STUDIORUM NOVI TESTAMENTI SOCIETAS

DATA PROTECTION POLICY

(Revised August 2019)

Contents

1. *Purpose of this policy*

1.1. SNTS ("**the Society**") is committed to complying with privacy and data protection laws including:

(a) the General Data Protection Regulation ("**the GDPR**") and any related legislation which applies in the UK, including, without limitation, any legislation derived from the Data Protection Bill 2017;

(b) the Privacy and Electronic Communications Regulations (2003) and any successor or related legislation, including without limitation, E-Privacy Regulation 2017/0003; and

(c) all other applicable laws and regulations relating to the processing of personal data and privacy, including statutory instruments and, where applicable, the guidance and codes of practice issued by the Information Commissioner's Office ("**ICO**") or any other supervisory authority.

(together "**the Legislation**")

1.2. This policy sets out what we do to protect individuals' personal data.

1.3. Anyone who handles personal data in any way on behalf of the Society must ensure that we comply with this policy. Section 3 of this policy describes what comes within the definition of "**personal data**". Any breach of this policy will be taken seriously and may result in disciplinary action or more serious sanctions.

1.4. This policy may be amended from time to time to reflect any changes in legislation, regulatory guidance or internal policy decisions.

2. *About this policy*

2.1. The types of personal data that we may handle include details of: the names, contact details, institution, and country of location of those who are or were members of the Society or were nominated to be members of the Society, together with a list of roles held or presentations/papers delivered within the Society, and the date on which they became a member or resigned from membership; names and contact details of those who attend General Meetings or other events or take out subscriptions to our publications; names and contact details in relation to those who organise and deliver General Meetings or other events on behalf of the Society; and names, contact details and other personal data in relation to the Society's Officers, Trustees and volunteers.

The Secretary of the Society ("**the Secretary**") is responsible for ensuring compliance with the Legislation and with this policy. Any questions or concerns about this policy should be referred in the first instance to the Secretary who can be contacted at secretary@snts.international.

3. *Definitions of data protection terms*

3.1. The following terms will be used in this policy and are defined below:

3.2. data subjects include all living individuals about whom we hold personal data, for instance a member or former member of the Society. A data subject need not be a UK national or resident. All data subjects have legal rights in relation to their personal data.

3.3. personal data means any information relating to a living person who can be identified directly or indirectly from that information (or from that information and other information in our possession). Personal data can be factual (such as a name, address or date of birth) or it can be an opinion (such as a performance appraisal). It can also include an identifier such as an identification number, location data, an online identifier specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person.

3.4. data controllers are the people who, or organisations which, decide the purposes for which, and the means for which, any personal data is processed. They have a responsibility to process personal data in compliance with the Legislation. The Society is the data controller of all personal data that we manage in connection with our work and activities.

3.5. data processors include any person who processes personal data on behalf of a data controller. Employees of data controllers are excluded from this definition but it could include other organisations such as website hosts, fulfilment houses or other service providers which handle personal data on our behalf.

3.6. European Economic Area includes all countries in the European Union as well as Norway, Iceland and Liechtenstein.

3.7. ICO means the Information Commissioner's Office (the authority which oversees data protection regulation in the UK).

3.8. processing is any activity that involves use of personal data, whether or not by automated means. It includes but is not limited to collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction of personal data.

3.9. sensitive personal data (which is defined as "**special categories of personal data**" under the GDPR) includes information about a person's:

(a) racial or ethnic origin;

(b) political opinions;

(c) religious, philosophical or similar beliefs;

(d) trade union membership;

(e) physical or mental health or condition;

(f) sexual life or orientation;

(g) genetic data;

(h) biometric data; and

(i) such other categories of personal data as may be designated as "**special categories of personal data**" under the Legislation.

4. *Data protection principles*

4.1. Anyone processing personal data must comply with the six data protection principles set out in the GDPR. We are required to comply with these principles (summarised below),

and show that we comply, in respect of any personal data that we deal with as a data controller.

