Data Protection Policy

May 2018

1. Introduction

Tyndale Theological Seminary processes the Personal Data of various individuals including students, staff, supporters and vendors. This processing is regulated by the European Union General Data Protection Regulation, May 2018 (EU Data Protection Law). The EU Data Protection Law is an extensive regulation that seeks to protect an individual's Personal Data. This Tyndale Data Protection Policy is intended to serve as a guide to how the law applies to all of the people who process Personal Data for the Seminary.

One of the main purposes of the EU Data Protection Law is to protect personal information and control how it is used in accordance with the legal rights of individuals. Consistent with the law, Tyndale seeks to protect and process Personal Data maintained by the seminary. For example, a student who applies for admission to the seminary must provide the school with his or her phone number. This would be protected Personal Data under the EU Data Protection Law.

In order to comply with the EU Data Protection Law, Tyndale's Data Protection Policy sets out responsibilities for all faculty (visiting or regular), staff, board members, external committee members (e.g. Program Advisory Committee), volunteers, vendors, students, and anyone else who accesses or processes Personal Data in their work or involvement with the Seminary.

The statements in this policy must be adhered to whether a person processes the Personal Data on Tyndale property or at another location. The Tyndale Data Protection Policy also seeks to avoid any improper uses of Personal Data, including loss of data or unauthorized uses. We recognize that in our context we have many visiting professors and volunteers, and our computer processing is often done on personal computers, not school-owned computers. As noted above, this policy applies to anyone who accesses or processes Personal Data for the Seminary.

2. Purpose

This policy and supporting procedures describe the Seminary's compliance with its obligation as a *data controller* and where applicable, a *data processor* under the EU Data Protection Law. (See Appendix A for Key Definitions).

Article 5 of the EU Data Protection Law has established at least six key principles to protect an individual's Personal Data. Consistent with these six principles, **Personal Data** should be processed (1) in a **lawfully, fairly, and transparent way** and (2) for a **legitimate purpose**. The Personal Data processed should be (3) **adequate, relevant and limited to what is necessary**. It should be (4) **accurate**, (5) **not stored longer than necessary** and (6) **protected with an appropriate level of security**. These six principles are further discussed below at point 3.1.

Personal Data is defined as any Information in any format that relates to an identified or identifiable living person.

3. Scope

This policy applies to all Personal Data received or created in the course of Seminary business. This includes all Personal Data contained in paper and electronic formats or communicated verbally in conversations, meetings or over the telephone or email.

The EU Data Protection Law seeks to protect the Personal Data of individuals, referred to as "Data Subjects." Data Subjects include, but are not limited to : inquirers, prospective students and employees, current students, employees and volunteers; alumni, former employees and volunteers, family members where emergency contacts are held, visiting faculty, board members, committee members, past, current or potential supporters, partners and vendors.

The EU Data Protection Law describes those individuals at or involved with the Seminary who may use Personal Data. For Tyndale's purposes a *User of Personal Data* is anyone who obtains, records, has access to, stores or uses Personal Data in the course of their work or involvement at Tyndale Theological Seminary. Users of Personal Data include but are not limited to students, employees, volunteers, visiting faculty, board members and committee members.

3.1 Principle 1

Personal Data shall be processed lawfully, fairly and in a transparent manner in relation to the Data Subject.

In practice, this means that you, as a User of Personal Data, must:

- collect and use Personal Data in accordance with the legitimate grounds established in the EU Data Protection Law;
- not use data in ways that have unjustified adverse effects on the individual concerned;
- be transparent and explain how the data is intended to be used, and give individuals appropriate Privacy Notices when collecting their Personal Data [Tyndale has developed the following Privacy Notices for: (1) Applicants; (2) Students; (3) Alumni; (4) Inquirers and Applicants (Employee/Volunteer); (5) Employees, Volunteers and Board Members; and (6) Supporters.];
- handle Personal Data only in ways that the Data Subjects would reasonably expect;
- rely on the consent of the individual to process. Such consent must be informed, freely given, with the understanding that the individual (Data Subject) can withdraw such consent at any time without detriment to their interests (There are certain types of data which are processed not based on consent but to deliver services. For example, employees have contracts that provide for monthly pay, remission of taxes to the Dutch Tax Authorities and other employee administrative matters. Privacy Notices delineate much of these uses, but one must evaluate if extra permissions are required for a particular means of processing Personal Data, e.g. using student stories or photographs in prayer letters);
- obtain additional consent if there is an intent to use "special categories of Personal Data," these are defined in Appendix A,
- do not do anything unlawful with the data.

3.2 Principle 2

Personal Data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.

