Destiny House International and DHI Education and Arts

Data Protection Policy

Contents

Data Protection Policy and Procedure

1. Policy and Purpose

Destiny House International CIO, referred to as 'the Church, ' recognises that we will process personal data about you and the need to manage this data appropriately and in line with current legislation. This policy covers the processing of your personal data held in manual and electronic records during your employment and/or association with the Church.

As well as current employees, this policy applies to the personal data of job applicants, former employees, apprentices, volunteers, placement students, service users, workers and self-employed contractors. These are referred to in this policy as relevant individuals.

It also covers the Church's response to any data breach and other rights under the General Data Protection Regulation and the current Data Protection Act.

2. Definitions

- "**Personal data**" is information that relates to an identifiable person who can be directly or indirectly identified from that information, for example, a person's name, identification number, location, or online identifier. It can also include pseudonymised data.
- "**Special categories of personal data**" is data which relates to an individual's health, sex life, sexual orientation, race, ethnic origin, political opinion, religion, and trade union membership. It also includes genetic and biometric data (where used for ID purposes).
- "**Data subject**" means the individual to whom the personal information relates;
- "**Criminal offence data**" is data which relates to an individual's criminal convictions and offences.
- "**Data breach**" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal information.
- "**Data processing**" is any operation or set of operations which is performed on personal data or sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

The Church commits to ensuring that personal data, including special categories of personal data and criminal offence data (where appropriate), is processed in line with GDPR and domestic laws and that all its employees and associates conduct themselves in line with this and other related policies.

Where 3rd parties process data on behalf of the Church, the Church will ensure that the 3rd party takes such measures in order to maintain The Church's commitment to protecting data.

In line with current data protection legislation, the Church understands that it will be accountable for processing, managing, regulating, storing, and retaining all personal data held in the form of manual records and on computers.

3. Principles

The Church will comply with the following principles when processing personal information:

- to process personal information lawfully, fairly and in a transparent manner
- to collect personal information for specified, explicit and legitimate purposes only and will not process it in a way that is incompatible with those legitimate purposes
- to only process the personal information that is adequate, relevant and necessary for the relevant purposes
- to keep accurate and up-to-date personal information and take reasonable steps to ensure that inaccurate personal information is deleted or corrected without delay
- to keep personal information for no longer than is necessary for the purposes for which the information is processed
- to take appropriate technical and organisational measures to ensure that personal information is kept secure and protected against unauthorised or unlawful processing and against accidental loss, destruction or damage
- to comply with the relevant data protection procedures for the international transferring of personal data

In addition, you have the following individual data protection rights in relation to your personal data:

- the right to be informed about how, why and on what basis information is processed

- the right of access, through a subject access request
- the right for rectification, i.e. in respect of any inaccuracies or incomplete data
- the right to have information deleted (erasure) if it is no longer necessary for the purpose for which it was originally collected/processed or if there is no overriding legitimate grounds for the processing
- the right to restrict the processing of the data if certain criteria are met
- the right to data portability
- the right to object to the inclusion of any information
- the right to regulate any automated decision-making and profiling of personal data.

4. Types of data held

Personal data is kept in secure personnel files or within the Church's secure systems. Access permissions are kept to those individuals with legitimate organisational needs.

Relevant individuals should refer to the Church's privacy notice for more information on what data is processed, the reasons for its processing activities during your employment and the lawful basis it relies on for the processing.

We will never retain your data for any longer than is necessary for the purposes we need to use it or as specified by law.

5. Procedure

The Church has taken the following steps to protect the personal data of relevant individuals which it holds or to which it has access:

- It appoints employees with specific responsibilities for:
    a. the processing and controlling of data
    b. the comprehensive reviewing and auditing of its data protection systems and procedures
    c. overviewing the effectiveness and integrity of all the data that must be protected.

  There are clear lines of responsibility and accountability for these different roles.
- It provides information to you on your data protection rights, how it uses your personal data, and how it protects it. The information includes the actions relevant individuals can take if they think that their data has been compromised in any way

- it provides you with information and training to make you aware of the importance of protecting personal data, teaches you how to do this, and understand how to treat the information confidentially
- it can account for all personal data it holds, where it comes from, who it is shared with and also who it might be shared with
- it carries out risk assessments as part of its review activities to identify any vulnerabilities in its personal data handling and processing and to take measures to reduce the risks of mishandling and potential data security breaches. The procedure includes an assessment of the impact of both the use and potential misuse of personal data in and by the Church. It recognises the importance of seeking individuals' consent for obtaining, recording, using, sharing, storing and retaining their personal data and regularly reviews its procedures, including the audit trails that are needed and followed for all consent decisions. The Church understands that consent must be freely given, specific, informed and unambiguous. The Church will seek consent on a specific and individual basis where appropriate. Full information will be given regarding the activities about which consent is sought. Relevant individuals have the absolute and unimpeded right to withdraw that consent at any time
- it has the appropriate mechanisms for detecting, reporting and investigating suspected or actual personal data breaches, including security breaches. It is aware of its duty to report significant breaches that cause significant harm to the affected individuals to the Information Commissioner and is aware of the possible consequences
- it is aware of the implications of international transfer of personal data internationally.