4.2. Personal data should be:

(a) processed fairly, lawfully and transparently;

(b) collected for specified, explicit and legitimate purposes and not further processed in a way which is incompatible with those purposes;

(c) adequate, relevant and limited to what is necessary for the purpose for which it is held;

(d) accurate and, where necessary, kept up to date;

(e) not kept longer than necessary; and

(f) processed in a manner that ensures appropriate security of the personal data.

5. *Processing data fairly and lawfully*

5.1. The first data protection principle requires that personal data is obtained fairly and lawfully and processed for purposes that the data subject has been told about. Processing will only be lawful if certain conditions can be satisfied, including where the data subject has given consent, or where the processing is necessary for one or more specified reasons, such as where it is necessary for the performance of a contract.

5.2. To comply with this principle, every time we receive personal data about a person directly from that individual, which we intend to keep, we need to provide that person with "**the fair processing information**". In other words we need to tell them:

(a) the type of information we will be collecting (categories of personal data concerned);

(b) who will be holding their information, i.e. the Society, including contact details and the contact details of the Officer who is responsible for data protection;

(c) why we are collecting their information and what we intend to do with it, for instance to send them mailing updates about our activities;

(d) the legal basis for collecting their information (for example, are we relying on their consent, or on our legitimate interests or on another legal basis);

(e) if we are relying on legitimate interests as a basis for processing what those legitimate interests are;

(f) whether the provision of their personal data is part of a statutory or contractual obligation and details of the consequences of the data subject not providing that data;

(g) the period for which their personal data will be stored or, where that is not possible, the criteria that will be used to decide that period;

(h) details of people or organisations with whom we will be sharing their personal data;

(i) if relevant, the fact that we will be transferring their personal data outside the EEA and details of relevant safeguards; and

(j) the existence of any automated decision-making including profiling in relation to that personal data.

5.3. Where we obtain personal data about a person from a source other than the person his or her self, we must provide that individual with the following information in addition to that listed under 5.2 above:

(a) the categories of personal data that we hold; and

(b) the source of the personal data and whether this is a public source.

5.4. In addition, in both scenarios, (where personal data is obtained both directly and indirectly) we must also inform individuals of their rights outlined in section 9 below, including the right to lodge a complaint with the ICO and, the right to withdraw consent to the processing of their personal data.

5.5. This fair processing information can be provided in a number of places including on web pages, in mailings or on application forms. We must ensure that the fair processing information is concise, transparent, intelligible and easily accessible.

6. *Processing data for the original purpose*

6.1. The second data protection principle requires that personal data is only processed for the specific, explicit and legitimate purposes that the individual was told about when we first obtained their information.

6.2. This means that we should not collect personal data for one purpose and then use it for another. If it becomes necessary to process a person's information for a new purpose, the individual should be informed of the new purpose beforehand. For example, if we collect personal data such as an email address, in order to update a person about our activities it should not then be used for any new purpose, for example to share it with other organisations for marketing purposes, without first getting the individual's consent.

7. *Personal data should be adequate and accurate*

The third and fourth data protection principles require that personal data that we keep should be accurate, adequate and relevant. Data should be limited to what is necessary in relation to the purposes for which it is processed. Inaccurate or out-of-date data should be destroyed securely, and we must take every reasonable step to ensure that personal data which is inaccurate is corrected.

8. *Not retaining data longer than necessary*

8.1. The fifth data protection principle requires that we should not keep personal data for longer than we need to for the purpose it was collected for. This means that the personal data that we hold should be destroyed or erased from our systems when it is no longer needed. If you think that we are holding out-of-date or inaccurate personal data, please refer to the Secretary.

8.2. For guidance on how long particular types of personal data that we collect should be kept before being destroyed or erased, please refer to the Society's Data Retention Policy, contact the Secretary or seek legal advice.

