

Resurrection Life Church Computer and Network Usage Policy

The computers, servers and networking equipment at Resurrection Life Church are provided for the ongoing operations of the staff involved in supporting the mission and vision of ResLife. The computers are intended to be used as tools for productivity, communication, creativity, and other tasks critical to the operations of the church. Although personal use of the computers is allowed, there are some rules concerning the equipment. These are in place to ensure the security and reliability of the computers, network, and the data stored on the servers. Please consider the needs of ResLife above personal preferences and conveniences when using the equipment provided. The rules are as follows, please read and understand these before signing. If you have any questions, please contact either the Human Resources or Information Technology departments for clarification.

1. Logins and Passwords

A. Sharing your ResLife login information with anyone, whether they are a member of the staff, your family, or a volunteer is strictly forbidden. This also covers logins for programs used by ResLife such as Shelby or CCB. Sharing your login can allow another person unauthorized access to sensitive or critical information or communications in your departmental folders, as well as your email. Allowing someone else to use your login can also cause unacceptable internet use to be logged under your name, even if you are not responsible. Never share your login information for any reason. If you have a volunteer that needs computer access please contact Human Resources to request a new account. If you ever feel there is someone who may know your password, please change it immediately.

B. The default password given with a new account should be changed as soon as possible. Please choose a password that no one can easily guess, and keep it secret to prevent unauthorized access. People have been known to stand at a computer and try different user names with simple passwords such as 1234 until they find one that works, you can easily prevent this by changing your password to something only you know. Do not tape the password under your keyboard, on the back of the monitor, or on a piece of paper in your drawer. These are common habits that reduce the integrity of the network. A quick, easy way to help keep your information secure is to get in the habit of locking your computer when you step away from it. Press CTRL+ALT+DELETE and select Lock.

2. Computer Access

A. There are many computers in the building that are critical to the daily operation of ResLife. Some control building heating and cooling systems, some simply run software that is expensive to reinstall and reconfigure. Some computers are used daily by people who can not perform their responsibilities without the computer, and can be seriously affected by it's absence during a repair or reinstallation. General access to these computers is restricted.

Some of examples of these restricted computers are as follows –

1. Any network server
2. Any Sanctuary computer, or any computer critical to services
3. Sound booth computers, including the Zone and Oneighty
3. Nursery and RezKidz check in system computers
3. Greenroom reception area computer
4. Front Desk reception area computers
5. Guest Services computers
6. Maintenance department and building management computers
7. Information Technology department computers
8. Print Center computers
9. Bookstore computers

These computers should never be used by any unauthorized person for any reason. For every person that logs in the chances of infection, corruption, or accidental damage increases, which can have a much greater affect than is obvious. There are plenty of computers in the building, please do not use any in the above list unless you are implicitly authorized to do so.

B. The computers in the individual offices are used daily by the people who occupy that space. Please be courteous and respectful and **do not** unplug, reconfigure, or move these computers. Do not install personal software on other people's computers, or remove software that they have installed. Please consider that computer as personal as their desk drawers, if someone is not in their office do not take it as an invitation to log them out and log in yourself. Also, do not consider it an invitation to sit down and surf the web or log in to your personal email. Especially if it means logging them out of theirs.

C. Everyone who has a login to the network at ResLife has also been given a certain level of access to files and folders stored on the servers, as well as to potentially sensitive information in CCB and Shelby. Please do not allow non-staff, volunteers, or children to sit and work or play at a desk under your login, or anyone else's login. This would allow that person to read, change, or even delete that data. A child playing at a desk could potentially erase every file in the 100-General folder by simply hitting the wrong combination of keys. Leaving someone with access to sensitive information could also lead to legal complications if that information was accidentally passed to the wrong person. Please treat the computers as what they are, tools to facilitate the mission and vision of Resurrection life Church.

3. Personal Equipment

A. Many people, either staff or volunteers, work from home to help complete projects or communicate after hours through email or terminal services. The IT department at Reslife is happy to help with connectivity issues concerning that access, but cannot provide further support for home computers. We welcome any help people give from home, but it is impossible to isolate a problem generated by working directly for ResLife from general home computer use. There are several people in IT who are happy to provide support and repairs during non-working hours, however, any service and compensation agreed to, or related to such repairs, does not involve Resurrection Life Church.

B. Personal laptops can be used at ResLife, but **must** be configured with effective, up to date antivirus and antispyware programs. Please bring your computer to the IT department to ensure you're protected, if not there are several free programs that can be installed to keep your computer, and ResLife's network, well protected from infection. Wireless internet access is provided throughout the building for staff and guest access, please **do not unplug the network cable** from any computer or printer and plug it in to a personal laptop. You may interrupt connectivity to something important, or interrupt a job left active by someone else.

C. Please remember that any personal equipment, either at home or in the building, is not backed up or protected by the systems at ResLife. Please be sure to perform regular back ups of your data, if you need recommendations on good back up software or hardware, please contact the Information Technology department.

4. Personal Data and Usage

A. Please remember that the computers here at ResLife are for the support of church operations, and should be treated as church property. You may store personal music and pictures in your My Documents folder (H: Drive), but keep in mind that server space and back up tapes are expensive. Please limit your personal data storage as best you can, and do not use the shared departmental folders as personal storage space.

B. Please refrain from streaming live music or video during working hours. Video and music consume large amounts of internet bandwidth and can affect web access to critical programs such as CCB, as well as connectivity to the Holland Campus. Most high bandwidth sites are blocked during the day, but some can be accessed before 9:00AM, during lunch, and after 4:00PM. If you have music you like to listen to, please bring in your MP3 player (iPod, etc), or play the CD from your computer or a portable player instead of listening to an internet station.

If you have any questions about this policy, please be sure request clarification from either the Human Resources or Information Technology department. Please sign below to verify that you have read and understand this policy, and agree uphold its terms.

Signed _____ **Date:** _____

Printed Name _____