Riverview Seventh-day Adventist Church

Information Technology/Computer Use and Security Policy

Approved by Riverview SDA Church Board on October 16, 2017

PURPOSE

Riverview Seventh-day Adventist Church (Church) has an information technology and computer use policy to outline acceptable use of computer equipment and electronic communication systems provided for use by employees, church officers and volunteers. The policy is designed to:

1. Acknowledge that use of Church-owned technology systems constitutes a representation of the Church, its values, teachings, standards and reputation.
2. Ensure that Church-owned technology and communication systems are used for the ministry purposes of the Church, are secure and that any personal information collected by the Church is used only for appropriate Church purposes.
3. Protect both the Church and the technology/communication system user. Violation of the policy may be grounds for disciplinary action including loss of access to or use of the system and any stored information and may lead to other disciplinary measures available to the Church. Violation of some policies may also call for additional legal or civil actions.

POLICY APPLICATION

This policy applies to all individuals who use computer equipment and electronic communication systems provided by the Church for use in the administration, programs, and records of the Church. This policy also applies to anyone who is granted access to privileged and personal information or who manages the Church website information or who may be involved in creating intellectual property belonging to the Church.

POLICY ADMINISTRATION

The Church Board is responsible for oversight, management and interpretation of the policy. Persons who are authorized to use Church computers and electronic communication systems shall indicate an understanding and acceptance of the policy. The Church Board shall address questions that arise concerning compliance or noncompliance with this policy. The Church Board may make appropriate amendments to the policy at any Church Board meeting provided there has been prior consultation with those to whom this policy applies.

TERMS OF THE POLICY

1. **Ownership of equipment**: Computers and other technology equipment purchased by the Church remain the property of the Church unless otherwise determined by action of the Church Board.

2. **Software**: Only authorized and licensed software, approved by the Riverview SDA Church Network Management Team, will be used on Church-owned computers and related hardware including printers, scanners, cameras or other devices.

3. **System access**: Employee/church leader access to the Church technology system will be login name and password protected. Access granted to an individual does not include the grant of access to family members or friends. Passwords are not used to protect a user's privacy but to ensure security of the system, the network and any stored information. Users of the Church's technology system must comply with all licensing, copyright and intellectual property laws.

4. **Protection of personal information**: The Church is committed to maintaining the accuracy, confidentiality and security of all personal information in its possession.

    a. Each Board, committee, employee, leader or volunteer is responsible for maintaining and protecting the personal information under its control and is accountable for such information to the Board.
    b. The Church collects and uses personal information to enable communication; to compile membership records; to provide income tax receipts and to meet statutory and regulatory requirements. The Church will only disclose personal information to third parties in fulfillment of the purposes identified above, or as required by law.
    c. Unless indicated otherwise, provision of personal information on official Church forms constitutes consent for the Church to collect, use and disclose personal information for the purposes stated above. An individual may refuse or withdraw consent at any time for the Church to store and use personal information by written notice to the person serving as secretary in the Church office.
    d. The Church will make reasonable effort to ensure that personal information is accurate, complete and current. Inaccuracies will be corrected promptly when new information is supplied. The Church relies on its members to ensure that information such as mailing address, email address and telephone number details are accurate.
    e. The Church uses appropriate security safeguards to protect personal information from risks such as loss, misuse, unauthorized access, disclosure, or alteration. Safeguards include physical, administrative, and electronic security measures.
    f. Church members have the right to know of the existence and use of their personal information and by written request to the person serving as secretary in the Church office may request such details.

5. **Use of personal devices for Church-related business**: A Church employee may use personal devices (cell phone, computer, etc.) in accomplishing his/her responsibilities as an employee. However, the Church employee shall ensure that e-mails and their replies, generated in the course of work for the Church shall also be stored on the Church server under the employee's assigned e-mail address. Therefore, any e-mail related to Church business must include the employee's assigned Church email address.
   An employee who uses personal devices to create Intellectual property (see #9 below) that rightfully belongs to the Church shall ensure that the material in question is also stored on Church-owned equipment. Text messages originating on personal devices will not be considered as Church property. However, anyone generating text messages should realize that these messages are stored or kept by the service provider so that if needed, the equipment owner or a

subpoena holder can require the cell service provider to give copies of text messages as requested.

6. **Unauthorized activity and disruption of system features**: Any unauthorized activity may be treated as a hostile attack against the Church. Users of the Church's technology system must not knowingly attempt to disable, defeat, overload, or circumvent any enterprise security implementation. Effecting security breaches or disruptions of network communication. Security breaches include but are not limited to, access data of which the employee is not an intended recipient or logging into a server or account that the employee is not expressly authorized to access, unless these duties are within the scope of regular duties. For purpose of this section, "disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes. Port scanning or security scanning is expressly prohibited. Executing any form of network monitoring to intercept data is prohibited.

7. **Internet access**: The use and provision of the Internet is for Church purposes and not for self-entertainment.

8. **Social media and social networking**: The Church technology system user's online presence reflects the Church at all times. Actions captured via images, posts, or comments can reflect that of the organization. Therefore, the Church has adopted the following social media and social networking policy. The absence of, or lack of explicit reference to a specific site does not limit the extent of the application of this policy. Where no policy or guideline exists, employees should use their professional judgment and take the most prudent action possible. (Consult with the chair of the Technology Committee if you are uncertain.)
    a. Personal blogs should have clear disclaimers that the views expressed by the author in the blog is the author's alone and does not represent the views of the employer. Be clear and write in first person. Information published on blog(s), whether personal or professional, should comply with the employer's confidentiality and disclosure of confidential information policies. This also applies to comments posted on other blogs, forums, and social networking sites.
    b. Unless the user is engaging in social networking for the specific purpose of promoting the Church the user should refrain from listing the Church on any blogs, social networking or other non-business related internet sites.

9. **Intellectual property**: The Church shall follow the intellectual property policies of the North American Division of the General Conference of Seventh-day Adventists. (See North American Division Working Policy BA 70 25 or any currently valid amendment.) Under this policy, the Church is owner of any work prepared on the job by an employee. The Church has no obligation for royalty or reimbursement for any work prepared on the Church's equipment. Sermon files and graduate study materials are exempted from this policy. Exemptions from any portion of this policy must be approved by the Church Board.

10. **Policy compliance**: The Church reserves the broadest right to inspect and monitor computer and network equipment, Internet usage, email, and other electronic information and files for appropriate usage and content consistent with this policy. Users should have no expectation of privacy. Church equipment must not be used for outside business ventures, personal solicitation, political campaigns or causes that oppose or contradict the mission and values of

the Church. Church computing resources, software, systems and network must not be used to violate any local, state and/or federal laws. The Church will cooperate with investigations by any legitimate law enforcement entity. Church computer equipment and networks shall never be used to create, display, store or transmit illegal, inappropriate, derogatory, harassing or offensive material.

11. **Revisions to this policy**: Development of this policy is an on-going process due to changes in technology or use of electronic information systems. Accordingly, this policy may be changed from time to time by action of the Church Board.