ANGLICAN DIOCESE OF ISLANDS AND INLETS

900 Vancouver Street
Victoria BC V8V 3V7
p 250.386.7781
w bc.anglican.ca

INFORMATION SECURITY POLICY

1. INTRODUCTION

The diocese, including its parishes, employees, volunteers and other representatives, will adhere to the diocesan Privacy Policy and the provisions of the Personal Information Protection Act (PIPA) relating to the collection, accuracy, protection, use, retention, archival transfer and disclosure of personal information.

We require these policies to be followed not only to increase our overall information security, but also for the reason of consistency. Should the Synod office be asked to provide support or need to access an account in the event of an emergency, a consistent set-up allows us to immediately begin work on the issue without first needing to understand each parish's set-up.

2. ROLE OF THE SYNOD OFFICE IN TECH SUPPORT

The Synod office is available to provide training and support to parish administrators but is not to be utilized as the Diocese's tech support. It is expected that parish administrators or their equivalent will know or learn the basics of the Microsoft 365 Admin center to support their parish's information security. Tenom (previously Total Support) is available at the parish's expense for technology issues which are beyond the purview of the Synod office.

We encourage parish administrators to take the time to watch the past Parish Learning Hub sessions on Microsoft 365, SharePoint, and Cybersecurity – and for the incumbent to provide the administrator with the time needed to do this training.

3. USE OF ANTI-VIRUS SOFTWARE

In order to protect against the inadvertent introduction of malicious software, it is best practice that every device owned by the diocese or a parish be equipped with a current, industry standard, anti-virus (aka anti malicious software) program that is properly maintained and updated.

4. USER ACCOUNTABILITY AND PASSWORD MANAGEMENT

Password access control for authentication shall be unique to each User and serves, not only as their access credentials, but also as a tracking mechanism for after the fact accountability for actions related to information security and privacy.

Passwords must be complex using a mixture of alphabetic (upper and lower case), numeric characters, and non-alphabetic characters (such as $, !, #. %, *). Passwords should not contain the user's account name or personal identifiers like dog's name or home street.

5. MULTIFACTOR AUTHENTICATION

Multifactor authentication (MFA) provides a second layer of information security for User accounts. All Users with a parish account are required by the diocese have MFAs enabled. It is the responsibility of the parish administrator or designated technology support volunteer to enable MFAs for each parish account.

As of February 2027, SMS (text message) verification is no longer offered as an authentication method. Passkeys – either through Microsoft Authenticator, or Windows Password Manager/similar will be used instead.

6. CYBERSECURITY

To help safeguard against increased phishing attempts, we ask that users utilize electronic mail signatures to identify themselves to email recipients. This should include name, phone number, and job title. Scammers are able to pull information such as emails and names from our websites, so adding extra identifying information may help to differentiate between a legitimate and illegitimate email. If you receive an email and are uncertain about if it is safe, please do the following:

- If it is spear-phishing (imitating someone trusted within the parish), reach out to them via a verified email or phone number to confirm if they sent it
- If it is coming from an unknown source but you think it may be a legitimate request, send it to the Synod office
- Should the email be confirmed as phishing, block and report the sender. In the case of spear-phishing, it would also be prudent to inform others within the parish of the attempt

7. STANDARDIZED EMAIL ADDRESSING FOR PARISH ELECTRONIC MAIL

Unless explicit permission has been granted by the Synod office, it is a requirement that individuals in these positions utilize their parish email addresses for parish-related business. For each parish there are specific email IDs for the following parish positions:

- treasurer@domain (the domain name will be @YOUR PARISH CHOSEN DOMAIN NAME)
- admin@domain
- incumbent@domain
- safechurch@domain
- wardens@domain (see 8. SHARED MAILBOXES)

Additional email addresses may be assigned by the parish office for other ministries as required. Each of these usernames e.g. “treasurer” will be assigned to a named user account e.g. “John Smith”. Upon completion of the term, the email from the account will be archived and the username (e.g. “treasurer”) will be reassigned to the person assuming the position using a new named user account. This allows for continuity of any ongoing communications and can provide a useful reference tool.

8. SHARED MAILBOXES

Shared mailboxes allow multiple users to simultaneously access a single inbox, while ensuring information security is maintained through the use of user-unique passwords and MFAs. Some parishes may have multiple positions which are shared amongst two or more people, but all will have the *wardens@domain* shared mailbox. Each warden has a specific email address in the form of *FirstInitialLastName@domain*, which is added as a member to the *wardens@domain* account. The individual wardens have access to the shared account by way of signing in through their personal account.

9. CLERGY EMAILS

When clergy retire or move to another parish, the incumbent@ parish email will be transferred to the incoming interim or permanent incumbent. The email from the previous clergy will be archived but will be available as required by the new incumbent or the diocese. For communication with the bishop or other emails that pertain only to that specific person, the cleric should use their individualname@bc.anglican.ca address.

Personal email addresses should not be published on a parish website. Personal email addresses are to be published in print only with the consent of the individual.

10. DIGITAL AND PHYSICAL FILE STORAGE AND RETENTION

Digital files should not be stored locally. All individuals with a parish email address are expected to use Microsoft 365’s SharePoint to retain their files. As a cloud-based storage platform, files stored on SharePoint are remotely backed up, meaning that if a device at the parish breaks, information can still be accessed.

Physical files should be stored in a cool, dry, dark location. Refer to the Parish Records Retention Schedule for details on how long physical and digital documents should be retained, and if they require transfer to the diocesan archives. Following retention policy is crucial to ensure adherence to provincial and national laws such as PIPA.

11. NO GUARANTEED MESSAGE PRIVACY

The diocese cannot guarantee that electronic communications will be private. Users must be aware that, depending on the technology, electronic communications can be forwarded, intercepted, printed, and stored by others.

12. AUTHORIZED USAGE

The diocesan electronic communications systems generally must be used for business activities. Incidental personal use is permissible as long as it does not consume more than a trivial amount of system resources, does not interfere with worker productivity, and does not preempt any business activity.

Updated: August 2026