

Document Number:	9.A
Document Name:	TECHNOLOGY USE POLICY
Effective Date:	09 2020
Document Status:	ADOPTED

1.0 Purpose

The purpose of the Technology Use Policy of the Culpeper Presbyterian Church (CPC) is to provide guidelines to prevent inappropriate, unethical, or unlawful behavior by any of its users. The policy will detail the terms and conditions for the use of various technology products including but not limited to computers, computer systems, software, networks, and social media.

2.0 Policy Scope

The policy applies to all employees, volunteers, and youth utilizing any and all computer resources, internet, and social media. This policy is designed to express CPC's philosophy and general principles as no policy can cover every possible situation. Personal use is limited as long as there is no cost to the Church, burden to the Church's computer and networking resources, and has no adverse effect on the Mission Statement of the Church.

3.0 Policy Statement

The Church will maintain the Technology Use Policy in the Culpeper Presbyterian Church Policy Manual ensuring the integrity of the policy. The Business Manager will be a member of the Technology Team for the daily management of all technology resources. The Team will meet on a regular basis, to review and carry out the intent of the Policy. All meetings are open to the congregation and anyone interested in serving on this important team is encouraged to do so.

4.0 Compliance

All users of CPC's computers, computer systems, software, networks, and social media must comply with all federal and state laws, church policies, and the terms of software licenses. No downloads or software installations to any computers are allowed without the permission of the Business Manager.

5.0 Responsibilities

Users are responsible for all operations within their control affiliated with their account. Any detected or suspected unauthorized usage of their account should be reported to the Business Manager, and then to the Minister and/or Session. No misuse or unauthorized altering of church, minister, or personnel files is permitted. Conscious attempts to bypass data protection or other security measures are not permitted. Anyone who violates this policy may be denied access to the Church's computing resources and may be subject to other penalties and disciplinary action, up to and including possible termination (refer to the Personnel P&P Handbook, Section 5.11). CPC may also refer violations to the applicable law enforcement agencies.

The Technology Team is responsible for maintaining written procedures of all technology resources which will be housed in a separate binder in the Business Manager's office.

6.0 Data Protection

Users are required to create and maintain all church related documents and files on the church main network server, to ensure security backups and recovery of application files and data. Backup data files are stored on the church's Microsoft OneDrive account and are considered property of CPC. CPC cannot guarantee security and confidentiality. Users should establish access restrictions, monitoring passwords and changing them on a regular basis.

7.0 Church Electronic Accounts

This category includes but not limited to E-Mail, Facebook, Website, Constant Contact, etc. and detailing the appropriate usage of each platform. All data that is stored on CPC's server becomes property of the church. All correspondence and postings on these platforms coming from church@culpeperpresbyterian.org or someone acting as a representative of the church must be compatible with the church's mission.

8.0 Inappropriate Use

This not being a comprehensive list, the following are considered inappropriate and unacceptable:

- Chain mail that misuses or disrupts resources
- Virus hoaxes
- Spamming or e-mail bombing
- Offensive or disruptive language including harassing or hate email, vulgar language, pornography, sexual comments or images, and derogatory messages
- Junk E-Mail
- Playing of Games
- Representing the church through church or personal platforms that are a) not within the policy guidelines or the church's mission, or b) without authorization of the Business Manager, Minister, or Session

Anyone connecting to the church's wireless network, even with personal technology, is expected to comply with this policy.

9.0 Technology Equipment

No equipment shall be removed from the property without the permission of the Business Manager, and not for personal use. Only trained personnel are authorized to use church owned equipment.

10.0 Reporting

Minutes of the Technology Team monthly meetings will be recorded and forwarded to the Team members and the church office. Minutes will be included in the monthly Session Packet for review.

11.0 Policy Owner

The Technology Team in coordination with the Business Manager and approved by Session.