6. Access to data

Relevant individuals have a right to be informed whether the Church processes personal data relating to them and to access the data that the Church holds about them. Requests for access to this data will be actioned under the following summary guidelines:

- A written request is made of your subject access request. The request should include as much information as you can about what information you need, the timeline you need the information for and the reason for the request. The request should be sent to the Data Controller.
- The Church will not charge for the data supply unless the request is manifestly unfounded, excessive, or repetitive or if a request is made for duplicate copies to be provided to parties other than the employee making the request.

- The Church will respond to a request without delay. Access to data will be provided, subject to legally permitted exemptions, within one month at a maximum. This may be extended by a further two months when requests are complex or numerous.

Relevant individuals must inform the Church immediately if they believe that the data is inaccurate, either as a result of a subject access request or otherwise. The Church will take immediate steps to rectify the information.

For further information on making a subject access request, contact the *Data Controller.*

7. Data Disclosures

The Church may be required to disclose certain data/information to any person. The circumstances leading to such disclosures include:

- any benefit you receive as operated by third parties
- disabled individuals - whether any reasonable adjustments are required to assist them at work
- individuals' health data - to comply with health and safety or occupational health obligations towards you
- for Statutory Sick Pay purposes
- HR management and administration - to consider how your health affects your ability to do your job
- the smooth operation of any employee insurance policies or pension plans.

These kinds of disclosures will only be made when strictly necessary for the purpose.

8. Security of Data

The Church uses appropriate technical and organisational measures to maintain the security of data that is stored and transported.

In addition, you must:

- ensure that all files or written information of a confidential nature are stored in a secure manner and are only accessed by people who need to and have a right to access them

- ensure that all files or written information of a confidential nature are kept secure and not left where they can be read by unauthorised people
- not send emails containing sensitive work-related information to their personal email address
- ensure the accuracy of data entered into the systems or documents
- always use the passwords provided to access the computer system and not share them with others who should not have them
- use computer screen blanking to ensure that personal data is not left on the screen for people to view when not in use

- Personal data relating to you or your colleagues should not be kept or transported on laptops, USB sticks, or similar devices unless authorised ensuring that data is recorded on such devices only where necessary

Where personal data is recorded on any such device, it should be protected by:

- using an encrypted system
- ensuring that laptops or USB drives are not left where they can be stolen

Failure to follow the Church rules on data security may be dealt with via the Church's disciplinary procedure. Appropriate sanctions include dismissal with or without notice, dependent on the severity of the failure.

9. Breach notification

Where a data breach is likely to result in a risk to the rights and freedoms of individuals, it will be reported to the Information Commissioner without undue delay and within 72 hours of the Church becoming aware of it. It may be reported in more than one instalment.

Individuals will be informed directly in the event that the breach is likely to result in a high risk to the rights and freedoms of that individual.

If the breach is sufficient to warrant notification to the public, the Church will do so without undue delay.

10. Training

Individuals must read and understand the policies on data protection as part of their induction. In addition, you will receive training covering basic information about confidentiality, data protection and the actions to take upon identifying a potential data breach.

The nominated data protection officers for the Church are trained appropriately in their roles under data protection legislation.

If you need to use the computer system, you will be trained to protect individuals' personal data, to ensure data security, and to understand the consequences to you, as individuals, and the Church of any potential lapses and breaches of the Church's policies and procedures.

11. Non-compliance

We take compliance with this policy very seriously. Failure to comply with the policy puts at risk the individuals whose personal information is being processed and carries the risk of significant civil and criminal sanctions for the individual. Because of the importance of this policy, if you fail to comply with any requirements, it may lead to disciplinary action under our procedures.

12. Records

The Church keeps records of its processing activities, including the purpose for the processing and retention periods in its data record. These records will be kept up to date so that they reflect current processing activities.

13. Data Controller

The Church's Data controller is *Evey Jean-Marie*
can be contacted at *[]*.

I have read and understood this policy and agree to abide by its terms:

Name: _____

Signed: _____

Date: _____

Approved by:	DHI CIO Board of Trustees
Last reviewed on:	September 2022