UNION THEOLOGICAL COLLEGE

DATA PROTECTION POLICY

1.0 Introduction

Union Theological College needs to gather and use certain information about individuals. This can include information about:

- Students
- Applicants
- Licentiates
- Accredited Preachers
- Alumni
- Staff
- Adjunct Faculty
- External Examiners
- Event attendees
- Library members
- Residents
- Members of the governance structure (including committee and panel members)
- Suppliers
- Residents of the Gibson Chambers
- Business contacts, and
- Other people we have a relationship with or may need to contact

This policy describes how this personal data must be collected, handled and stored to meet data protection standards and to comply with the law. It should be read in conjunction with the Data Protection Policy of the Presbyterian Church in Ireland.

2.0 Why this Policy Exists

This Data Protection Policy ensures that we:

- Comply with data protection law and follow good practice.
- Protect the rights of individuals.
- Are open about how we store and process individuals' data.
- Protect ourselves from the risk of a data breach.

3.0 Data Protection Law

The General Data Protection Regulation (EU 2016/679) (GDPR) and the Data Protection Act 2018 regulate how organisations collect, handle and store personal information.

These rules apply regardless of whether data is stored electronically, on paper or on other materials. To comply with the law, personal information must be collected and

used fairly, stored and disposed of safely, and not disclosed unlawfully. The GDPR is underpinned by six important principles. These say that personal data shall be:

1. Processed lawfully, fairly and in a transparent manner in relation to individuals.
2. Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposed or statistical purposes shall not be considered to be incompatible with the initial purposes.
3. Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.
4. Accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.
5. Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals.
6. Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

4.0 Policy Scope

This policy applies to any individual processing personal data on behalf of Union Theological College, including all PCI employees, part-time and agency staff.

It applies to all data that the College holds relating to identifiable individuals. This can include for example:

- Names of individuals, postal/email addresses, telephone numbers, bank details
- Sensitive personal data such as information in relation to physical or mental health conditions, religious beliefs or ethnic origin.

5.0 Data Protection Risks

This policy helps to protect the College from some very real data security risks, including:

- Breaches of confidentiality – for instance, information being given out inappropriately about our students or staff.
- Failing to offer choice when seeking consent as our legal basis for processing – for instance, all individuals should be free to choose how we use data relating to them.
- Reputational damage – for example, the College could suffer if hackers or cyber thieves successfully gained access to personal data.

6.0 Responsibilities

Everyone who works for or with the College has some responsibility for ensuring personal data is collected, stored and handled appropriately.

Everyone who works for or on behalf of Union Theological College is required to respect the confidentiality of personal data, to take all reasonable measures to ensure its security while in their position, and to return or securely destroy/delete personal data held on Union Theological College's behalf when they leave their position.

Everyone who handles personal data must ensure that it is handled and processed in line with this policy and data protection principles. Failure to comply with the data protection policy and principles is a serious offence and in the case of staff could result in disciplinary action.

In any situation which requires the development of a new system or where personal data is going to be processed in a different way to previously then the need for a Data Protection Impact Assessment (DPIA) will need to be considered. In such circumstances this must be referred to the Data Protection Coordinator.

The following have key areas of responsibility:

- The Management Committee is ultimately responsible for ensuring that the College meets its legal obligations

- The Faculty is responsible for ensuring that the Management Committee is kept apprised of any issues relating to data protection

- The Data Protection Coordinator is responsible for:
    - Keeping Faculty updated about data protection responsibilities, risks and issues
    - Reviewing all data protection procedures and related policies, in line with an agreed schedule
    - Arranging data protection training and advice for any individual processing personal data on behalf of Union Theological College
    - Dealing with requests from individuals to see the data the College holds about them (subject access requests)
    - Checking and approving any contracts or agreements with third parties that may process personal data on behalf of Union Theological College
    - Ensuring that any marketing initiatives comply with data protection principles

- Liaising with the PCI IT Manager to ensuring that all systems, services and equipment meet acceptable security standards.

7.0 General College Staff Guidelines

1. The only people able to access data covered by this policy should be those who need it for their work.
2. Data should not be shared informally.
3. The College will provide guidance to any individual processing personal data on behalf of Union Theological College to help them understand their responsibilities when handling data.
4. Data must be kept secure by taking sensible precautions and following the guidelines below.
5. Strong passwords must be used and changed regularly – they should never be shared.
6. Personal data should not be disclosed to unauthorised people, either internally or externally.
7. When receiving telephone enquiries, staff will only disclose personal data held on College systems if the following conditions are met:

   (i) The caller's identity is checked to make sure that information is given only to a person who is entitled to it.

