

Diocese of Nova Scotia and Prince Edward Island
HR Policy 2.1.28: Technology and Internet Acceptable Use Policy

A. PURPOSE

Diocesan Office Staff (Lay and Clergy)

The efficient operation of the Diocese of Nova Scotia and Prince Edward Island (*the Diocese, Diocesan*) requires an ongoing investment in technology infrastructure, its configuration and support. **Hardware, software, CD/DVD resources, access to the Internet, electronic mail, and other technologies are provided to users for the accomplishment of the work of the Diocese.** Decisions concerning the appropriate use of various technologies are made with this primary consideration in mind.

B. OVERVIEW

The defining nature of technology is that it is constantly evolving. Establishing and maintaining such an environment has become significantly more complicated as the capabilities of technology have expanded. Decisions concerning the appropriate use of the technology are influenced by four major considerations:

1. to safeguard the confidentiality of Diocesan work and clients;
2. the protection of the Diocesan technology environment from both malicious and unintended attacks on its infrastructure from computer viruses and unauthorized access;
3. the maintenance of a stable computing environment in which the various systems and devices are always available for use (with reasonable exceptions); and,
4. ensuring that all applications and content stored on Diocesan resources are legally obtained and licensed.

The rise in the number and sophistication of various Virus, Malware, and Hacking approaches requires that the Diocese limit the use of its technology and Internet access by individuals for business use only. The Diocese will endeavor to provide access for personal use but not through any device connected directly to the Diocesan Computer Network. Personal access to **all Social Media**, except where required for purposes directly related to the work of the Diocese, is prohibited. Similarly, utilizing Diocesan resources to browse the Internet for non-work-related purposes is prohibited. **The implications to the Diocese with regards to confidentiality and lost productivity are so significant that failure to adhere to this policy may be considered grounds for dismissal.**

The Internet is a worldwide network of computers containing billions of pages of information and many diverse points of view, including material that is inappropriate, offensive, and, in some cases, illegal. The Diocese does not want to control or restrict access to this information for legitimate operational purposes. Users of Diocesan technology resources and Internet access are notified that they are responsible for the material they review, download from the Internet, and/or store on Diocesan computers.

This *Technology and Acceptable Internet Use Policy* covers various circumstances regarding the use of Diocesan technology and Internet access. As technology progresses, users will encounter circumstances that are not clearly covered in the Policy. In such circumstances, users should consult with the Executive Director before proceeding with the intended activity.

C. ACCEPTABLE USE

1. **Primary Purpose of Technology Infrastructure:** The primary purpose of the Diocese' technology and Internet access is for the accomplishment of the work of the Diocese. Users are provided with technology and Internet access to assist them in the accomplishment of their work. Equipment and access is owned by the Diocese and may only be used for authorized purposes by users at the Diocese.
2. **Communication Standards:** Established policies concerning professional standards of communication,

Diocese of Nova Scotia and Prince Edward Island
HR Policy 2.1.28: Technology and Internet Acceptable Use Policy

confidentiality, and form of presentation of materials are not to be adversely affected by the utilization of current technologies. For example: the nature and content of communication by email can very easily slip into the familiar mode. Professional relationships and the established standards of communication with clients should be maintained despite the ease of response facilitated by email. It is important that all communications adhere to Diocesan standards for form and content as outlined in the *Confidentiality and Non-Disclosure Agreement* (Policy 2.1.27).