9. *Rights of individuals under the GDPR*

9.1. The GDPR gives people rights in relation to how organisations process their personal data. Everyone who holds personal data on behalf of the Society needs to be aware of these rights. They include (but are not limited to) the right:

(a) to request a copy of any personal data that we hold about them (as data controller), as well as a description of the type of information that we are processing, the uses that are being made of the information, details of anyone to whom their personal data has been disclosed, and how long the data will be stored (known as subject access rights). We cannot charge a fee for providing this information, and we must provide any information without delay and at the latest within one month of receipt of the request. Any Officer or Trustee receiving a written request from an individual for the personal information we hold on them should immediately inform the Secretary so that the request can be handled in accordance with relevant legislation and completed within the timescales specified above;

(b) to be told, where any information is not collected from the person directly, any available information as to the source of the information;

(c) to be told of the existence of automated decision-making;

(d) to object to the processing of data where the processing is based on either the conditions of public interest or legitimate interests;

(e) to have all personal data erased (the right to be forgotten) unless certain limited conditions apply;

(f) to restrict processing where the individual has objected to the processing;

(g) to have inaccurate data amended or destroyed; and

(h) to prevent processing that is likely to cause unwarranted substantial damage or distress to themselves or anyone else.

10. *Contacting members*

10.1. We will ensure that we comply with the Legislation, and particularly the Privacy and Electronic Communications Regulations (2003) and any successor or related legislation, when contacting members or those attending a General Meeting.

11. *Data security*

11.1. The sixth data protection principle requires that we keep secure any personal data that we hold.

11.2. We are required to put in place procedures to keep the personal data that we hold secure, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

11.3. When we are dealing with sensitive personal data, more rigorous security measures are likely to be needed, for instance, if sensitive personal data (such as details of an individual's health, race or sexuality) is held on a memory stick or other portable device it should always be encrypted.

11.4. When deciding what level of security is needed, your starting point should be to look at whether the information is sensitive or highly confidential and how much damage could be caused if it fell into the wrong hands.

11.5. The following security procedures and monitoring processes must be followed where possible and appropriate in relation to all personal data processed by us:

(a) encryption of personal data;

(b) other measures to ensure confidentiality, integrity, availability and resilience of processing systems;

(c) measures to restore availability and access to data in a timely manner in event of physical or technical incident;

(d) backing up data: daily back-ups should be taken of all electronic data;

(e) equipment: officers and trustees should ensure that individual monitors do not show confidential information to passers-by and that they log off from their PC when it is left unattended;

(f) methods of disposal: paper documents should be incinerated or shredded. Memory sticks, CD-ROMs and other media on which personal data is stored should be physically destroyed when they are no longer required;

(g) secure exchange of data: personal data must always be transferred in a secure manner. The degree of security required will depend on the nature of the data; the more sensitive and confidential the data, the more stringent the security measures should be;

(h) secure lockable desks and cupboards: desks and cupboards should be kept locked if they hold confidential information of any kind (personal information is always considered confidential); and

(i) travelling with personal data and remote working: officers and trustees must keep data secure when travelling.

12. *Transferring Data Outside the EEA*

12.1. The GDPR requires that when organisations transfer personal data outside the EEA, they take steps to ensure that the data is properly protected.

12.2. The European Commission has determined that certain countries provide an adequate data protection regime. These countries currently include Andorra, Argentina, Canada, Guernsey, Isle of Man, Israel, New Zealand, Switzerland, Faroe Islands, Jersey and Uruguay, but may be updated.

12.3. As such, personal data may be transferred to people or organisations in these countries without the need to take additional steps beyond those you would take when sharing personal data with any other organisation. In transferring personal data to other countries outside the EEA (which are not on this approved list), it will be necessary to enter into an EC-approved agreement, seek the explicit consent of the individual, or rely on one of the other derogations under the GDPR that apply to the transfer of personal data outside the EEA.

12.4. The EU-US Privacy Shield is an instrument that can be used as a legal basis for transferring personal data to organisations in the US, although specific advice should be sought from the data protection officer (if we have one) before transferring personal data to organisations in the US.

12.5. For more information, please refer to the Secretary or seek further legal advice.

13. *Processing sensitive personal data*

13.1. We may rarely collect information about individuals that is defined by the GDPR as special categories of personal data, and special rules will apply to the processing of it. In this policy we refer to "**special categories of personal data**" as "**sensitive personal data**". The categories of sensitive personal data are set out in the definition in Section 3.9.

13.2. Purely financial information is not technically defined as sensitive personal data by the GDPR. However, particular care should be taken when processing such data, as the ICO will treat a breach relating to financial data very seriously.

