ANGLICAN DIOCESE
OF ISLANDS AND INLETS

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.

2. USE OF ANTI-VIRUS SOFTWARE

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

3. 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.

4. SHARED EMAIL ADDRESSING FOR PARISH ELECTRONIC MAIL

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)
warden1@domain
admin@domain
incumbent@domain
safechurch@domain

Additional email addresses may be assigned by the parish office for other ministries as required. Such changes or additions are to be communicated to the synod office as they are made.

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.

Retired clergy t\or clergy moving to another parish will give up their incumbent @ parish email and it will be assigned 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.

Personal email addresses should not be published on a parish website.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.

5. 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.

6. 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.