In practice, this means that you, as a User of Personal Data, must:

- be clear from the beginning about why the Personal Data is being collected and its intended use (Privacy Notices explain these details);
- ensure that if the Personal Data will be used or disclosed for any purpose beyond what was initially intended, the new use or disclosure is fair and made known; and
- ensure the processing is necessary:
    - in relation to a contract which the individual has entered into (e.g. student, staff),
    - because the Data Subject has asked for something to be done so that they can enter into a contract,
    - because of a legal obligation that applies to Tyndale other than a contract,
    - for Tyndale's legitimate interest or a third-party recipients legitimate interest (e.g. statistical and historical records),
    - to protect an individual's "vital interests." This condition only applies in cases of life or death, such as the need for an individual's medical history for emergency treatment, or
    - for administering justice, or for exercising statutory, governmental or other public functions.

3.3 Principle 3

Personal Data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

In practice, this means that you, as a User of Personal Data, must:

- maintain Personal Data that is sufficient for the specific purpose for holding such data, and
- not hold more information than is needed for that purpose. Thus, a user must identify the minimum amount of Personal Data needed to fulfill the purpose, and hold that amount and no more.

3.4 Principle 4

Personal Data shall be accurate and, where necessary, kept up to date.

In practice, this means that you, as a User of Personal Data, must:

- take reasonable steps to ensure that both your Personal Data and the data you hold is accurate and
- take reasonable steps to ensure that Personal Data which is inaccurate is erased or rectified.

3.5 Principle 5

Personal Data shall be kept in a form which permits identification of Data Subjects for no longer than is necessary for the purposes for which the Personal Data is processed.

In practice, this means that you, as a User of Personal Data, must:

- review the length of time that you keep Personal Data;
- make Personal Data anonymous whenever appropriate, so that the individual can no longer be identified (e.g. keeping student papers as examples or accreditation purposes);
- consider the purposes for holding the information and in determining how long to retain it;
- securely delete information no longer needed for these purposes; and
- archive or delete information based on the Records Retention Policy.

3.6 Principle 6

Personal Data shall be processed in a manner that ensures appropriate security of the Personal Data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organizational measures.

In practice, this means that you, as a User of Personal Data, must:

- design your security to fit the nature of the Personal Data held and assess the harm that may result from a security breach;
- be ready to respond to any breach of security swiftly and effectively;
- report all suspected breaches to the Management Team promptly so that appropriate action can be taken;

Processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes is compatible with the storage limitation principles, subject to the appropriate safeguards for the rights of the Data Subjects.

The EU Data Protection Law also states that the Seminary must:

- proactively inform Data Subjects about his/her data processing activities and his/her rights under the law (e.g. Privacy Notices, Data Subject access requests);
- meet its legal obligations, as applicable, as a Data Controller and/or Data Processor, including data protection by design and default, maintaining records of processing activities, measures to ensure the security of the processing and handling of data breaches;
- allow Personal Data to be transferred to other countries only if those countries maintain the same level of protection for the privacy rights of the Data Subject concerned.

4. Additional Information

4.1 Privacy by Design and Privacy by Default

The EU Data Protection Law requires everyone at Tyndale to think about data protection and privacy whenever someone processes data. This means that data protection measures must be taken into account from the very start of using Personal Data in a new way. This would apply when using a new

data hosting software, beginning a new project or when making significant changes to how we process Personal Data.

Privacy by design includes examining the purposes for the data collection and use, the security measures that will protect it, the retention and deletion requirements, and how it can be accessed. Privacy by design therefore means that we will have measures in place to protect privacy from the outset of an activity. The phrase often used to protect privacy from the outset of an activity is "Data Protection Impact Assessment." This is especially needed when conducting activities that would be deemed of higher risk.

Privacy by default is processing based on current Privacy Notices.

4.2 Disclosure of Personal Data to Third Parties

The Data Subject is protected from disclosure of data to unauthorized third parties. Unauthorized third parties include a person or organization to whom the Data Subject has not consented that the data be disclosed or a person or organization to whom the Data Subject has consented that the data be disclosed, but where the request is for reasons other than that for which the data was collected or for which the consent was given. Unauthorized third parties may include family members, friends, local authorities, governmental bodies and the police. These parties may have legal reasons to request information, but that must be clearly determined before any information is disclosed.

Family members and friends often think that they may be entitled to information about students or staff members, however, unless there is a legal basis for this, e.g. power of attorney or contractual arrangement, they are not entitled to this information without consent.

Examples of authorized third party contacts (those which enable us to fulfill our contracts with students, employees or supporters) would be those that process Tyndale's payroll or the organization that does receipting for donations.

