Southern Adventist University

Website Privacy Policy

Version 1 Revised 12/12/21

1. Introduction

THIS DOCUMENT DESCRIBES THE PRIVACY AND DATA PROTECTION PRACTICES OF THE SOUTHERN ADVENTIST UNIVERSITY IN CONNECTION WITH THE RIGHTS AVAILABLE TO VISITORS AND USERS PERSONAL INFORMATION WHEN THEY ACCESS AND USE THE WEBSITE AND ANY OF OUR SERVICES.

The website: https://www.southern.edu ("Website") is owned and operated by the Southern Adventist University (collectively referred to as "Southern Adventist University" and/or "University" and/or "We" and/or "Us").

Please note that for the purposes of this Privacy Policy, "You" and/or "User" means any individual who may access and/or browse and/or register and use our Website and Services.

We guarantee that your Personal Information is protected by all privacy and data protection rights under the Tennessee Code § 47-18-2107 (2019) (Tennessee's Data Breach Notification Law) as well as the California Consumer Privacy Act (CCPA) and California Online Privacy Protection Act (CalOPPA), along with the Children's Online Privacy Protection Act (COPPA) and the CAN-SPAM Act of 2003, applicable throughout the United States of America; and the General Data Protection Regulation (GDPR) approved by the European Parliament and all other privacy and data protection regulations and international treaties.

This Privacy Policy is a legally binding agreement between you and the Southern Adventist University, and is incorporated into and subject to our Terms and Conditions. The use of our Website and Services is subject to your acceptance of this Privacy Policy.

By accessing, registering with us and/or using our Website and Services, you expressly agree and electronically consent to all provisions of this Privacy Policy.

If you do not agree with this Privacy Policy, you must not use our Services and leave this Website immediately.

Please note that the access to and/or browsing and/or registration of an User Account and/or the use of this Website and Services implies that you grant your consent and are expressly accepting the provision of this Privacy Policy.

Please read the definitions applicable to this Privacy Policy in Section 23 set out below.

2. Data Controller and Data Processor

The Southern Adventist University is the Data Controller and Data Processor of your Personal Information.

The University details are as follows:

- Name: Southern Adventist University.
- Address: 4881 Taylor Circle Collegedale, TN 37315, USA.
- Phone: 1.800.SOUTHERN (768.8437).
  Local: 423.236.2000.
  Fax: 423.236.1000.
- Website: https://www.southern.edu.
- Email: webhelp@southern.edu.

By accepting this Privacy Policy, you are expressly consenting and agreeing that the Southern Adventist University is the Data Controller and Data Processor of the information you provide when using our Services.

3. Data Subject to this Privacy Policy

This Privacy Policy applies to any information collected from you ("Personal Information"), in accordance with this document, when you access and use our Website and Services and also when you contact us by email or otherwise.

This Privacy Policy does not apply to any information about you provided by third parties and/or publicly available with no restrictions. We are not responsible for the privacy practices of third parties.

4. Granting Consent

By accepting this Privacy Policy you expressly agree to grant the Southern Adventist University a non-exclusive, worldwide, temporary, revocable, royalty-free, sub licensable right, to exercise the copyright, publicity, and/or any database rights (but no other rights) you have on your Personal Information, in any media now known or that may be known in the future, with respect to your Personal Information, solely for the purpose of enabling the University the use of the information provided by you for the use of the Website and Services and to avoid the violation of any rights over that information.

The Southern Adventist University does not collect Personal Information from you or any third party without the prior express consent of the owner of such information.

By accepting this Privacy Policy you expressly represent and warrant that you are of legal age, and accordingly, in the legal capacity to consent to the collection of your Personal Information in accordance with the applicable law in your jurisdiction.

5. Information Collect by Us

We only request Personal Information that is necessary for you to use this Website and Services. We do not collect, retain or store information from you regarding any payment methods.

We reserve the right to confirm and validate your Personal Information and any other information provided by you at any time. In the event that we determine that the information provided by you is unlawful, fraudulent, erroneous or incorrect (totally or partially), we may cancel your access and use of our Website and Services at any time and without prior notice.

The information we collect from you when you use this Website and Services is as follows ("Personal Information"):

5.1. Information Provided By You.

We will collect the following information from you through our Website:

a) When you register on the Website (for Undergraduate or Graduate Students):

- Email Address;
- First Name;
- Last Name; and
- Birthday.

b) When you create your Southern Account on our Website (Students, Employees and Board Members):

- Southern ID number;
- Birth Date;
- Social Security Number;
- User Name; and
- Password,

c) When you Reactivate your Academic Program:

(i) Demographic Information:

- First Name;
- Middle Name;
- Last Name;
- Person ID; and
- Date of Birth.

(ii) Contact Information:

- Street Address;

- City;
- State;
- Zip/Postal Code;
- Email Address; and
- Mobile Phone.