   (ii) The caller will be asked to put their request in writing when their identity is unclear and cannot be checked.

   Staff should refer a request to the Data Protection Coordinator for assistance in difficult situations. Individuals should not be pressurised into disclosing personal information.
8. Data should be regularly reviewed and updated if it is found to be out of date. If no longer required, it should be deleted and disposed of in line with the College's data retention policy.
9. Staff should request help from the Data Protection Coordinator if they are unsure about any aspect of data protection.

8.0 Data Collection

The College will only process personal data when there is an appropriate legal basis for doing so. Special category personal data will only be processed when one of the appropriate legal conditions permitting such processing applies. There are particular provisions under the General Data Protection Regulation when the legal basis being relied on is consent. In certain circumstances the College may need to seek consent

to process personal data, particularly if it is outside of normal day to day activities or it would involve sharing personal data with a third party.

Informed consent is when:

- An individual clearly understands why their information is needed, who it will be shared with, the possible consequences of them agreeing or refusing the proposed use of the data
- And then gives their informed and unambiguous consent.

When collecting data, the College will ensure that the individual (the data subject):

- Has received sufficient information on why their data is needed and how it will be used.
- Is made aware what the data will be used for and what the consequences are should the individual decide not to give consent to processing.
- Where necessary, grants explicit consent, either written or oral for data to be processed.
- Is, as far as reasonably practicable, competent enough to give consent and has given so freely without any duress.
- In the absence of valid consent (that which is freely given, specific, informed and unambiguous) or where consent is deemed unnecessary, i.e., another legal basis applies, has received information as to the lawful basis for processing their information.

The College will ensure that data is collected within the boundaries defined in this policy. This applies to data that is collected in person or by completing a form.

9.0 Processing in Line with Data Subject's Rights

The College will process all personal data in line with the data subject's rights, in particular their right to:

(i) Request access to data held about them by a data controller.

(ii) Prevent the processing of their data for direct-marketing purposes.

(iii) Ask to have inaccurate data corrected or erased.

(iv) Prevent processing that is likely to cause damage or distress to themselves or anyone else.

10.0 Data Storage

When data is stored on paper, it should be kept in a secure place where unauthorised people cannot see it. These guidelines also apply to data that is usually stored electronically but has been printed out for some reason:

- When not required, papers or files should be put away securely.
- Staff should make sure papers and printouts are not left where unauthorised people can see them, for instance, on a printer.

- Paper based data should be shredded and disposed of securely when no longer required.

When data is stored electronically, it must be protected from unauthorised access, accidental deletion and malicious hacking attempts. It must be password protected and encryption should also be considered. Personal data collected should not be stored exclusively on a personal device as this may prevent legitimate access to and use of that data by the College.

11.0 Data Retention and Secure Destruction

Personal data will not be retained longer than necessary, in relation to the purpose for which such data is processed. The College will ensure that secure storage/archiving periods are clearly defined for each type of data and ensure confidential destruction of data when no longer required.

12.0 Data Use

Personal data is of no value to the College unless it can be used. However, it is when personal data is accessed and used that it can be at the greatest risk of loss, corruption or theft and so the following security measures are required:

- When working with personal data, staff should ensure that data presented on screen is not accessible to unauthorised persons, for example, screen locking or screen positioning.
- Personal data should not be shared informally. In particular, staff should be particularly vigilant when sending data by email as this form of communication is not secure.
- Personal financial data, and in particular bank details of individuals should not be transferred electronically. Bank details should usually only be transferred by letter and/or confirmed by telephone.
- Personal data should never be transferred outside of the European Economic Area without the approval of the Data Protection Coordinator and will only be permitted in the event that an adequate level of protection can be guaranteed. Some suppliers (e.g. cloud storage, survey software etc.) may operate outside of the EEA in terms of the processing they carry out and we will only use suppliers that can demonstrate GDPR compliance and have agreed to this in their terms and conditions.
- College staff, adjunct Faculty and part-time teachers should not save copies of UTC-obtained personal data to their own computers. Always access and update the central copy of any data where possible. Where access is not permitted then the College Administration should be asked to update the central copy.
- Consideration will be given to the anonymization or pseudonymising of personal data to promote the safe use or sharing of data within the College.