

BCC Policy: Computer Use

Approved February 2002

Updated August 2007

Scope

This document describes the policy regarding use of computers in the church facility. This includes staff computers that are part of the church network as well as other outside computers that could be connected to the network.

Authorized Users

BCC usernames are assigned to individuals because those persons have a designated need for access to BCC Applications and Data. Authorized users should protect the BCC Applications and Data from misuse by not giving out their username and password. All BCC computers are to be primarily used for church business.

Access Rights

All authorized users of the computers will have personal accounts. (There are a few exceptions to this: for example, the worship and missions teams each have a single account used by multiple people.) This will prevent any unauthorized users from logging into the systems. Any access given to unauthorized individuals could result in the revocation of the responsible user's account.

Use of Local Hard Drives

Local workstations should, for the most part, not be used to store data files. All working files should be kept on one of the virtual drives on the server. The disk drives on a local workstation should be able to be completely reformatted or replaced without loss of data other than configuration settings for the user's account.

Internet Access

All authorized users have access to the public internet. Accessing the internet should be done with great care and deliberate focus. Users who access the internet can pose great risk to themselves as well as to the BCC network. Children should not be allowed to have access to the Internet from BCC computers. Misuse of the Internet will result in revocation of the user's account.

All BCC computers are to have internet filtering software installed and enabled.

Approved Software

BCC users should not install personal software or games whether downloaded from the Internet or brought in from home. Downloaded software from the Internet can introduce virus infected programs and compatibility issues with approved software. Software brought in from home can cause incompatibilities and other issues with the overall software installation of the computer. The Finance or Communications Committees should approve all regularly used software.