- 3. Security of Electronic Communication:** Electronic communication is not secure and is discoverable. Accordingly, all electronic communication should be composed as if the person you would least like to view it will, in fact, have opportunity to view it.
- 4. Professional Standards:** The Diocese has expectations relating to standard of dress, appearance of office space, etc. In similar fashion computer systems shall reflect professional standards in the appearance of screen backgrounds, screen savers, sound themes, etc. As in other areas of the maintenance of Diocesan policies, the Executive Director will establish acceptable standards and be responsible for their enforcement.
- 5. Installation of Software:** Installation of any software, game, enhancement, or other program from installation media (Floppy Disk, Zip Disk, CD/DVD, USB Drive, etc.) or download from the Internet is not permitted without the approval of the Executive Director. This approval is to be sought only after securing the endorsement of your immediate supervisor.
- 6. Email and Email Attachments:** Files received attached to email messages with the extension “.com”, “.vbs”, “.msi”, and “.exe” are program files and should be reviewed by the external technology consultant of the diocese before being opened or installed. Email attachments should not be opened unless the user is reasonably sure of their origin. Email messages which state that the attached file is “*free from viruses*” should not be opened under any circumstances. Receipt of any such messages should be reported immediately to the external technology consultant of the diocese.
- 7. Installation of Hardware and Peripheral Devices:** Installation of any hardware or peripheral device is not permitted without the approval of the Executive Director. This approval is to be sought only after securing the endorsement of your immediate supervisor.
- 8. Care and Use of Hardware:** Users are responsible to take reasonable care to ensure that food or beverages are not spilled onto the various hardware components.
- 9. Virus Infection Reports:** all notifications regarding virus infection should be reported to the Executive Director and external technology consultant of the diocese, immediately.
- 10. The following are considered Prohibited Activities:**
 - a. The use of Diocesan resources to send, receive, display, print, or otherwise access and disseminate material that is fraudulent, harassing, illegal, embarrassing, sexually explicit, obscene, intimidating, defamatory, racist, or other material that may be deemed undesirable by the Diocese from time to time.
 - b. The use of Diocesan resources for accessing and engaging in chat groups, utilizing IRC, ICQ, Skype, Facebook, Instagram, Twitter, personal Internet browsing, Skype and other long-distance phone calling for personal business, etc. The Diocese provides **Public WiFi** (not the secure, password protected Wifi) access that users can utilize to undertake such activities on their personal devices, phones, tablets. etc. The Public WiFi is outside the Corporate Network and so these personal activities do not pose a risk to Diocesan IT infrastructure.

Diocese of Nova Scotia and Prince Edward Island
HR Policy 2.1.28: Technology and Internet Acceptable Use Policy

- c. Accessing such devices as Internet Radio, Streaming Video, and other such content that requires an ongoing link to a web site except for business purposes as authorized by the Executive Director.
- d. Installation of such applications as Limewire, BitTorrent, MicroTorrent, other “content players,” “download software” and Torrent software and storing the associated content files.
- e. Due to the risk of cross-device infection Personal Electronic Devices (Phones, Tablets, etc.) are prohibited from being connected to the Diocese computers via USB Cables for charging or data transfer. Charging at work should only be accomplished via the use of AC Power plugged in charging devices.
- f. Use of Diocesan resources and Internet access for commercial or personal advertisements, solicitations, promotions, or other business activities not related to the accomplishment of the work of the Diocese.

11. Copyrighted Materials: Diocesan resources are not to be used to download or distribute copyrighted materials except where permission to do so has been obtained.

12. Compliance With Applicable Laws and Licenses: Users must comply with all software licenses, copyrights, and all other Provincial and Federal laws governing intellectual property and online activity. No Diocesan licensed software or License Keys are to be copied or installed onto computers outside of the Diocese.

13. Waiver of Privacy: The Diocese maintains the right to monitor the use of the Diocese’ technology and Internet access to ensure compliance with the terms of this Acceptable Use Policy. The Diocese has the right, but not the duty, to monitor any and all aspects of its technology infrastructure, including, but not limited to, monitoring sites accessed through the Diocese’s Internet access, monitoring chat and news groups, reviewing material downloaded and uploaded, and reviewing email sent and received by users. Users waive any right to privacy in anything they create, store, send, or receive on Diocesan computers or the Internet. Users are further notified that they should have no expectation of privacy of personal electronic data anywhere within the Diocese’s technology infrastructure.

14. Inter-Personal Privacy: The Diocese expects that users will respect each other’s privacy and limit their review of other user’s email, phone messages, schedules, documents, etc., except as required in the performance of assigned duties; for example, review of email while on vacation.

15. Diocesan Data Storage: All work-related data should be stored on Server or Cloud Storage Drives in order to ensure the data is backed up and not lost to the Diocese in the event of system failure or disaster. No data should ever be stored locally, solely, on the user’s computer Desktop, *My Documents* or the local computer’s *Drive C* .

16. Responsibility for Personal Data: The Diocese is not responsible for information of a personal nature which may be stored on Diocesan resources.

17. Disclaimer of Liability: The Diocese is not responsible for any damages, direct or indirect, arising out of the inappropriate use of its technology or Internet resources by Diocesan users.

Signature of Compliance on following page.

Diocese of Nova Scotia and Prince Edward Island
HR Policy 2.1.28: Technology and Internet Acceptable Use Policy

Compliance Agreement

I _____ have read and agree to comply with the rules and conditions of this Policy governing the use of Diocese of Nova Scotia and Prince Edward Island computer, technology, Internet, and other on-line resources (Policy 2.1.XX Technology and Acceptable Internet Use). I agree to adhere to this policy and will ensure that employees and volunteers working under my direction adhere to this policy. I understand that if I violate the rules set forth by this policy, I may face disciplinary action up to and including termination of employment or service.

Name Printed

Signature

Date

Witness

Date