**Information Technology Systems Policy**

**of**

**Chesapeake Conference of Seventh-day Adventists**

Effective Date: August 22, 2017

## Section I – General Statement

Information Technology Systems (ITS), when properly used, provide timely communication and technological support to help fulfill the mission of the Church. This policy contains principles and practices designed to ensure that Information Technology Systems are used in ways that are consistent with the mission of the Chesapeake Conference (Conference) and will deter the use of the Systems for illegal, immoral, unethical, or otherwise inappropriate, purposes.

## Section II -- Policy Application

This policy applies to all employees of the Chesapeake Conference and all persons who, as volunteers, use Chesapeake provided ITS, or are guest users as described in this policy.

## Section III - Definitions

1. *Information Technology Systems* include, but are not limited to, computers, computer networks, PDAs (personal digital assistants), fax machines, telephones (land lines and mobile), mobile devices including tablets, voice mail, audio and video teleconferencing devices, video equipment, software, operating systems, storage media, network accounts providing electronic mail, electronic handheld devices, photocopy machines, postage machines, printers, and typewriters owned by the Conference, its entities, or institutions.

2. *"Conference,"* as used in this policy, refers to all entities of Chesapeake Conference, i.e., churches, church schools, retreat center, commissions, councils, committees, task forces, boards, advisory boards, entities and other institutions that are sponsored by, or affiliated with, the Conference.

3. *Users of ITS* are the persons described above under "Policy Application" of the Chesapeake Conference.

4. *Guest Users* of the ITS are those who are outside consultants or contracted by the Conference such as, vendors, technicians or other persons allowed to access ITS, but are not employed by Chesapeake.

5. *System Administrator* is a User responsible for monitoring the functioning of the ITS for the Conference. The System Administrator is appointed by the Conference.

6. *Guest System Administrator* is a Guest User that is an outside consultant or contractor entrusted with the responsibility for monitoring the functions of the IT system.

7. *Administration* refers to the Conference Administrative Committee and/or members thereof.

8. *Directives* are the policies and guidelines issued by the Conference.

**Section IV -- General Policy applying to the Conference**

Article 1 - General Provisions

1. Information Technology Systems and equipment purchased or provided by the Conference for its related entities, schools, and institutions, and all information, messages and files created with the aid of the ITS in the performance of the ministry and business of the Conference are the property of the Conference.

2. The Conference may develop Directives that are specific to its mission and operation. Such Directives must be consistent with the ITS Policy.

3. Users who violate the policy may face suspension of ITS privileges and/or other disciplinary action up to and including reassignment, termination of employment or volunteer position, and other discipline as deemed appropriate.

Article II- Acceptable Use

1. Information Technology Systems are to be used for business and ministry purposes. The Conference allows minimal, occasional or incidental personal use of ITS (sending or receiving) for non-business purposes. Personal use must not in any way interfere with, or impede, the Conference's mission, must be occasional and minor, must be promptly discontinued at the request of Administration, and is expressly subject to all the provisions of this policy.

2. Users who use ITS for personal communications without permission are subject to Administrative discipline, including the restriction or loss of ITS privileges.

Article III - Unacceptable Use

1. Creating or issuing personal communications that appear to be an official communication of the Conference without proper authorization.

2. Using ITS in such a way that it interferes with the employee's productivity or creates unnecessary expense or violates the Directives of the Conference.

3. Disseminating or intentionally accessing material that is considered defamatory, abusive, obscene, profane, sexually suggestive, pornographic, harassing, intimidating, threatening, racially offensive, illegal, gambling related, fraudulent, or otherwise inappropriate or illegal written, recorded, or electronically retrieved or transmitted communication; nor shall the user encourage the use, sale or distribution of controlled substances or other illegal activity. Administration may exempt those persons whose job may necessitate access to such material for investigative purposes, including when a System Administrator conducts a compliance check.

4. Disseminating the Conference's confidential information to persons, organizations or agencies, including other entities sponsored by the Conference, unless authorized by the Administration. Confidential information includes all information that is not generally available to the public, including but not limited to, financial information, personnel files, personal information provided by members of the church, or any information deemed confidential.

5. Hacking or attempting to gain illegal or unauthorized access to secured or restricted sites.

6. Deliberately damaging, modifying, or tampering with computers or other ITS components.

7. Violating copyright laws, including the acquisition, use, or distribution of pirated software.

8. Downloading proprietary materials or information (e.g., trademarked or patented materials, copyrighted music, videos, etc.) without the owner's permission, or proper licensure.

9. Using someone else's Username or password (except as provided under Required Best Practices).

10. Trespassing in another User's folder, files, or work, unless searching in another Users' folder, files or work is authorized by an Administrative Authority for purposes of obtaining information needed to conduct the business of the Conference or for monitoring or inspection purposes.