(iii) Academic Information:

- Semester;
- Year;
- If your attended another college since you last applied or enrolled:
- Academic Level;
- Intendent Major;
- Specification on whether you made a medical withdrawal during your last semester at the University ; and
- Your signature.

d) When you complete the New Social Account Registration Form on the Website:

- Name;
- The Department of Organization Account is set up for;
- Social Media Platform (Facebook; Instagram; Twitter; Tik Tok; SnapChat; YouTube; LinkedIn; or Other);
- Account's password (if it's not a Facebook or LinkedIn Account); and
- List the name of all employees who will have access to the Account.

e) When you make an appointment to visit our Campus through our Website (Graduate Students):

- First Name;
- Middle Name;
- Last Name;
- Email Address;
- Birthdate; and

- Level of Study.

f) When you apply on our website for University Admission, Program and Course Enrollment.

Some pages on our Website link to an external system at https://www.southern.edu/undergrad/homepage/index.html.

This is the Customer Relationship Management (CRM) platform used by the University. It is used to identify and track potential and current applicants, and it does collect Personal Information. This data is closely held by the University and stored in a secure manner.

Users who have questions about data submitted through https://www.southern.edu/undergrad/homepage/index.html should contact marketing@southern.edu

g) When you use any Forms on our Website and make any Voluntary Submission of Information.

Some pages on our Website contain web forms to collect information from the user. The information collected is used by the University academic and business units and is not stored in a secure manner. Please note that Users should not submit sensitive personal, financial, business or academic information via web forms on our Website.

5.2. Information Collected by our Website:

We automatically collect the following Data about you, through this Website:

a) Device data, such as Device operating system type and version number, manufacturer and model, browser type, screen resolution, IP address, the website you visited before accessing and using our Website and Services;

b) Geolocation data, such as your city, state, locality or geographic area.

c) Online activity data, such as pages or screens you viewed on our Website; how long you stayed on a page or screen; navigation paths between pages or screens; information about your activity on a page or screen, access times, and access duration.

6. Use of your Personal Information

We collect and process Personal Information about you where we have a legal basis to do so, including for the following reasons:

a) To render Services to you or to fulfill a contractual agreement with you when you visit the Website. This includes to:

- Provide you with information, emails, or services that you request from us;

- Recruit employee applicants for job openings, communicate with applicants and process applications; and

- Communicate and provide additional information that may be of interest to you about the University and our third-party partners at your request.

b) When we have legitimate business reasons to do so. This includes to:

- Respond to your questions, comments, feedback, or inquiries, including those concerning technical and user support;

- Share your Personal Information amongst the University organization;
- Ensure that content from our Website is presented in the most effective manner for you and for your device;

- Operate, maintain, improve, and develop our Website and Services;

- Allow you to interact with certain third-party content service providers (for example, to enable you to link to, or view content from,

third-party sites within our Website, or view our content on a third-party site);

- Allow you to participate in interactive features of our Website when you choose to do so; and

- Identify your preferences so we can notify you of new or additional information or, that might be of interest to you.

c) When we have your consent (You will be requested to provide your consent prior to submitting information to us). This includes to:

- Send you emails, newsletters or information about the University , or subscribe or unsubscribe you to one of our mailing lists upon your request;

- Manage your Personal Information through our service providers; and

- Obtain information about your medical condition.

d) To comply with legal obligations to which we are subject. This includes to:

- Comply with legal obligations, regulatory investigations or litigation and protecting the University against injury, theft, legal liability, fraud, abuse or other misconduct;

- For fraud prevention, public safety, and enforcement of our reporting obligations and Terms of Use; and

- To comply with court orders, subpoena or other legal process.

7. Data Protection

The University guarantees the privacy, confidentiality, security and protection of your Personal Information and also guarantees that it has implemented physical and electronic security measures, as well as other appropriate administrative

procedures to prevent unauthorized or unlawful access by third parties to your Personal Information.

We maintain and enforce various policies, standards and processes designed to secure our Users' Personal Information and other data to which the University´s employees are provided access to, and protect our Users' Personal Information as other data from accidental loss or destruction.

Please read the description below of some of the core technical and organizational security measures implemented by the University**.**

Our data protection and security practices include, but are not limited to:

- The continuous review and updates of our security policies and controls, as technology changes to ensure ongoing information security.

- Implementation of reasonable and appropriate technical security measures to protect the Personal Information we process, from unauthorized access, alteration, disclosure, loss or destruction.

- Application of the duty of confidentiality for any authorized personnel who processes your Personal Information.

- Regular audits of the security measures of the Website by requesting third party experts to review our security controls against international standards. These audits help us to further improve our security levels.

- All information in transit and at rest is encrypted, and where possible specific fields are encrypted using industry recognized cryptographic measures.

a) Information Security Policies and Standards.

