Policy Number:
Effective Date:
Approval:

All God's Children Metropolitan Community Church

Subject: COMPUTER USAGE

Scope:

This policy sets forth guidelines to be used by all AGC employees and volunteers with regard to the use of AGC-owned computer equipment. These guidelines are necessary to ensure maximum up time, system integrity, and data security and to ensure compliance with licensing agreements.

AGC-owned computer equipment includes, but may not be limited to:

- Desktop Computers
- Laptop Computers
- Personal Data Devices
- Printers, Copiers
- Fax Machines
- Network Servers
- Switches
- Hubs
- Routers
- Data Jacks
- Cables
- Accessories
- Peripherals

Practice:

User Access

All employees for whom computer usage is an essential part of their job function will be given a user name and password by the Technology Team with the appropriate access level. Volunteers needing access to the AGC network will also be given a user ID and password.

Computers

AGC provides a computer, to all employees for whom computer usage is an essential part of their job function. These computers are owned by AGC and are maintained by the Technology

Team and consultants as hired by the Technology Team. They are to be used primarily for church purposes.

Computers are also located in several common areas for employee and volunteer use.

All AGC employees and volunteers must abide by the following terms and conditions when using AGC-owned equipment.

Equipment

Each AGC computer installation is provided with the following equipment:

1. CPU (Central Processing Unit)
2. Monitor
3. Keyboard
4. Mouse & Mouse Pad
5. Power Strip/Surge Protector

Accessories

The Technology Team does ***not*** provide computer accessories.

These items include, but are not limited to:

Adjustable Monitor Stand
Adjustable Workstations
Arm Support
Copy Holders
Desktop Print Stand
Desktop Organizer
Diskette Storage Devices
Diskettes
Ergonomic Adjustable Chair
Foot Rest
Keyboard Cover
Keyboard Wrist Rests
Lights
Mouse Holder
Mouse Wrist Rests
PC Roll Out Keyboard
Radiation/Privacy/Glare Filters for Monitor
Speakers
Specialized Mouse Pad
Under the Desk Keyboard Trays
Headphones/Microphones

Operational Rules – *These guidelines cover any and all computer and related equipment owned by AGC whether on or off the premises.*

Security

1. Only AGC employees, volunteers or contracted workers with a user ID and password supplied by the Technology Team are permitted to use AGC computers and related equipment.
2. Use of AGC computers by other individuals, including family, friends and AGC employee's without their own unique user ID and password is strictly prohibited.
3. Passwords will expire every 90 days and should be changed to a unique password.
4. Passwords should not be written down or shared with anyone other than an authorized member of the Technology Team as needed for troubleshooting purposes.
5. If any other individual discovers a user's password it should be changed immediately.
6. Computers should be shut down every night so as not to interfere with the backup process unless overnight processing is required for business reasons.

7. A full system backup is performed every night beginning at approximately 1:30 a.m. and ending at approximately 4:00 a.m. Interference with this backup routine is strictly prohibited.
8. No unauthorized persons are permitted in the central server room. Authorized personnel include, members of the Technology Team, select employees and approved vendors and repair technicians.
9. No unauthorized personnel are to attempt to fix, alter or in any way access any equipment in the server room. This includes, but is not limited to servers, hubs, switches, monitors, UPS backups, phone system, voicemail, security systems and all connections and peripherals therein.

Hardware

1. All computer-related hardware is purchased through the Technology Team in order to maintain church-wide standards and consistency and to ensure proper support.
2. Any employee or volunteer found to have caused physical damage to AGC-owned hardware beyond normal wear and tear will be held legally and financially responsible for its replacement.
3. Users may not move or exchange computers or computer-related equipment. All equipment will be placed by a member of the Technology Team.
4. All computer equipment is installed with a power strip/surge protector. At no time may the surge protector be removed as it may cause irreversible damage to the unit. Computers should never be plugged directly into a wall outlet.
5. Upon termination all AGC-owned hardware must be returned in the same condition as when it was assigned. Employee's will be held financially responsible for any equipment that is not returned or is returned damaged beyond normal wear and tear.