11. Using the ITS for commercial purposes, private financial or commercial gains, commercial or private advertising, product advertisement, nor for the establishment of personal web-pages or social media accounts. Unauthorized personal "chat," or chain letter communication is also prohibited.

12. Intentionally introducing a virus, worm, Trojan horse or other code that will disrupt ITS.

13. Changing ITS settings unless authorized by an ITS System Administrator.

14. Installing software or hardware unless authorized to do so by the ITS System Administrator.

15. Downloading entertainment software or games, or playing computer games on Conference owned devices or on the Internet.

16. Downloading images or videos unless there is an explicit business-related use for the material.

17. Political lobbying, or making social announcements not related to the Conference or Conference entities.

18. Removing ITS equipment from the premises without the express permission of Administration. Equipment designated for check out (e.g. projectors, projection screens, laptop computers, netbooks, tablets and related peripheral equipment) is exempted.

19. Removal of printed paper-based confidential information from the premises of any Conference entity is not allowed without the authorization of Administration. Confidential information in electronic format can be removed from the premises provided the documents are stored in an approved, secure USB storage unit.

20. It is not acceptable to store files of the Conference or related church entities and institutions on any non-Conference authorized computer or other storage device at any time.

21. Using personal email accounts to send or receive information related to the business of the Conference, and associated Conference entities and institutions is discouraged, but may be allowed as circumstances dictate.

22. Using ITS equipment or systems in a manner that would result in violations of other Conference policies is not permitted.

Article IV - Access and Privacy

1. All electronic communications should be crafted with care and the understanding that all such communications are subject to monitoring by Administration, could be subject to monitoring by outside agencies, and may be subject to third-party legal disclosure and subpoena.

2. Users must maintain the secrecy of their passwords. Emergency access procedures are described under Required Best Practices. It is, however, understood that the purpose of passwords is for network security and not for the personal privacy of a user.

3. Administration may authorize access to all files stored in private areas of the network and hard drives, discs, and other storage devices to assure compliance with the policy and Directives.

4. Administration may authorize an outside consultant or contractor to access components of the ITS if such access is necessary for the consultant or contractor to perform a service for the Conference. These Guest Users or Guest System Administrators are expected to comply with the provisions of Article IV of this policy when using ITS components owned by the Conference and its associated entities

5. The System Administrator may authorize an outside technician or consultant to access ITS for the purposes of maintenance, repair, or evaluation with the authorization of Administration.

Article V - Compliance

Administration may authorize random compliance audits which may include access to any component of ITS at any time, with or without notice to the User.

**Section V -- Best Practices**

Article I - General Provision

Administration is free to develop or oversee the development of Best Practices specific to the Conference, and entities or institutions sponsored by the Conference, for which the Administrative Authority is responsible.

Article II - Required Best Practices

1. Install antivirus software (a function of ITS personnel or authorized agents).

2. Install and maintain a firewall for networks (as initiated and directed by ITS personnel).

3. Implement a data and equipment back-up, retention and destruction plan that provides for an orderly, cost effective, and secure back-up, storage and eventual destruction plan for all data and equipment. Contact the Conference IT Team for consultation to set up a plan.

4. To provide emergency access to accounts. Each User should write out his/her user name and password for his/her Conference owned devices, place it in a sealed envelope and place the envelope in a

secure place where Administration can access it if necessary. Emergencies include the death or incapacitation of the User.

5. Users using a personally owned home computer for job related purposes must meet Conference minimum security standards, including current anti-virus and anti-malware protection to minimize/prevent cross-contamination and infection of the Conference network.

Article III - Recommendations for Best Practice

1. Administration is urged to implement recommendations for Best Practices to the degree that the recommendations address the needs of the Conference and entities or institutions sponsored by the Conference.

2. Use care in creating email messages as the contents are neither private nor confidential. Even when a message has been deleted it may still exist on a back-up system, be restored, be printed out, or may have been forwarded to someone else without the creator's knowledge. Email messages may be subject to third-party legal disclosure.

3. Do not install personally owned hardware or software without the authorization of the IT Team or the System Administrator.

4. Refrain from downloading or sending/forwarding unsolicited advertisements, cute stories, cute pictures, videos, jokes, free screensavers and desktop backgrounds, emoticons, and other "free," or paid products as they often contain spyware, malware, viruses, or other harmful code, or code fragments.

5. Do not allow guests, including children, to use an office computer or other ITS device as entertainment. System security could be compromised.

**Article IV - Policy Acknowledgement**

By signing this document, I affirm having received it, and confirm that I have read it and agree to comply with the terms of the Information Technology Systems Policy of the Chesapeake Conference of Seventh-day Adventists.

_____

_____ _____

Signature and Title/Position Date

_____

Printed Name