13.3. In most cases, in order to process sensitive personal data, we must obtain explicit consent from the individuals involved. As with any other type of information we will also have to be absolutely clear with people about how we are going to use their information.

13.4. It is not always necessary to obtain explicit consent. There are a limited number of other circumstances in which the GDPR permits organisations to process sensitive personal data. If you are concerned that you are processing sensitive personal data and are not able to obtain explicit consent for the processing, please refer to the Secretary.

14. *Notification*

14.1. We recognise that whilst there is no obligation for us to make an annual notification to the ICO under the GDPR, we will consult with the ICO where necessary when we are carrying out "high risk" processing.

14.2. We will report breaches (other than those which are unlikely to be a risk to individuals) to the ICO where necessary, within 72 hours. We will also notify affected individuals where the breach is likely to result in a high risk to the rights and freedoms of individuals.

15. *Record keeping*

15.1. We must keep a record of our data processing activities, to demonstrate that we are complying with them. These records will include the purpose of processing, descriptions of categories of data subjects and categories of personal data, details of transfers to third countries and retention periods of personal data.

16. *Monitoring and review of the policy*

16.1. This policy is reviewed annually by the Society Committee to ensure that it is achieving its objectives.

STUDIORUM NOVI TESTAMENTI SOCIETAS

DATA RETENTION POLICY AND SCHEDULE

(Revised August 2019)

Studiorum Novi Testamenti Societas (SNTS – "the Society")

1. **Purpose of this policy**

1.1 This document sets out the policy of the Society on how long records will be retained for, and includes an Appendix setting out specific retention guidelines for the key records that we hold.

2. **Rules relating to the retention of records**

2.1 There are some statutory requirements which prescribe how long certain types of records must be kept, and these are set out where relevant in the Appendix to this policy. However, in many cases there will not be any prescriptive statutory retention period, and deciding how long a particular record should be retained for will require the Society to balance the possible need to have access to those records in the future, against the practical and legal requirement to maintain organised, accurate and relevant records which are not excessive.

2.2 In accordance with the relevant provisions of the Data Protection Act 1998 (the "**DPA**") and the General Data Protection Regulation ("**GDPR**"), the Society will not retain personal data for any longer than is necessary for the purposes for which the personal data is processed. There are no specific minimum periods set out in the DPA or GDPR for retaining personal data, but the Society has the necessary processes in place to ensure that, once records containing personal data are no longer needed, they are destroyed securely, and are not simply retained indefinitely (unless we have identified a clear and justifiable reason for doing so). Other procedures may also be implemented as part of the retention strategy, such as the archiving of data (in order to put it out of immediate use).

3. **Storage of data**

3.1 Any data that is retained by the Society will be held securely in order to prevent loss or unauthorised access.

3.2 Hard copy data will be stored in a secure location when not in use e.g. lockable filing cabinets, cupboards, rooms.

3.3 Electronic data containing personally identifiable information will be stored securely using encryption and/or password protection in order to prevent loss, theft or unauthorised access.

4. **Transfer of data**

4.1 This constitutes the transfer of records from one place/electronic system to another. The careless disposal of media could result in breaches of confidentiality or risk to the integrity of the organisation.

4.2 All records containing personally identifiable information will be subject to encryption and/or password protected whilst in transit.

4.3 All electronic records will be backed up at source so that in the event of a data loss, the contents of the original are not lost.

4.4 If information is transferred for the purposes of safer storage, for example from paper to scanned copy, then the original will be safely and securely destroyed.

5. **Destruction of data**

5.1 The destruction of records is an irreversible act. Records may contain sensitive and/or confidential information and their destruction will be undertaken in a secure way and location. Destruction of all records, regardless of the media, will be conducted in a secure manner to ensure there are safeguards against accidental loss or disclosure.

5.2 Paper records containing personal or organisationally sensitive information will be disposed of securely using methods such as incineration or shredding.

6. Retention schedule

6.1 The retention periods set out in the attached Appendix are guidelines rather than absolute requirements (except where a specific statutory requirement is referenced), but the presumption is that at the end of the specified period, the record should be destroyed or achieved/pseudo-anonymised, in accordance with any data disposal procedures set out above and any other guidelines issued by the Society from time to time.