We implement security requirements on our employees and staff, as well as all subcontractors, vendors, or agents who have access to Personal Information designed to ensure a level of security appropriate for the risk, to address the requirements detailed in these Security Standards.

For more details on our security requirements applicable to our employees, you may review our **Employee Computer and Internet Policy** available on our Website.

We conduct periodic risk assessments and review, as appropriate, and revise information security practices at least annually or whenever there is a material change in the University's business practices that may reasonably affect the security, confidentiality or integrity of Personal Information of our Users, provided that the University will not modify its information security practices in a manner that will weaken or compromise the confidentiality, availability or integrity of such Personal Information.

b) Physical Security.

The University maintains commercially reasonable security systems in its Website to protect and guarantee the security and confidentiality of Personal Information of our Users. We reasonably restrict access to our Users' Personal Information and have in place sufficient practices to prevent unauthorized individuals from gaining access to such information.

c) Use and Storage.

The University maintains records specifying which media are used to store the Personal Information of our Users.

When media are to be disposed of, or reused, procedures have been implemented to prevent any subsequent retrieval of any Personal Information stored by our Users before they are withdrawn from the inventory. When media are to be disposed of, or reused, procedures have been implemented to prevent undue retrieval of Personal Information stored on them.

All Personal Information security incidents are managed in accordance with appropriate incident response procedures.

We ensure: (i) that Personal Information of our Users cannot be read, copied, modified or deleted without authorization during electronic transmission,

transport or storage, and (ii) that the target entities for any transfer of information by means of data transmission through their Website can be established and verified.

We will burn, shred or otherwise destroy documents and magnetic records used for intermediate processing activities (e.g., portable disks used to upload restricted data to the server).

We ensure that the Personal Information of our Users collected and stored in the Website and servers for different purposes can be processed separately. We keep databases containing our Users' Personal Information separate from information obtained from any other third party.

For more detail about how we classify and store your Personal Information, you may review our **Data Classification, Access, Transmission, and Storage Policy** available on our Website.

d) Access Control.

The University maintains appropriate access controls, including, but not limited to, restricting access to our Users' Personal Information to the minimum number of University´s Personnel who require such access.

We will maintain a list of persons who have accessed restricted data and a list of those permitted access to the data (including their identification numbers, access codes and the types of information to which they are permitted access).

Among other safety practices, we ensure that:

i) The access codes must be changed periodically or upon a change of employees;

ii) Only authorized staff can grant, modify or revoke access to an information system that uses or houses the Personal Information of our Users;

iii) User administration procedures define Users´ roles and their privileges and how access is granted, changed and terminated;

address appropriate segregation of duties and define the logging/monitoring requirements and mechanisms;

iv) All employees of the University are assigned unique User-IDs; and

v) Access rights are implemented adhering to the "least privilege" approach.

We also implement commercially reasonable physical and electronic security measures to create and protect all passwords.

We establish systems to prevent recollecting, processing and/or storage systems on our Website from being used accidentally or without authorization, such as through logical access controls.

For more details on the access control measures we apply, please refer to our **Data Classification, Access, Transmission, and Storage Policy** available on our Website.

e) Website Security.

The University maintains the Website security using the industry standard techniques, including firewalls, intrusion detection and prevention systems, access control lists and routing protocols.

For more details about the use of our Website, please refer to our **Terms of Use** and **Acceptable Use Policy** available on our Website.

f) Virus and Malware Controls.

The University installs and maintains the latest anti-virus and malware protection software on its Website in place; scheduled malware monitoring and system scanning to protect User´s Information from anticipated threats or hazards and against unauthorized access to or the use of such information.

g) Unauthorized Access and Damage Prevention.

The University implements appropriate written back-up and contingency disaster

recovery and academic and business activities continuity plans. These plans will include processes to ensure recovery of Users' Personal Information that was modified or destroyed due to unauthorized access.

We review both academic and business activities continuity and risk assessment regularly. Academic and business activities continuity and contingency disaster recovery plans are tested and updated regularly to ensure that they are up to date and effective.

We will notify our Users promptly of any unauthorized access or damage to their Personal Information, in accordance with applicable law.

For more details on how we prevent or minimize accidental or intentional unauthorized access or damage to the Personal Information of our Users, please refer to our **Information Security Policy** available on our Website.

8. Data Retention

We keep your information for as long as needed to fulfill the particular purpose for which it was collected. We may also retain your records if legally required, or to fulfill a legitimate interest.

Unless otherwise required by law, the University will also erase Personal Information when it is no longer necessary in relation to the purposes for which it was collected or otherwise processed; when you withdraw your consent (where lawfulness of processing was based on your consent) and there is no other legal ground for the processing; when you object to the processing and there are no overriding legitimate grounds for the processing; when your Personal Information has been unlawfully processed; and when it is necessary to comply with legal obligations.

