identifies a data subject for longer than is necessary in relation to the purposes for which it was collected (except in order to comply with any legal, accounting or reporting requirements).

You must regularly review any personal data processed by you in the performance of your duties and tasks to assess whether the purposes for which the data were collected have expired. Where appropriate, you must take all reasonable steps to delete or destroy any personal data that Capernwray no longer requires in accordance with Capernwray's Data Retention Policy.

Security, integrity and confidentiality

Security of personal data

The personal data that Capernwray collects and processes must be secured by appropriate technical and organisational measures against accidental loss, destruction or damage, and against unauthorised or unlawful processing.

You are responsible for ensuring the security of the personal data processed by you in the performance of your duties and tasks. You must ensure that you follow all procedures that Capernwray has put in place to maintain the security of personal data from collection to destruction.

You must ensure that the confidentiality, integrity and availability of personal data are maintained at all times:

Confidentiality: means that only people who need to know and are authorised to process any personal data can access it;

Integrity: means that personal data must be accurate and suitable for the intended purposes;

Availability: means that those who need to access the personal data for authorised purposes are able to do so.

You must not attempt to circumvent any administrative, physical or technical measures Capernwray has implemented as doing so may result in disciplinary action and in certain circumstances, may constitute a criminal offence.

Reporting personal data breaches

In certain circumstances, the GDPR will require Capernwray to notify the Information Commissioner's Office (ICO), and potentially data subjects, of any personal data breach.

If you know or suspect that a personal data breach has occurred, you must contact the Data Protection Representative, Debbie Atkinson (Head of HR & Compliance) and the IT/AV Systems Coordinator, Heather Tallents, if relevant, immediately to report it and obtain advice, and take all appropriate steps to preserve evidence relating to the breach.

Sharing personal data

You are not permitted to share personal data with third parties unless Capernwray has agreed to this in advance, this has been communicated to the data subject in a privacy notice or fair

processing notice beforehand and, where such third party is processing the personal data on our behalf, Capernwray has undertaken appropriate due diligence of such processor and entered into an agreement with the processor that complies with the GDPR's requirements for such agreements.

The transfer of any personal data to an unauthorised third party would constitute a breach of the lawfulness, fairness and transparency principle and, where caused by a security breach, would constitute a personal data breach. Do not share any personal data with third parties, including the use of freely available online and cloud services for work-related purposes, unless you are certain that the conditions outlined above apply.

Seek advice from the Data Protection Representative or the IT/AV Systems Coordinator, if you are unsure.

Transfers outside of the European Economic Area (EEA)

The GDPR prohibits the transfer of personal data outside of the EEA in most circumstances in order to ensure that personal data are not transferred to a country that does not provide the same level of protection for the rights of data subjects. In this context, a "transfer" of personal data includes transmitting, sending, viewing or accessing personal data in or to a different country.

Capernwray may only transfer personal data outside of the EEA if one of the following conditions applies:

- the European Commission has issued an "adequacy decision" confirming that the country to which we propose transferring the personal data ensures an adequate level of protection for the rights and freedoms of data subjects (this applies to only a small number of countries);
- appropriate safeguards are in place, such as binding corporate rules, standard contractual clauses that have been approved by the European Commission;
- the data subject has given their explicit consent to the proposed transfer, having been fully informed of any potential risks;
- the transfer is necessary in order to perform a contract between Capernwray and a data subject, for reasons of public interest, to establish, exercise or defend legal claims or to protect the vital interests of the data subject in circumstances where the data subject is incapable of giving consent;
- the transfer is necessary, in limited circumstances, for Capernwray's legitimate interests.

You must ensure that you do not transfer any personal data outside of the EEA except in the circumstances set out above and provided that Capernwray has agreed to this in advance.

Data subject rights and requests

The GDPR provides data subjects with a number of rights in relation to their personal data. These include:

- **Right to withdraw consent:** where the lawful basis relied upon by Capernwray is the data subject's consent, the right to withdraw such consent at any time without having to explain why;
- **Right to be informed:** the right to be provided with certain information about how we collect and process the data subject's personal data (see Transparency above);

- **Right of subject access:** the right to receive a copy of the personal data that we hold, including certain information about how Capernwray has processed the data subject's personal data;
- **Right to rectification:** the right to have inaccurate personal data corrected or incomplete dated completed;
- **Right to erasure (right to be forgotten):** the right to ask Capernwray to delete or destroy the data subject's personal data if: the personal data are no longer necessary in relation to the purposes for which they were collected; the data subject has withdrawn their consent (where relevant); the data subject has objected to the processing; the processing was unlawful; the personal data have to be deleted to comply with a legal obligation; the personal data were collected from a data subject under the age of 13, and they have reached the age of 13;
- **Right to restrict processing:** the right to ask Capernwray to restrict processing if: the data subject believes the personal data are inaccurate; the processing was unlawful and the data subject prefers restriction of processing over erasure; the personal data are no longer necessary in relation to the purposes for which they were collected but they are required to establish, exercise or defend a legal claim; the data subject has objected to the processing pending confirmation of whether Capernwray's legitimate interests grounds for processing override those of the data subject;
- **Right to data portability:** in limited circumstances, the right to receive or ask Capernwray to transfer to a third party, a copy of the data subject's personal data in a structured, commonly-used machine-readable format;
- **Right to object:** the right to object to processing where the lawful basis for processing communicated to the data subject was Capernwray's legitimate interests and the data subject contests those interests;
- **Right to object to direct marketing:** the right to request that we do not process the data subject's personal data for direct marketing purposes;
- **Right to object to decisions based solely on automated processing (including profiling):** the right to object to decisions creating legal effects or significantly affecting the data subject which were made solely by automated means, including profiling, and the right to request human intervention;
- **Right to be notified of a personal data breach:** the right to be notified of a personal data breach which is likely to result in a high risk to the data subject's rights or freedoms;
- **Right to complain:** the right to make a complaint to the ICO or another appropriate supervisory authority.