4.3 Sharing Personal Data with Colleagues

Under the EU Data Protection Law, Tyndale Theological Seminary is a single "Data Controller." This means that anyone who is processing data on behalf of Tyndale processes it on behalf of the entire organization. As a single Data Controller, passing information about staff or students between staff is normal. However, this does not mean that information can be shared freely. There should be a legitimate reason for the information to be shared, and the minimum amount of information should be shared. For instance, staff personal contact details (e.g. private mobile numbers and personal email addresses) should not be disclosed to students or people outside of Tyndale unless consent is given. This information is located on the Tyndale Address List, available to all faculty and staff. However, a person may restrict the information included there. Data concerning special category Personal Data, such as health, should not be shared unless absolutely necessary. Emails and envelopes with this kind of data should be marked as confidential.

4.4 Transfer of Data Outside of the European Economic Area (EEA)

According to the EU Data Protection Law, Personal Data shall not be transferred to a country outside the European Economic Area unless that country ensures an adequate level of protection for the

rights and freedoms of Data Subjects in relation to processing Personal Data. There are exceptions to this rule. For example, when a student requests that a transcript be sent to a country outside the EEA. The student's request gives explicit consent for this action.

In our situation of the missionary model, special consideration should be given when using student stories in our prayer letters and support raising materials. If a student can be easily identified in the way you use their Personal Data, then you will need to have their consent to use their information in this manner. If you use general pictures, etc., then there should be no issue as the publicity permission form that Tyndale requires would cover those instances. Please confirm this however before utilizing data in this manner.

4.5 Data Subject Access Requests

Tyndale maintains relevant information on staff and students. Under the EU Data Protection Law, staff and students are therefore considered "Data Subjects." A Data Subject has the right to ask to see the information that is kept on them. The Data Subject also has the right to have personal information deleted or destroyed. However, this right is not absolute and only applies in certain circumstances, for example, where the Seminary cannot evidence a legitimate basis for retaining it.

A Data Subject may obtain access to data held by completing a Data Subject Access Request (See Appendix B). The Data Subject seeking information normally would complete the request form, but the EU Data Protection Law allows the request to come in any form, even verbally. Should you, as a User of Personal Data, receive either a verbal or written request to have access to information, please inform the Management Team immediately. We generally have 30 days to respond to the request, and a careful process needs to be followed.

Since Data Subjects can ask to see all of the relevant data that Tyndale maintains through the Data Subject Access Request, it is important that any comments made on any documents, such as applications, references, interviews, examinations, projects and papers be made with the knowledge that your comments may be seen by the Data Subject. This means that you should use balanced and measured language in all instances. Try to avoid opinions and give instead the facts that may back up your opinion. For instance, if an instructor notices that a student misses class on a regular basis, the instructor should record this data by writing something objective, such as, "this student missed 9 out of 12 lectures," rather than "this student never showed up!"

Information about a Data Subject may also include information not in a physical file. To illustrate, a request can also include emails and electronic files. Therefore, you should think carefully about the substance of your emails and the kinds of electronic files that you keep. Electronic files should also be maintained to provide easy access about a particular Data Subject.

4.6 Release of Diploma and Transcripts to Student with Debts to the School

If a student remains in debt to the Seminary after he or she graduates, the diploma and accompanying paperwork and transcripts will not be released until payment is made in full. The student record will be annotated to note that the degree has not yet been conferred due to indebtedness. This will be available should the student make a Data Subject Access Request.

4.7 Community Duties

There may be times when a student is assigned a community duty that puts them into contact with Personal Data. In such cases the immediate supervisor must make sure that the student(s) are told about the importance of data protection and understand that the information they may have access to needs to be treated confidentially.

4.8 Photographs

A photograph of a person is considered "Personal Data." There are times when pictures and brief biographical information is put on our website and in other materials. When a student arrives at Tyndale, s/he will be asked to sign a publicity consent slip that will allow the Seminary to know the parameters under which this information can be used. Regular faculty, staff, volunteers, board members and other visiting lecturers will have given consent because of their position and the Privacy Notice associated with that consent. In any case, people do have a right to refuse to have their photograph or personal information published in this manner. It is best practice to seek permission for these types of activities.

4.9 Website

Information on the website is public. Therefore, anyone whose name and other information appears there needs to know that their data is being used in this manner and that they can object to the information that is shared and ask that it be removed.

4.10 References

The organization or person supplying a reference for a Data Subject does not have to show a copy to the Data Subject. However, if you are requested to provide a reference, you may choose to provide the information to the Data Subject. It would seem reasonable to provide a copy if a reference is wholly or largely factual in nature, or if the individual is aware of an appraisal of their work. However, please keep in mind that the organization who receives the reference does have to show it to the Data Subject if requested.