If you hold an account with the University , then we do not delete the data in your account (Except for Users from the European Union. For more details please see Section 14 below). There are controls in your account where you can edit or delete certain data; however, the University retains any data related to classes you have

taken at the University or treatment you have received at one of the University medical care facilities as they are relevant and necessary in relation to the purposes for which they were collected or otherwise processed.

9. Disclosure or your Personal Information

We may share and/or disclose your Personal Information in accordance with applicable laws. Additionally, we must cooperate with law enforcement inquiries, as well as other third parties to enforce laws, as well as to help protect you and us, and all our Users of any crime or fraud. For this reason, and in response to a verified request by law enforcement or other government officials relating to a criminal investigation or alleged illegal or fraudulent activity, we may (and you expressly authorize us to) disclose the Personal Information we collect from you, in accordance with this Privacy Policy, without a subpoena. However, in an effort to respect your privacy, we will not otherwise disclose your Personal Information to law enforcement or other government officials without a subpoena, court order or substantially similar legal procedure, except when we believe in good faith that the disclosure of information is necessary to prevent imminent physical harm, fraud or financial loss; or report suspected illegal or fraudulent activities.

We are committed to notifying you, as soon as possible, in the event that we receive any legal request from a public authority, including judicial authorities, regarding your Personal Information within the limits established by applicable law.

10. Personal Information Shared with Third Parties

We do not use, share, sell and/or exchange any of your Personal Information with third parties for any purposes without your express consent. However, in order to enable you access to, and/or use our Website and Services, we may share your Personal Information with companies that we hire to perform services or operate on our behalf as our service providers (“Data Processors”). In all cases in which we share your Personal Information with a third party for the purpose of providing you our Services, we will not authorize them to keep, disclose or use your

information with others except for the purpose of providing the services we asked them to provide.

By accepting this Privacy Policy, you expressly give us authorization to use and share your Personal Information with our Data Processors (e.g. Technosolutions, AdRoll, Google Analytics, among others) under their corresponding privacy conditions, within the limits set in this Privacy Policy.

We are not responsible for the privacy and data protection practices of our service providers and/or any third party. However, we warrant that we have used reasonable efforts to determine that our Data Processors have adequate technical and organizational measures in place and are able to satisfy the privacy, security and data protection parameters used by the University.

11. International Transfers of your Personal Information

The Southern Adventist University is a college based in Collegedale, State of Tennessee, United States of America and its servers are located in our country.

We process and store your information in the United States of America. However, our Data Processors may process and store your Personal Information in our country and/or elsewhere.

If you are located outside the United States of America and choose to provide us with your Personal Information, we will transfer such information to the United States of America for due processing and storage, and our Data Processors may process and store your Personal Information in the United States of America and/or any other country. You expressly accept and acknowledge that some States of the United States of America and/or the countries of our Data Processor may not have the same data protection laws as your country or the country in which you initially provided your Personal Information. Notwithstanding, we will always apply this Policy in our country to ensure the privacy and protection of your Personal Information and we will ensure that our Data Processors are aware of this Privacy Policy and we will urge them and make our reasonable efforts to

ensure that they implement the necessary and adequate measures to comply with the privacy, security and data protection parameters set forth herein.

By accepting this Privacy Policy you have expressly given us authorization to transfer your Personal Information to the United States of America and/or to other countries where our Data Processors may be located at, if necessary, to provide you with our Services.

12. Transferable Information Details (EU Residents)

The details of the Personal Information of the European Union ("EU") residents that we may transfer in accordance with Section 11 above are as follows:

- *Data Controller:* The Southern Adventist University.
- *Data Processors:*
    - The Southern Adventist University.
    - Technosolutions.
    - AdRoll.
    - Google Analytics.
    - Other Data Processors.
- *Place*:
    - The Southern Adventist University: Collegedale, Tennessee, USA.
    - Technosolutions: New Haven, Connecticut, USA.
    - AdRoll: San Francisco, California, USA
    - Google Analytics: Mountain View, California, USA.
    - Other Data Processors: Any place these may be located at.
- *Category of Data Subjects*: Visitors, Students, Employees, Board Members and Users.
- *Data Category:* Personal Information.

- *Sensitive Data*: Users information regarding the withdrawal from the Academic Program for medical reasons.
- Frequency of the Transfer: Each time an individual registers on our Website to use our Services.
- *Nature of the Processing:* Collection, process and storage.
- *Purpose of Data Transfer and Processing:* Provide our Services.
- *Data Retention Period:* 1 year in accordance with Section 14 (f) below.

13. Regulations Applicable to U.S. Residents

a) Tennessee Code § 47-18-2107 (Tennessee's Data Breach Notification Law) (Tennessee Residents).

The Tennessee Code § 47-18-2107 applies to any person or business that conducts business in the State of Tennessee, including any agency or its political subdivisions, that owns or licenses computerized data that includes personal information ("Information Holder").