You must be able to identify when a request has been made and must verify the identity of the individual making a request before complying with it. You should be wary of third parties deceiving you into providing personal data relating to a data subject without their authorisation.

You must immediately forward any request made by a data subject (even if you are uncertain whether it represents a request as set out above) to the Data Protection Representative. Capernwray will only have one month to respond in most circumstances.

As an employee you have the right to access personal data held about you.

In certain circumstances Capernwray may be entitled to charge a reasonable administration fee for subject access requests.

<u>Research exemption</u>

Some of the rules outlined above do not apply when personal data is being used for research purposes due to an exemption contained in the GDPR and DPA 2018. This exemption applies if the following conditions are met:

a. appropriate technical and organisational safeguards exist to protect the personal data e.g. data minimisation, pseudonymisation, or access controls;
b. there is no likelihood of substantial damage or distress to the data subjects from the data processing;
c. the research will not lead to measures or decisions being taken about individuals (except for ethically approved interventional medical purposes);
d. compliance with the requirements that the exemption negates would prevent or seriously impair the research purpose.

If these conditions apply then the following rules can be applied:

a. personal data originally collected for other purposes can be used for the research and can be kept indefinitely;
b. the right of individuals to access their personal data does not apply if the research results will be made public in a form that does not identify them;
c. the rights of rectification, erasure, restriction and objection do not apply.

Accountability and record-keeping

Capernwray is responsible for and must be able to demonstrate compliance with the data protection principles and Capernwray's other obligations under the GDPR. This is known as the 'accountability principle'.

Capernwray must ensure that it has adequate resources, systems and processes in place to demonstrate compliance with Capernwray's obligations including:

- appointing a suitably qualified and experienced Data Protection Representative and providing them with adequate support and resource;
- ensuring that at the time of deciding how Capernwray will process personal data, and throughout its processing, implementing appropriate technical and organisational measures that are designed to ensure compliance with the data protection principles;
- ensuring that, by default, only personal data that is necessary for each specific purpose are processed both in relation to the nature, extent and volume of such personal data, the period of storage and the accessibility of the personal data;
- ensuring that where any intended processing presents a high risk to the rights and freedoms of data subjects, Capernwray has carried out an assessment of those risks and is taking steps to mitigate those risks;
- integrating data protection into Capernwray's internal documents, privacy policies and fair processing notices;
- regularly training Capernwray's staff on the GDPR, this policy and Capernwray's related policies and procedures, and maintaining a record of training completion by members of staff;
- regularly testing the measures implemented by Capernwray and conducting periodic reviews to assess the adequacy and effectiveness of this policy, and Capernwray's related policies and procedures.

Capernwray must keep full and accurate records of all its processing activities in accordance with the GDPR's requirements.

You must ensure that you have undertaken the necessary training provided by Capernwray and, where you are responsible for other members of staff, that they have done so.

You must further review all the systems and processes under your control to ensure that they are adequate and effective for the purposes of facilitating compliance with Capernwray's obligations under this Policy.

Data Protection Impact Assessment

A Data Protection Impact Assessment (DPIA), also known as a Privacy Impact Assessment, is a process to help identify and minimise the data protection risks involved in projects, processes and activities involving the processing of personal data. DPIAs are required for processing likely to result in high risk to the individuals and their personal data, and where new technologies are involved.

A DPIA must:

- describe the nature, scope, context and purposes of the processing;
- assess necessity, proportionality and compliance measures;
- identify and assess risks to individuals;
- identify any additional measures to mitigate those risks.

DPIAs need to be assessed and signed off by the Data Protection Representative.

Direct Marketing

There are specific rules in relation to direct marketing by email, fax, SMS or telephone.

Capernwray must ensure that it has appropriate consent from individuals to send them direct marketing communications, and that when a data subject exercises their right to object to direct marketing it has honoured such requests promptly.

You must ensure that you consult with our Data Protection Representative before embarking upon any direct marketing campaign.

How to make a complaint

We endeavour to meet the highest standards when collecting and using personal information. For this reason, we take any complaints we receive about this very seriously and encourage individuals to bring it to our attention if they think that our collection or use of information is unfair, misleading or inappropriate, and welcome any suggestions for improving our procedures.

To exercise all relevant rights, queries or complaints please in the first instance contact our Data Protection Representative, Debbie Atkinson, at privacy@capernwray.org

If this does not resolve your complaint to your satisfaction, you have the right to lodge a complaint with the Information Commissioner's Office on 03031231113 or via email or at the Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF, England.

This Policy was last updated on 9 October 2020