6.2 In some situations it may be appropriate to continue to retain personal data even after the guideline retention period has expired, including situations where:

(a) the record is relevant to legal action which has been started or is anticipated, in which case the record should be retained for at least the period in which a claim could be brought against the Society. For most legal claims, the limitation period requires a claim to be brought within 6 years following the event in question;

(b) a contractual obligation term requires the Society to retain the record; or

(c) there is another good reason why it should be retained beyond the guideline retention period. If you believe this to be the case, you should discuss this with the data protection officer.

6.3 When records are being kept for more than the recommended retention period, the records will be clearly marked and the reasons for the extension clearly identified.

6.4 If no retention period for a certain type of record is specified in the Appendix, then you should seek guidance from the data protection contact on how long the record should be retained for.

APPENDIX: Retention Schedule

Member Records

Document/data type	Guideline Retention Period	Reason
Name: • First and last names • Title • Country of location	Permanently	In order to keep a permanent record of Society membership
Location: • Email addresses • Associated academic institution	On resignation	
Demographic information: • Date of birth • Gender (may be inferred based on name)	6 years from resignation	Date of birth is only necessary with regard to Life Membership
Annual Membership Subscription information: • Details of payments	6 years from resignation	
Activity information: • Event attendance • Roles in the Society (including Committee Membership; Officers; Seminar convener) • Presentation/papers delivered in the Society	Permanently	
Suppression information (including TPS and FPS where relevant) – name and address	Permanently	To prevent the person being contacted again

Membership Nomination records

Document	Guideline Retention Period	Reason
Membership nomination application, of those who are unsuccessful	Two years after notifying the unsuccessful candidate	
References, of those who are unsuccessful	Two years after notifying the unsuccessful candidate	

Committee records

Document	Guideline Retention Period	Reason
Society minutes of meetings and decisions	Permanently	S. 248 Companies Act 2006 requires these to be kept for at least ten years from the date of the meeting or decision, the Society's policy is to keep these records permanently
Annual accounts and reports	Permanently	

Accounts

Document	Guideline Retention Period	Reason
Bank records	Six years from the end of the relevant financial year	Companies Act 2006/Taxes Management Act 1970/HMRC

STUDIORUM NOVI TESTAMENTI SOCIETAS

PRIVACY POLICY

(Revised August 2019)

Studiorum Novi Testamenti Societas (SNTS – "the Society")

1. Introduction

The Society is a charity registered in England and Wales with charity number 313862 and registered address BEDW ARIAN, LLANARTH, CEREDIGION, SA47 0NT. The Secretary (secretary@snts.international) is the point of contact for any questions relating to Data Protection and related issues.

The Society's webpages are hosted on the website snts.international ("**the website**").

We are committed to protecting your privacy and will only use the information that we collect about you lawfully. This policy is intended to give you an understanding of how and why we use the information you provide to us both online and otherwise.

Please read this policy carefully to understand how we will collect, use and store your data. We may update this policy from time to time without notice to you, so please check it regularly.

2. Why we collect information

We collect information to allow us to:

(a) provide you with the information, goods or service you have requested from us, including subscriptions to our publications;

(b) to facilitate our events and programmes;

(c) to invite you to events that we organise;

(d) to inform you about the work of the Society; and

(e) so we can improve how we communicate with you and how we operate more generally.

3. What information do we collect about you?

We collect information whenever you interact with us, for example if you provide us with your details for any reason (through our website or otherwise), buy goods from us, attend our events. We also collect your information if you work with us.

The personal data we collect can include:

(a) Your full name and title;

(b) email addresses;

(c) country of location;

(d) associated academic institution;

(e) records of your correspondence with us;

(f) details of your education, including academic qualifications, publications and/or other relevant achievements;

(g) details of academic references;

(h) records of your attendance and involvement at Society events;

(i) subscription and other payment details; and

(j) information you enter onto the website.

We may sometimes, in addition to the above, ask you to provide information about your date of birth and gender. However, this is completely voluntary, and we will never collect sensitive personal data such as this without your explicit consent.