It is best to assume that at some point a reference will be seen by the person you are writing it about. When writing a reference, distinguish very carefully between opinion and presenting facts. You should also reveal only what is necessary and what you know the Data Subject has revealed about themselves. For instance, if a student had trouble during a term because of health issues and you think this affected their performance, then you should not reveal this without asking the student if this can be revealed in this reference.

If you receive and hold a reference for a Data Subject and that person asks to see it, you must weigh the confidentiality factor of the person who wrote it. If it is not clear that the Data Subject would already be aware of a referee's statements or opinions, then you should contact the referee for permission before disclosing it. Even then, the Data Subject may still have a legal basis for obtaining the reference. You must consider the following:

- any express assurance of confidentiality given to the person writing the reference;
- any relevant reasons the person gives for withholding consent;

- the potential effect of the reference on the Data Subject;
- the fact that the reference must be truthful and accurate and that without access to it the person is not able to challenge the accuracy
- is it possible to keep the identity of the person writing the reference confidential

4.11 Protecting Personal Data

All people representing Tyndale must do all they can to ensure that Personal Data is not accidentally lost or revealed to anyone who does not have a right to see it or hear it. The following provides guidelines to help you protect Personal Data.

- Computers which are used by staff to access Personal Data should not be placed in public areas where unauthorized persons can read the screens.
- Computers used in classroom settings should have password protection so that they cannot be accessed by an unauthorized person when you are out of the room for any reason.
- Personal files should be kept in locked filing cabinets or at the very least within a locked office. Never leave personal information lying openly available on your desk. If possible clean your papers off your desk when you leave work for the day.
- USB sticks, other media and printed data should be locked away when not in use and not left in public areas.
- Unwanted materials which contain Personal Data should be shredded.
- Computer passwords should not be easily deduced and should be changed regularly. They should also not be shared with another person.
- Permissions to systems, folders, etc. are properly set to prevent unauthorized access and are updated when staff and students leave the Seminary or change roles at the school.
- If your personal computer is also your work computer it must be protected by password controls and Tyndale files must not be accessible to your family members or friends if they are using your computer.
- Do not access Personal Data related to Tyndale in an unsecure wifi setting, such as a coffee shop.
- For Tyndale related activities, please use only your Tyndale email address. Your personal email will then not have any Personal Data information related to Data Subjects at Tyndale.
- If you use your mobile phone for Tyndale related information, make sure that it is set to lock out when it is not in use.
- Consider whether the content of an email should be encrypted or password protected. Note: If you do encrypt any emails you will need to be confident that you can access them if asked to do so for a Data Subject access request.
- Consider whether you want to use the blind copy (bcc) setting for people on an email so as to not reveal the addresses of all the recipients to each other. When you use (cc) every recipient of the message can see the addresses of one another.
- Be careful using group email addresses to make sure that you want the entire group to receive the email.
- Make sure you have virus and spyware protection that is up to date on your devices.
- Back up your files so that if you lose your computer, you do not lose the information.
- Securely remove all personal information before disposing of old computers (by using technology or destroying the hard disk)

- Think carefully about what you post on social media, especially in terms of people with whom you have contact because of your relationship with Tyndale. The protections for Personal Data apply in those venues.

4.12 Reporting

Please contact the Management Team immediately, if you suspect or are concerned that:

- a breach of the EU Data Protection Law has occurred or may occur;
- Personal Data is being used in a way that is not covered by a Privacy Notice;
- Personal Data is being used in a way that could result in unauthorized disclosure of that Personal Data (e.g. storing Personal Data on a computer that is not password protected).

It is also very important that the Management Team be immediately advised if you receive a Data Subject Access Request in any form. (See 4.5 and Appendix B)

4.13 Training

Relevant training sessions will be conducted during Administration Meetings, Faculty Meetings or Student Orientations. For those who serve here as outside lecturers and in other capacities, this Data Protection Policy will be made available, and any questions regarding compliance can be addressed to the Management Team. These materials are available on the website: www.tyndale-europe.edu.

Appendix A – General Data Protection Regulation (EU Data Protection Law)

Article 4 of the EU Data Protection Law provides a comprehensive list of definitions for terms used in the law. The following list seeks to provide a general understanding of some of the more frequently used terms in the law.