Under the Tennessee Code § 47-18-2107, "Personal Information" means an individual's first name or first initial and last name, in combination with any one (1) or more of the following data elements, when either the name or the data elements are not encrypted:

i) Social security number;

ii) Driver license number; or

iii) Account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account.

Personal Information does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records.

Also, in accordance with that law, "breach of the security of the system" means unauthorized acquisition of unencrypted computerized data that materially compromises the security, confidentiality, or integrity of personal information maintained by the information holder. Good faith acquisition of personal information by an employee or agent of the information holder for the purposes of the information holder is not a breach of the security of the system; provided that the Personal Information is not used or subject to further unauthorized disclosure.

In compliance with the Tennessee Code § 47-18-2107, we will notify any User who is a resident of Tennessee, within forty-five (45) days when its personal information was acquired, or reasonably believed acquired, by an unauthorized person following a "breach of system security".

b) California Consumer Privacy Act (California Residents).

We provide the following additional details regarding the categories of Personal Information about California residents that we have collected or disclosed in the past 12 months, in accordance with the California Consumer Privacy Act (CCPA), as described in this Section.

We collected the following categories of Personal Information:

- Identifiers, such as name, last name, social security number, contact information, online identifiers and any other government-issued ID numbers;
- Personal Information, as defined in the California customer records law, such as name, last name, postal address, signature, and any other information that allows to identify a person individually.
- Commercial information, such as transaction information and commercial history;
- Internet or network activity information, such as browsing history, online behavior, and interactions with our and other websites, applications and systems;
- Geolocation data, such as device location and IP location; and

- Inferences drawn from any of the Personal Information listed above to create a profile or summary about you, such as an individual's preferences and characteristics.

We collect this Personal Information from you and from other categories of sources: information received as part of routine card verification (fraud) checks; social networks; publicly available databases; and joint marketing partners, when they share the information with us.

We share this Personal Information with our service providers, data processors, business partners, auditors, advisors and public or government authorities.

We disclosed the following Personal Information to third parties (such as our service providers, data processors, business partners, auditors, advisors and public or government authorities) for our operational business purposes:

- Identifiers, such as name, last name, social security number, contact information, and any other government-issued ID numbers;
- Personal Information, as defined in the California customer records law, such as name, last name, postal address, signature, and any other information that allows to identify a person individually.
- Commercial information, such as transaction information and commercial history;
- Internet or network activity information, such as browsing history, online behavior, and interactions with our and other websites, applications and systems;
- Geolocation data, such as device location and IP location; and
- Inferences drawn from any of the Personal Information listed above to create a profile or summary about you, such as an individual's preferences and characteristics.

We do not "sell" Personal Information for purposes of the CCPA. For purposes of this Section about CCPA, "sell" means the disclosure of Personal Information for monetary or other valuable consideration but does not include, for example, the

transfer of Personal Information as an asset that is part of a merger, bankruptcy, or other disposition of all or any portion of our business.

If you are a California resident, you may request that we:

(i) Disclose to you the following information covering the 12 months preceding your request:

- The categories of Personal Information we collected about you and the categories of sources from which we collected such Personal Information;
- The specific pieces of Personal Information we collected about you;
- The business or commercial purpose for collecting Personal Information about you;
- The categories of Personal Information about you that we otherwise shared or disclosed, and the categories of third parties with whom we shared or to whom we disclosed such Personal Information.

(ii) Delete Personal Information we collected from you.

We will respond to your request consistent with applicable law. Nonetheless, you have the right to be free from unlawful discrimination for exercising your rights under the CCPA.

(iii) Requests about your Personal Information

If you are a California resident, you may make a request for the disclosures described above or make a request to delete Personal Information we collected from you, by contacting us at: webhelp@southern.edu.

C) California Online Privacy Protection Act (California Residents).

The California Online Privacy Protection Act (CalOPPA) applies to any individual, entity or business operating websites that collect Personal Information from California viewers and/or consumers and/or users.

The CalOPPA defines as "personally identifiable information" the following: first and last name; physical address; email address; telephone number; social security numbers; details of physical appearance (height, weight, hair color); contact information; and any other information stored online that may identify an individual.

For the purposes of CalOPPA, we only collect the following "personally identifiable information" to provide you with our Services: first and last name, physical address, email address; telephone number; social security number; social media accounts; education history; and data included in submitted forms as described in Section 5 above. As to sensitive data collected by us, we only require our Users to inform us when they reactivate their academic program through our Website, whether or not they have withdrawn for medical reasons during their last semester at the University.

Pursuant to CalOPPA, we agree to the following:

- You and any User may visit our Website anonymously.
- There is a link to this Privacy Policy on the footer of the homepage of this Website.
- Our Privacy Policy link does include the word "Privacy'" and may easily be found on the footer of our homepage. It is titled "Privacy Policy" very clearly.
- You will be notified of any Privacy Policy changes on our Privacy Policy Page.

d) Children's Online Privacy Protection Act.

