ELECTRONIC USAGE POLICY FOR THE FIRST PREBYTERIAN CHURCH IN PHILADELPHIA

January 11, 2018

This Policy governs the use of electronic communications systems ("Systems") of the First Presbyterian Church in Philadelphia ("FPCP"), which include computers, electronic tablets, smartphones, printers and other peripherals, programs, data, networks, voicemail and the Internet. These Systems may be made available or provided to guests, visitors, members and volunteers of the church ("Users"), to better serve our congregation and the mission of FPCP, by providing employees and volunteers with appropriate tools to do their jobs.

1. Acceptable Use

FPCP's Systems are provided to Users for the purpose of increasing efficiency and productivity for the business and mission of FPCP and are to be used for legitimate church purposes, in a manner that is responsible, professional, ethical and in accordance with this agreement, except for responsible, limited and incidental personal usage, otherwise consistent with this Policy, which does not create any expense for FPCP.

2. Prohibited Use

It is prohibited to use FPCP's Systems in a manner that interferes with FPCP's ability to conduct its business in a manner consistent with its mission and that has an adverse impact on its efficiency and productivity. FPCP's Systems may not be used for personal gain or for any purpose that would violate any federal, state or local law or regulation. Examples of applicable laws, rules, and policies include the laws of libel, privacy, copyright, trademark, obscenity and child pornography, the Electronic Communications Privacy Act, and the Computer Fraud and Abuse Act, which prohibit "hacking," "cracking" and similar activities. Other examples of prohibited activities include, but are not limited to:

- Using FPCP's Systems in furtherance of any illegal act, including violation of any criminal or civil laws or regulations, whether state, federal or local
- Any commercial or "for profit" purposes, or to generate personal income
- Sending threatening, bullying or harassing messages, whether sexual or otherwise
- Accessing or sharing sexually explicit, obscene or otherwise inappropriate materials
- Gaining or attempt to gain unauthorized access to any computer or network
- Any use that causes interference with or disruption of network users and resources, including propagation of computer viruses, other harmful programs or virus hoaxes
- Intercepting communications intended for other persons or sending chain letters that misuse or disrupt resources
- Misrepresenting either FPCP or a person's role at FPCP
- Accessing online gambling sites
- Conducting activities that are illegal, inappropriate or offensive to others, including, but not limited to: libel or defamation; hate speech or ridiculing others on the basis of race, color, religious creed, national origin, age, genetic information, sex, sexual orientation, ancestry, disability, veteran status or political beliefs; illegal weapons and terrorist activities;

3. Data Confidentiality and Privacy

The provisions of this section recognize that certain electronic communications are ethically or legally privileged and/or confidential. However, Users are encouraged to have particularly sensitive communications verbally or by some other method that does not involve use of

FPCP's electronic communication system, since FPCP cannot guarantee security and confidentiality, as noted below.

- All data files stored on the church's computer systems become the property of First Presbyterian Church. Users also should be aware that files or messages that the user has deleted may be stored elsewhere and are not necessarily erased from the network.
- Under no circumstances is it permissible for a User to acquire access to confidential data or to disseminate any confidential information through FPCP's Systems, unless required as part of his or her role as an employee or volunteer (such as a member of Session or the Board of Trustees).
- FPCP cannot guarantee security and confidentiality. Users should therefore engage in "safe computing" practices by establishing appropriate access restrictions for their accounts, guarding their passwords, and changing them regularly.
- The equipment, services and technology used to access the Internet are the property of FPCP and FPCP maintains the right to monitor network traffic and access all data that is composed, sent or received through any of its systems and online connections.
- Users understand that:
    1) their activity is periodically monitored and that any communication is not necessarily private;
    2) when reasonable and appropriate, FPCP will exercise its right to inspect, monitor, log, record or inspect any data that Users create or receive, any messages they send or receive, websites they access, and any files or information maintained or passed through its Systems or equipment; and
    3) the public WiFi network is not encrypted.
- Users of FPCP Systems understand and agree that they have no expectation of or actual privacy rights regarding their usage of FPCP Systems.

4. Copyright Protection

Attention should be paid to not violating intellectual property rights by inappropriate use or copying of computer programs, software or information published on the Internet, such as text and graphics on a website. The fact that information is publicly available on the Internet does not mean that it is in the "public domain;" the information may still be protected by copyright. Users should exercise care and judgment with copying or distributing computer programs, pictures, articles or other information that could reasonably be expected to be copyrighted.

5. Computer Viruses

Users should exercise reasonable precautions to avoid computer viruses and virus-scanning software should be used to check any files downloaded from the Internet or obtained from any questionable source. Executable files (e.g. program files that end in ".exe.") should not be stored on, or run from, FPCP network drives.

6. Computer Software

Users are not permitted to download and/or install any personal, web, social networking or other software onto any computer system without express permission from the IT Committee of the Board of Trustees. If installs are required, a member of the committee with administrative rights to the computer system will perform any installs.

7. Music & Video Files, Streaming

Unless related to their church responsibilities or at inconsequential cost to FPCP, users are not to store personal music or video files on FPCP computers or to stream audio or video over the Internet to FPCP-computers, and such use is to be otherwise consistent with this policy.

8. Network Security

Users should never share their passwords and should promptly notify FPCP IT personnel if they suspect their passwords have been compromised. Users should either log off their computer or use a password-protected screen saver if they will be away from the computer for periods of time where is may be reasonably anticipated that another user may have access to the computer.

9. Email and Internet Use as a Representative of FPCP

- Church staff and members should be mindful of creating personal communications, whether online or elsewhere, that may be perceived as representing the views or position of FPCP and are encouraged to note, whether on platforms such as Twitter or FaceBook, that their views are personal and not representing FPCP.
- Any email sent from an fpcphila.org email address (or other FPCP email address) might be viewed as representing an official statement from FPCP. Therefore, all e-mail must be appropriately worded and compatible with the mission of FPCP.
- Users are not to setup or use personal email client software such as Outlook Express or Thunderbird on FPCP Systems.

10. Additional Provisions for Users Under 18 Years Old

- Personal information (i.e., name, address, phone number, etc.) should never be disclosed online.
- If a youth accidentally finds anything inappropriate on a website, they are to immediately turn off the monitor and notify the head of staff, Church Administrator or a member of the IT Committee.
- Any youth that sees another person, student or adult, not adhering to this policy is to notify the head of staff, Church Administrator or a member of the IT Committee.
- Automatic notification will be made to the individual and parent/guardian of any student under the age of 18 involved in any significant violation of this Policy.

11. FPCP Responsibility

FPCP has no responsibility for maintaining, recovering, transferring or any other action, regarding any personal files, applications, software or data that Users install on the Systems. The User accepts responsibility for any loss or damage that is related or due to the User's installation of applications or software for personal use.

12. User Responsibility

Users who violate this policy may be denied access to FPCP's computing resources and may be subject to other penalties and disciplinary action, including possible termination of employment. FPCP may also refer suspected violations of applicable law to appropriate law enforcement agencies.

This Electronic Usage Policy is approved by the Session of The First Presbyterian Church in Philadelphia.

Approved by Session on: January 14, 2018