Data Controller	A natural or legal person (e.g. company) which, alone or jointly with others, determines the purposes and means for processing Personal Data.
Data Processor	A natural or legal person (e.g. company), public agency or other body which processes Personal Data on behalf of Tyndale.
Personal Data	Any information relating to an identified or identifiable living natural person (Data Subject). An identifiable natural person is one who can be identified directly or indirectly, in particular by reference to an identifier such as a name, and identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, economic, cultural or social identity of that natural person.
Special Categories Of Personal Data	Special categories of Personal Data include: a) racial or ethnic origin; b) political opinions; c) religious or philosophical beliefs; d) membership of a trade union; e) physical or mental health condition; f) sexual life or sexual orientation; g) proven or alleged offenses, including any legal proceedings and their outcome h) genetic or biometric data when processed to identify that individual
Processing	Processing means any operation or set of operations which is performed on Personal Data or on 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.

A full copy of the law can be viewed at https://gdpr-info.eu/.

Appendix B – Data Subject Access Request

Data Subject Access Request

Article 15 of the EU Data Protection Law provides that individuals (the Data Subject) have the right to know what Personal Data is being held about them and how that data is used.

You may apply to access your data. It is our preferred method for the Data Subject seeking information to do so by completing our Data Subject Access Request Form. Using this form better ensures that you know the types of information that we need in order to comply with your request.

Before we can act on your request as an individual (Data Subject), we must be sure of your identity and be supplied with information from you in order to locate the information that you are seeking. You have the right to obtain from the Seminary confirmation as to whether Personal Data concerning you is being processed by the Seminary, and, where that is the case, have access to the Personal Data.

Article 15 lays out your rights as follows:

The Data Subject shall have the right to obtain from the Data Controller confirmation as to whether Personal Data concerning him or her is being processed, and, where that is the case, access to the Personal Data and the following information:

a) the purposes of the processing;
b) the categories of Personal Data concerned;
c) the recipients or categories of recipient to whom the Personal Data have been or will be disclosed, in particular recipients in third countries or international organisations;
d) where possible, the envisaged period for which the Personal Data will be stored, or, if not possible, the criteria used to determine that period;
e) the existence of the right to request from the Data Controller rectification or erasure of Personal Data or restriction of processing of Personal Data concerning the Data Subject or to object to such processing;
f) the right to lodge a complaint with a supervisory authority;
g) where the Personal Data are not collected from the Data Subject, any available information as to their source;
h) the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) of the EU Data Protection Law, and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the Data Subject.

On receipt of your completed request, with the verification of your identity and sufficient details given to enable us to locate the information, the Seminary will generally respond within 30 calendar days.

All Data Subject Access Requests can be communicated through info@tyndale-europe.edu.

Data Subject Access Request Form

The following information is needed to help us respond to your inquiry. Please complete the information below and return the form by post or email to: info@tyndale-europe.edu.

Part 1 Your request

Title:	
Surname:	
Forename(s):	
Address:	
Telephone number:	
Email address:	
Other name by which you have been known, if applicable:	
Relationship to the Seminary:	
Dates at the Seminary:	

Please provide a detailed description of your request, and any further information which will enable us to locate your Personal Data (continue on the other side if necessary). The type of information you are interested in, e.g. student transcript.

Part 2 Proof of identity

The EU Data Protection Law requires the Seminary to satisfy itself as to the identity of the person making the request. Please send a photocopy of one form of identification containing a photograph (e.g. Tyndale ID Card, Passport, Driver's License with a picture) to info@tyndale-europe.edu or via the post to the address below. If your ability to provide this documentation is prohibitive please contact us to discuss alternative proof of identity arrangements. If the Seminary is unable to satisfy itself as to your identity from the documentation you send us, we will contact you as soon as possible.

Part 3 Fee

The EU Data Protection Law states that a fee may not be charged in most instances. There are exceptions if the request is either "manifestly unfounded or excessive, in particular because of their repetitive character" (Article 12(5)) or if the request is for additional copies of information already supplied. In such cases, the fee assessed will be the reasonable administrative costs of providing the information. Should a fee be required, you will be notified.

Part 4 Means of conveying the data to you, please check one:

_____ Paper copy mailed to the address given above.

_____ Commonly used electronic format emailed to the email address given above.

Part 4 Declaration

I am the Data Subject named in Part 1 of this document, and hereby request, under the provisions of the EU General Data Protection Regulation 2018, that Tyndale Theological Seminary provides me with copies of my Personal Data as described in Part 1.

I have provided my proof of identity.

Signature: ……

Date: ……

Tyndale Theological Seminary
Egelantierstraat 1
1171 JM Badhoevedorp
The Netherlands

Tel: +31 (0) 20 659 6455
Email: info@tyndale-europe.edu