

Calvary Chapel Costa Mesa

Computer and Internet Use Policy with Appropriateness Guidelines

Date of Revision: September 2017

Date of Issue: October 2017

Policy Scope:

These policies cover assigned devices, privileged file data, and internet connections within Calvary Chapel of Costa Mesa (CCCM), its staff/volunteers, and its facilities. Use of the CCCM equipment/data/Internet is restricted to activities that legitimately further the operations and programs of CCCM and its individual departments.

Computer Device Provisioning Statement:

All computer devices distributed by CCCM and its Calvary Technical Services (CTS) department are the property of CCCM and must be returned to CCCM/CTS upon employee/volunteer termination, and that handled via the Human Resources (HR) department within CCCM.

Computer Device Security and Threat Protection:

All devices distributed by CCCM are pre-equipped with anti-malware and/or anti-virus software in order to prevent contraction and spread of threats to the local area network (LAN), the Internet, and CCCM owned facilities. Users should contact CTS if virus protection is not installed on a device, or if suspected virus/malware/threat is discovered.

Supervision of Computer Users:

Department managerial accountability for the privileged access and the actions of subordinates applies equally to computer access, network file access, Internet use, and to any other technology-related access.

Computer, email and internet usage

- CCCM employees are expected to use the Internet responsibly and productively. Internet access is limited to job-related activities only

and personal use is not permitted unless granted by direct management.

- Job-related activities include research and educational tasks that may be found via the Internet that would help in an employee's or volunteer's role
- All Internet data that is composed, transmitted and/or received by CCCM's computer systems is considered to belong to CCCM and is recognized as part of its official data. It is therefore subject to disclosure for legal reasons or to other appropriate third parties
- The equipment, services and technology used to access the Internet are the property of CCCM, therefore CCCM reserves the right to monitor Internet traffic and monitor and access data that is composed, sent or received through its online connections
- Emails, instant messages, and the like, sent via the CCCM email or message systems should not contain content that is deemed to be offensive. This includes, though is not restricted to, the use of vulgar or harassing language/images
- All sites and downloads may be monitored and/or blocked by CCCM if they are deemed to be harmful and/or not productive to business

Unacceptable use of the internet by employees includes, but is not limited to:

- Sending or posting discriminatory, harassing, or threatening messages or images on the Internet or via CCCM's email service
- Using computers to perpetrate any form of fraud, and/or software, film or music piracy

- Stealing, using, or disclosing someone else's password without managerial authorization
- Downloading, copying or pirating software and electronic files that are copyrighted or without authorization
- Sharing confidential material, trade secrets, or proprietary information outside of the organization
- Hacking into unauthorized sites or websites
- Sending or posting information that is defamatory to the CCCM, its products/services, colleagues and/or customers
- Introducing malicious software onto the CCCM network and/or jeopardizing the security of the organization's electronic communications systems
- Sending or posting chain letters, solicitations, or advertisements not related to business purposes or activities
- Passing off personal views as representing those of the organization

If an employee is unsure about what constitutes acceptable Internet usage, then he/she should ask his/her supervisor for further guidance and clarification

User compliance

All terms and conditions as stated in this document are applicable to all users of CCCM's networks and Internet connections. All terms and conditions as stated in this document reflect an agreement of all parties and should be governed and interpreted in accordance with the policies

and procedures mentioned above. Any user violating these policies is subject to disciplinary actions deemed appropriate by CCCM.

I understand and will abide by this Computer and Internet Usage Policy. I further understand that should I commit any violation of this policy, my access privileges may be revoked, my assigned device(s) confiscated, and disciplinary action and/or appropriate legal action may be taken.

Printed Name _____

Employee signature

Date