Software

Employees not following the procedures in the software policy shall be held personally liable for any and all violations of copyright laws and subject to the penalties contained in Title 17 and Title 18 of the United States Code. Software pirating and failure to adhere to licensing agreements is a federal offense and will be dealt with severely. Computers will be audited at least yearly and all non-AGC-licensed software removed. For a complete listing of all AGC approved software, please contact the Technology Team.

1. All AGC computer software is purchased through the Technology Team for the following reasons:
    a. To maintain proper licensing levels
    b. To preserve church standards
    c. To guarantee compatibility with existing hardware and software
    d. To ensure proper installation and support

    The Technology Team reserves the right to determine if there is a church-owned software that will meet the employee's or volunteer's needs before purchasing new software and is committed to working with all users to guarantee that all needs are being adequately met.
2. A Technology Team member will perform all software installations.
3. No personal software is permitted in the facility or on AGC-owned computers. If discovered it will be deleted immediately and without notice.

4. No downloading or uploading of any non-AGC software is permitted. This includes screen savers, freeware, shareware and games.
5. Personal background pictures are permitted so long as they do not interfere with the normal operation of the computer and are not of an obscene or objectionable nature. This includes images that may contain or promote some of all of the following: pornography (nude or semi-nude), violence, blaspheme, discriminatory language, political affiliation, illegal or unethical practices, and any other images deemed inappropriate by the church leadership.
6. Programs such as Web Shots, which automatically change the background pictures, are not permitted as they interfere with many applications, degrade the performance of the computer and congest the Internet Connection. If found they will be removed immediately and without notice.
7. Evaluation copies of software for a specific business purpose may be installed only with the permission of the Technology Team and must be removed immediately when the evaluation period has expired.
8. No AGC-owned software may be removed from the premises.
9. No AGC-owned software may be copied or installed on non-AGC-owned systems unless it is purchased for that specific purpose. Once installed on the personal computer that individual becomes wholly responsible for its maintenance and support.
10. Any employee found to have destroyed or disabled AGC software will be held personally and financially responsible for all damage resulting from this action.
11. At least annually an inventory of all software on each individual PC and all servers will be audited against the organization's license agreements. All illegal software will be removed immediately and without notification. Church leadership will be notified of all non-AGC software discovered.

Data

1. All data stored on AGC computers, file servers or other storage devices is considered the property of AGC.
2. All AGC documents and data must be stored on the file server in the appropriate folders. The user may not store church data on their CPU (C drive), or floppy disks without also copying the document to the file server. Any files not stored on the appropriate file server may be lost due to hard disk failure or error. PC's are not backed up and the Technology Team is not responsible for loss of any data that may occur due to storage of files on PC's or floppy disks.
3. Upon termination employees must leave all relevant files in tact. Destroying data either by deleting or encrypting it on the workstation or network is considered a criminal act and legal action may be taken.
4. Upon termination employees may not copy or in any way take with them any data that is the property of AGC.
5. Any employee, former employee or volunteer who is responsible for the destruction or deletion of data during employ or upon termination will be held personally liable and financially responsible for the recovery of such data.
6. Passwords may be used on files, but the passwords must be given to the Technology Team Leader who will keep them in an encrypted file. A file with a password will be considered destroyed if the employee leaves AGC and the Technology Team Lead or the

employee's successor does not have the password. The employee may be held responsible for any damages or extra expense that is incurred by having to recreate or "hack" into a file.

7. All company data and documents may be reviewed by the employee's supervisor/manager or the board at any time.
8. The Technology Team Lead and select members have access to all areas of the computer network and in some cases find it necessary to access documents for security, safety or emergency reasons. All information is held in strictest confidence.

General Computer Health

1. Anti-virus software is installed on all AGC computers and servers. This software ensures the integrity of all data. Disabling the anti-virus program is strictly prohibited.