



**Grace Presbyterian Church**  
**Arlington, Texas**  
**Computer Use Policy**

June 10,2008  
Version 2.1

## Table of Contents

Overview .....	3
Purpose.....	3
Repercussions .....	3
Revision History .....	3
Computer Policy .....	4
Computer Usage.....	4
Password Management .....	4
Email Use.....	4
Internet Use and Access.....	5
Information Management.....	5
Website Management and Usage .....	6
Systems Management .....	6
Computer Policy Management .....	6

## Overview

Computer systems, the networks that the computer systems use,, and the information contained within the computer systems are an important part of the business assets at Grace Presbyterian Church (GPC). It is important that these assets be protected from intentional or unintentional misuse.

---

## Purpose

The purpose of this policy is to outline and define the acceptable use of the computers and computer resources at Grace Presbyterian Church (GPC). These policies are in place to protect the users of the computers as well as GPC.

The intent of this policy is not to provide or include the detailed procedures for complying with the policy but the overarching guidelines that will be used to guide and direct the use of computers and computer resources at GPC. The detailed policies and procedures will be developed by the Computer Ministry and follow the tenets contained in this document.

---

## Repercussions

Employees or church members found to have violated this policy may be subject to disciplinary action, up to and including termination of employment/removal from all use of computer equipment.

---

## Revision History

Version	Description	Approved
R2.0, April 2008	Consolidation and simplification of policy.	Ministry
R2.1, June 2008	Input per committee	Ministry

## Computer Policy

---

### Computer Usage

---

The following general computer use policy statements must be followed:

- Access to all GPC computers – including those in common areas such as the library – will require the use of a user ID and password.
- All users of the computer systems at Grace must know and abide by all applicable GPC policies dealing with security and confidentiality of church records.
- Access to computers at Grace will be granted on an as-requested and as-needed basis. Access to specific applications will be granted on an as-needed and as-required basis.
- Under no circumstances is a user of the computers and/or computer resources at GPC authorized to engage in any activity that is illegal under local, state, federal or international law while utilizing GPC-owned resources.
- Employees/church members *shall not* download, install, and/or copy software unless authorized by the Computer Ministry.
- Only licensed and authorized software may be installed on GPC computer systems.

---

### Password Management

---

The following statements provide the required practices for password-management at GPC:

- A password will be assigned to each user granted access to the GPC system.
- Users can only access the GPC system(s) after entering a valid user ID and password.
- Passwords should be kept secure. Authorized users are responsible for the security of their passwords and accounts.
- Accounts and access to GPC computers should not be shared even within family units.
- A user's password must be changed periodically.

---

### Email Use

---

E-mail sent using the church account gives the outside world an impression of who we are and what we represent. No objectionable materials/content may be sent using the church e-mail accounts. An employee/church member who uses e-mail at GPC is:

- Responsible for the content of all text, audio, or images that are sent over the Internet via a GPC email account. All communications must have the employee/church member's name and disclaimer attached.
- Responsible for validating and ensuring that copyrighted materials are not transmitted without permission.
- Responsible for ensuring that any attachments attached to outbound emails are clean and free of viruses.
- Responsible for ensuring that all attachments detached from inbound emails are clean and free of viruses.
- Responsible for ensuring that the transmission of confidential or sensitive information via email utilizes secure delivery to the designated recipient(s).

---

## **Internet Use and Access**

---

Users of GPC computers who use the Internet are representing GPC. As such, all users who access the Internet are responsible for ensuring that they use the Internet in an effective, ethical, and lawful manner. Examples of acceptable use are using Web browsers to obtain business information from commercial Web sites; accessing databases for information as needed; and using e-mail for business contacts.

- Access to all GPC computers – including those in common areas such as the library – will require the use of a user ID and password.
- Users of the computers at GPC may not use the Internet for purposes that are illegal, unethical and/or harmful to the church. Examples of unacceptable use are conducting personal business using church resources; and/or transmitting any content that is offensive, harassing, or fraudulent.
- All internet access should be controlled via the use of a user ID and password.
- Postings by employees/church members from a GPC email address to newsgroups should contain a disclaimer stating that the opinions expressed are strictly their own and not necessarily those of GPC, unless posting is in the course of church/business duties.
- File downloads from the Internet are not permitted unless specifically authorized by the Computer Ministry.
- GPC Internet users are responsible for validating and ensuring that copyrighted materials are not utilized without the required permissions and citing.

---

## **Information Management**

---

Given the sensitive nature of some of the information contained on the GPC computers, the following information management policies will be followed:

- Access to sensitive data will be controlled by agreement between the affected Ministry (Finance Ministry, Personnel Ministry, etc), and the Computer Ministry. Permission for the Ministries and individuals to access sensitive information must be approved by Session.
- All use of computer systems at GPC including email, internet use, and business applications may be monitored for usage.

---

## **Website Management and Usage**

---

The GPC web-site is a mechanism that allows us to communicate with each other and the public. As such, we must take great care in what we communicate and how we communicate it. The following statements will apply to the management and implementation of the GPC web-site.

- Only information pertaining to the worship, fellowship, and missions of Grace Presbyterian Church should be published on the church web-site.
- Statements on the web-site pertaining to theology accepted by GPC and the Presbyterian Church USA must be approved by Session.
- Names of church members should not be published without their express permission.
- The phone numbers of members and/or visitors will not be published on the church web-site.
- The use of pictures, photos, and/or names of youth (defined as individuals under the age of 18) are not permitted on the GPC web-site. Refer to the GPC Child Protection Policy for additional details.
- Dialogs from any GPC sponsored online blog, discussion board, etc may be monitored. Inappropriate discussion and comments may result in the discussion forum being discontinued or access to the discussion forum being disabled.

---

## **Systems Management**

---

- All computers used by the employee/church member that are connected to the GPC Internet/Intranet/Extranet, whether owned by the employee/church member or GPC, are required to use approved virus-scanning software with a current virus database.
- The most recent security patches must be installed on GPS servers as soon as practical, the only exception being when immediate application would interfere with business requirements.
- Prior to any desktop or laptop computers being allowed to access the GPC network, the computer must have the latest available Microsoft security patches. Exceptions must be approved by the Computer Ministry.
- For security and network maintenance purposes, authorized individuals within GPC may monitor equipment, systems and network traffic at any time. GPC's Computer Ministry reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.

---

## **Computer Policy Management**

---

- Updates to the GPC computer policy will be reviewed/approved by the Computer Ministry and then must be approved by Session
- Updates to the procedures for describing the details of the computer use at GPC may be updated with the approval of the Computer Ministry.
- Updated computer use policies and procedures will be published and made available within the church office.
- Users will be expected to sign off on the computer policy on an annual basis.