The Children's Online Privacy Protection Act (COPPA) is intended to prevent websites and any online marketers from targeting children with deceptive campaigns that extract Personal Information from children.

For purposes of COPPA, we represent that:

- This Website and Services are not provided and do not exist for a commercial or academic purpose to children under the age of 13;

- We do not in any way collect, any Personal Information from children under the age of 13 on this Website;

- We do not provide our Services to other websites by collecting information from users of websites that are directed to children; and

- We do not process, use, share, store, maintain, and/or disclose any Personal Information from children under 13.

If you are a parent or guardian who has discovered that your child under the age of 13 has submitted Personal Information to us, please notify us at: webhelp@southern.edu. We will promptly delete the information submitted by your child under 13 from our records, once we receive such notification.

e) Controlling the Assault of Non-Solicited Pornography And Marketing Act of 2003 (CAN-SPAM Act).

The Controlling the Assault of Non Solicited Pornography and Marketing Act of 2003 (CAN-SPAM Act), is a U.S. federal law regulating "commercial e-mail" which applies to any individual, entity or business that engage in any advertising/marketing of products or services via e-mail.

The CAN-SPAM Act sets forth the rules and requirements for commercial email and gives recipients the right to prevent or stop the sending of commercial or marketing emails to them.

We collect your email address, name and last name, so we can:

- Send information, respond to inquiries, and/or other requests or questions.
- Process your requests about our Services and to send information and updates pertaining to thereon.
- Send you additional information related to our Services.
- Market to our mailing list or continue to send emails to you after any transaction.

- Email you free information and advertising certain Services we offer.

In compliance with CAN-SPAM Act, we agree to the following:

- We will not use false or misleading subjects or email addresses.
- We will identify the email message as an advertisement in some reasonable way.
- We will include our business mailing address and/or physical address in our emails.
- We will monitor third-party email marketing services for compliance.
- We will honor opt-out/unsubscribe requests quickly.
- We will allow Users to unsubscribe by using the appropriate link at the bottom of each email.

How to unsubscribe to our emails:

If at any time you would like to unsubscribe from receiving future emails, you may email us at webhelp@southern.edu or follow the instructions at the bottom of any email you receive from us and we will promptly remove you from future correspondence(s). If you experience any problems unsubscribing, please email us to that email address listed here and we will promptly handle your removal.

14. General Data Protection Regulation (European Union Residents)

If you are located within the European Union or if you are a citizen of any member country of the European Union, you are entitled to the following rights under the General Data Protection Regulation ("GDPR"):

a) Right to be Informed.

You have the right to be informed about the collection, use and disclosure of your Personal Information. For this reason, this Privacy Policy describes and explains how we collect, use and may disclose your Personal Information.

b) Right to Data Access and Portability.

You may issue queries or ask questions about your Personal Information by email at any time, and we will provide you with such information in a structured, commonly used, machine-readable format, or (where technically feasible) to have it ported directly to another data controller, provided this does not adversely affect the rights and freedoms of others.

c) Right to Data Rectification.

You have the right to ask us to update and/or rectify and/or complete your inaccurate or incomplete Personal Information. Please keep in mind that notwithstanding that all reasonable efforts will be made by us to keep your Personal Information updated, you are kindly requested to inform us promptly of any change, error or inaccuracy in your Personal Information.

d) Right to Data Objection or Restriction (Opt-Out).

You have the right to object, suspend or withdraw your consent to the processing of your Personal Information when you have a legitimate interest (or those of a third party) and there is something about your particular situation that causes you to object to the processing because it makes you feel it impacts your fundamental rights and freedoms. Please note that we only process your Personal Information when this is necessary to provide you with the Website Services and/or when it is necessary to comply with a legal obligation to which we are subject to, as when processing is necessary to protect your interests or those of another person or entity.

e) Right to Data Deletion

You have the right to ask us to delete your Personal Information when it is not relevant to the purpose for which we collect it, once the period set forth in paragraph "f" below has elapsed. We may delete your Personal Information before the expiration of that period, when such information is not necessary, at our sole discretion. However, please note, there may be legal obligations which may prohibit us from deleting all or part of the Personal Information

held about you immediately at the time of the request, however, we will process your request at the earliest opportunity whenever the data retention period expires in accordance with paragraph “7”below.

f) Data Retention Period

The University will retain your Personal Information only for as long as is necessary for the purposes set out in this Privacy Policy, but for a limited period of time that may not exceed one (1) year, since the cancellation of your User Account for any reason.

We will retain and use your Personal Information to the extent necessary to comply with our legal obligations (for example, if we are required to retain your data to comply with applicable laws), resolve disputes and enforce our legal agreements and policies.

g) How to Exercise Your Rights?

You may exercise the rights described in this Section 14, at any time, by contacting us at: webhelp@southern.edu or by contacting the competent regulatory authority of your country. Please note that we will verify your identity prior to responding to any request.