4. How will we use the information about you?

We will process your data for the following reasons:

a) to administer your payment or donation;

b) to acknowledge donations;

c) to administer our events and other programmes;

d) to deliver services, literature and/or other materials and information you have requested from us, such as our newsletter, subscriptions and other publications;

e) to allow you to attend our conferences or other events;

f) to process payment for and deliver goods you purchase from us;

g) where you have consented, to send you information that we think you may be interested in, including updates on our work, fundraising appeals and invitations to events by post and email;

h) to contact you about raising money for the Society;

i) for our own internal administrative purposes and to keep a record of your relationship with us;

j) to manage your communication preferences;

k) to carry out research to find out more information about our applicants' and supporters' backgrounds and interests (for example, academic and/or theological background); and

l) to comply with applicable laws and regulations, and requests from statutory agencies.

The legal basis that we rely on for processing your data is either where:

- you have provided your consent to us using your data in a certain way;
- it is necessary to for compliance with a legal obligation to which we are subject; or
- where it is in our legitimate interests to do so e.g. in order to process donations and administer the charity, provided this is not unwarranted by reason of prejudice to you. Our legitimate interest in these cases is in pursuance of our charitable purposes. When we process your personal information for our legitimate interests, we make sure to consider and balance any potential impact on you (both positive and negative), and your rights under data protection laws. We will not use your personal data for activities where our interests are overridden by the impact on you (unless we have your consent or are otherwise required or permitted to by law).

5. Communications and marketing

We will contact you by email or post, with communications to let you know about our events and activities that might be of particular interest to you; about the work of the Society more generally; and to request payments or donations and provide you with information about our fundraising activities. We may also send you surveys and requests for information from time to time.

6. Will we share this information with others?

We do not share, sell or rent your information to third parties for marketing purposes. We may share some of your information with Cambridge University Press. We will ensure that we have appropriate safeguards in place when we do this. We will not otherwise disclose your personal information unless required to do so by a regulatory agency or law.

We may allow our officers, trustees, consultants and/or external providers or conference organisers acting on our behalf to access and use your information for the purposes for which you have provided to us (e.g. to deliver mailings, to analyse data and to process payments). We only provide them with the information they need to deliver the relevant service, and we make sure your information is treated with the same level of care as if we were handling it directly.

7. How do we protect the security of personal data?

We aim to ensure that there are appropriate physical, technical and managerial controls in place to protect your personal details.

Your information is only accessible by officers, trustees, Society members acting on behalf of the Society, and organisers of Society events.

Unfortunately, the transmission of information via the internet is not completely secure. Although we will do our best to protect your personal data, we cannot guarantee the security of your data transmitted to our site; any transmission is at your own risk. Once we have received your information, we will use strict procedures and security features to try to prevent unauthorised access.

The information we collect from you may be transferred to and processed and/or stored at a destination outside the European Economic Area ("**EEA**"). If we send your personal data outside the EEA we will take reasonable steps to ensure that the recipient implements appropriate measures to protect your information.

8. How long do we keep your data for?

We will keep your personal data for no longer than is necessary for the purposes for which it is processed, in accordance with our Data Retention Policy.

If you request to receive no further contact from us, we will keep some basic information about you on our suppression list in order to avoid sending you unwanted materials in the future.

9. What if you have questions or need to make corrections to your information?

You have the right to request details of the information that we hold about you. If you would like to do so please contact us using the details below.

We also want to make sure that your personal information is accurate and up to date. Please let us know if your details change. You may also ask us to correct or remove information you think is inaccurate.

You can also request that we stop processing data about you for certain purposes (e.g. profiling) at any time by contacting us using the details below.

Please let us know if you have any queries or concerns about the way that your data is being processed by contacting us on the details below. You are also entitled to make a complaint to the Information Commissioner's office, and for further information see the Information Commissioner's guidance here https://ico.org.uk/for-the-public/personal-information.

10. How will we let you know of changes to our privacy policy?

We may update this policy from time to time without notice to you, so please check it regularly. The privacy policy was last updated on 07 July, 2018.

11. How to contact us

Please contact us if you have any questions about our privacy policy or information we hold about you (secretary@snts.international).