We try to respond to all legitimate requests within 5 business days. Please keep in mind that occasionally it may take us longer if your request is particularly complex or you have made a number of requests. In this case, we will notify you and keep you updated on the status.

15. Emails and Newsletters

We will send emails and newsletters to our Users, from time to time, to let you know about our degrees, academic activities, services and important improvements and updates to our Website and Services. You will be able to opt out of these emails and newsletters at any time by clicking the unsubscribe option (opt-out), available at the end of such emails. However, we may send you other necessary emails as system notifications for security reasons (e.g. passwords resets, logins from new devices, etc.) which not be deactivated by you.

If you would like additional assistance on how to opt out of receiving email messages, then please contact us at webhelp@southern.edu.

By accepting this Privacy Policy, you expressly agree to receive the information described above, and also expressly accept receiving our ads.

16. Social Media Content and Sharing

Some pages on our Website display social media content. “Sharing” features of social media content furnish anonymous browsing data (for Users not logged in to social media services) and/or personally identifiable data (for Users logged in to those services).

We may use social media plug-ins on our Website to enable you to easily share information with others. We use the information collected from the plug-ins to learn about your interests and to help us better understand how to serve you. This information may include your preferences about how to contact you or further develop a business or professional relationship with you, your product preferences, languages, marketing preferences, and some demographic data. These plug-ins may include those from companies like Instagram, Twitter, Facebook, YouTube, and LinkedIn. The social media plug-ins may allow these companies to receive directly identifiable Personal Information about you and your visit to our Website.

When you visit our Website, the operators of the social media plug-ins on our Website place cookies on your computer that enable them to recognize you on websites belonging to them and their affiliates and partners after you have visited our Website, or that enable them to add the information collected from your visit to our Website with your prior activity on those websites. The social media plug-ins collect this information about users whether they specifically interact with the plug-in or not, and it may enable social media companies to share information about your web-browsing navigational information with some of their other Users.

The University does not control what information is collected by the social media plug-ins or the information practices adopted by those social media companies.

For more information about social plug-ins from social media websites, you should refer to those companies' privacy and data sharing statements.

By accepting this Privacy Policy, you are giving us your consent to use social media plug-ins to share content and/or Personal information in accordance with this document.

17. Cross-Tracking Devices

The University uses data analytics companies, advertising networks, or social media companies, and features offered by Google Analytics services or pixels such as from Facebook and LinkedIn to engage in "Cross-Device Tracking," which occurs when platforms, publishers, and advertising technology companies try to connect a user's activity across smartphones, tablets, desktop computers, and other connected devices. The goal of cross-device tracking is to enable companies to link a user's behavior across devices.

By accepting this Privacy Policy, you are giving us your consent to use Cross-Tracking Devices on our Website in accordance with this Privacy Policy.

18. Google Analytics

We use Google Analytics to measure the web traffic on different parts of our Website to improve it. Google Analytics, which anonymously tracks users who have JavaScript enabled, uses technical tools like first-party cookies and JavaScript code to collect information about your interactions with our Website. The tracking information may include detailed data about what you do on our Website, such as the web pages you visit and for how long and the websites you visited directly before and after coming to our Website.

We use information from Google Analytics to administer and update our Website, assess whether our Users match the expected Site demographics, and determine how key audiences are navigating the content. Google and its wholly owned subsidiaries may retain and use, subject to the terms of its Privacy Policy (located at https://policies.google.com/privacy or such other URL as Google may provide from time to time), information collected in your use of the Google Analytics

Information Disclosures and Sharing. Google Analytics offers website visitors the ability to prevent Google from recording, processing, and using the data generated by the Google Analytics cookies. Our use of Cookies is described in Section 19 below

By accepting this Privacy Policy, you are giving us your consent to use Google Analytics on our Website in accordance with this Privacy Policy.

19. Cookies

A Cookie is a small text file that websites store via browsers on each user's devices, upon prior consent, when they visit any website. Cookies are widely used in order to make websites work more efficiently and provide a better service and web features for their users. Cookies allow websites to identify and track their users, enabling them to recognize the user´s needs and preferences as well as provide them with security features.

Our Website uses "First Party Cookies" set up by us, and "Third-Party Cookies" set up by our service providers and advertisers. Cookies and their use are described below.

a) First-Party Cookies.

These Cookies are directly stored by our Website. These Cookies allow us to collect analytics data, remember Users settings, and perform other useful functions that provide a good experience to our visitors and Users (e.g. Strictly Necessary Cookies; Performance Cookies; and Functionality Cookies).

b) Third-Party Cookies.

These Cookies are created by third party websites that are not our Website, including but not limited to our service providers and advertisers. These types of Cookies are usually used for online-advertising purposes and placed on any website through a script or tag. A Third-Party cookie is accessible on any website that loads the third-party server's code. (e.g. Targeting Cookies).

The Third Party Cookies we use on this Website are as follows:

Service Provider	Purpose	Details
Slate by Technosolutions	Customer relationship management (CRM), To track Users activity on our Website.	https://technolutions.com/
AdRoll	To match the IP address and email address of our Users to advertise on their social networks and track them while they are on our Website.	https://www.adroll.com
Google Analytics/Tag Manager	To track the behavior of our users on the Website.	https://analytics.google.com

c) Consent.

When you first visit our Website we will require your consent to continue with the use of Cookies. By Clicking "Accept" when you first access this Website you are giving us your consent to use First-Party Cookies and/or Third-Party Cookies on our Website in accordance with this Privacy Policy.

d) Cookies Purpose

We use Cookies to:

- Identify you when you use our Website and Services;
- Provide our Services;
- Store information about your preferences and personalize our Services;
- Implement security measures to protect your Personal Information, including the prevention of fraudulent use of login credentials, and to protect our Website and Services;
- Display advertisements that will be relevant to you; and

- Analyze the use and performance of our Website and Services.

e) Cookies Control

You may easily control Cookies usage through your browser settings. The help function in your preferred browser should provide you with the correct information. You may also visit the following website to obtain further information on Cookies and how to manage them: www.all aboutcookies.org.

20. Changes to this Privacy Policy

The University reserves the right to modify all or part of this Privacy Policy at any time. The modified Privacy Policy will be published on our Website and will become effective five (5) business days following its publication on our Website. In case you do not agree to such changes, you must indicate so by sending an email to: webhelp@southern.edu within five (5) business days following such publication, in which case you must leave the Website immediately and also suspend the use of our Services.

Upon expiration of the term above, it will be understood that you accepted such modifications made to this Privacy Policy.

21. Governing Law and Jurisdiction

This Privacy Policy shall be governed by and construed in accordance with the applicable federal laws in the United States of America and with the law in force in the State of Tennessee, States United of America, without regard to conflict of laws provisions. In case of any Dispute, you expressly agree to submit to the exclusive jurisdiction of the Courts of Nashville, State of Tennessee, United States of America.

22. Comments or Questions

For any questions, comments, or complaints regarding this Privacy Policy, you may address us by sending an email to: webhelp@southern.edu and that email

receipt must be acknowledged by us, and in the event that delivery fails, notice can be sent by mail to the address mentioned below:

Southern Adventist University.
4881 Taylor Circle Collegedale, TN 37315,
United States of America.

23. Definitions

- *"Acceptable Use Policy"* means the document that governs the use of the Southern Adventist University's Network, including standards for appropriate and fair use of networking resources and for the protection, security and privacy of user information on that network.

- "Account" and / or "User Account" means the account that is created for each individual when registering on this Website. For the purposes of this document, "User Account" and/or "Account" refers to the User Account created by any individual on the Website, whether or not a student, employee or board member of the Southern Adventist University.

- *"Data Controller"* means any legal or natural person, agency, public authority, or any other entity who, alone or when joined with others, determines the purposes of any personal data and the means of processing it.

- *"Data Classification, Access, Transmittal, and Storage Policy"* means the document that governs the access, classification, access, transmittal, and storage of information provided to the Southern Adventist University by its students, alumni, faculty and staff.

- *"Data Processor"* means any natural or legal individual, entity, public authority, agency or entity which processes personal data on behalf of the Data Controller.

- *"Device"* means smartphones, tablets, laptops, desktops and any other similar digital or electronic equipment.

- *"Employee Computer and Internet Policy"* means the document that governs the employees' use of computer and Internet resources at Southern Adventist University.

- *"Information Security Policy"* means the document that establishes the requirements necessary to prevent or minimize accidental or intentional unauthorized access or damage to Southern Adventist University information resources.

- *"Personal Information"* means any information which is related to an identified or identifiable natural person (e.g. name, last name, address; email address, phone number, social security number, among others).

- *"Privacy Policy"* means this document that governs the privacy practices and data protection of the Southern Adventist University.

- *"Services"* means services provided by the Southern Adventist University through its Website.

- *"Service Provider"* means any natural or legal individual, entity, public authority, agency or entity which provides its services as Data Processor to the Southern Adventist University.

- *"Southern Adventist University" and/or "University" and/or "We" and/or "Us"* means a Seventh-day Adventist college based in Collegedale, Tennessee, United States of America, along with its Website and Services.

- *"Southern Account"* means the User Account created on the Website for students, employees or board members of the Southern Adventist University.

- *"User" and/or "Users" and/or "You"* means any person registered on this Website to use the Website Services provided by the University. For the purposes hereof "User" and/or "Users" and/or "You" shall mean indistinctly any Student, Employee or Board Member registered on this Website.

- *"Terms of Use"* means the document that governs the use of this Website and Services.

- *"Website"* means https://www.southern.edu.