

Bethlehem Evangelical Lutheran Church Computer, Internet, E-Mail, and Digital Network Usage Policy

Bethlehem Evangelical Lutheran Church (the 'Church' or BELC) believes all things should be done in an orderly way (see 1 Corinthians 14:40). Therefore, we have put into place this policy that defines boundaries for the use of the Church's information technology (IT) resources to ensure safety, good stewardship, fairness, and consistency during usage.

Table of Contents

	Page
Purpose	2
Scope	2
Definitions	2
Policy	3
Privacy	3
Waiver of Privacy Rights	3
Prohibited Activities	4
Security	5
Remote Access	6
Computer Laboratory	6
Personal Use of Internet	6
Internet Safety	7
E-Mail	7
Miscellaneous	9
Violations/Consequences	9
Attachments	10
Computer, Internet, E-mail, & Digital Network Use Agreement	11
BELC Computer User Responsibilities	12

PURPOSE

The IT resources, including computers and computer email accounts, belong to the congregation of this Church and are provided to users to assist in the performance of their Call, jobs, volunteer duties, and the ministries of the Church. They are not to be used for personal purposes except as allowed by this policy. The Congregation Council is to maintain this policy. However, implementation of this policy is the responsibility of the BELC's Office and Business Manager.

SCOPE

This policy is intended to address use of all BELC IT resources by staff (Called and lay), volunteers, and visitors (members and non-members) as well as use of personal electronic devices used on BELC premises.

DEFINITIONS

1. Access – The ability to read, change or enter data using a computer or an information system.
2. Computers – Refers to computers owned by BELC or used on the premises of BELC.
3. Data Storage Media – All forms of computer data storage and transport, including, but not limited to, computer floppy disks, writable CDs and DVDs, solid state storage cards, mobile computer storage and playback devices including MP3 players, iPods, USB drives, mobile phones or smart phones and personal digital assistants (PDAs), etc.
4. Information Technology Resources (IT) – All computer hardware, software, databases, electronic messaging systems, communication equipment, computer networks, telecommunications, and any information that is used to support BELC's operations, programs, and ministries.
5. Personal Electronic Devices – computers, laptops, iPads, Black Berries, mobile phones, smart phones, digital cameras, playback devices including MP3 players, iPods, etc.
6. Restricted Personal Data – Data containing confidential personal information including addresses, medical information, identification information or financial data.
7. Security Mechanism – Firewall, proxy, internet address-screening or filtering program, or other system installed to prevent the disruption or denial of services or the unauthorized use, damage, destruction, or modification of data and software.
8. Software – Authorized software is software that has been purchased by the BELC office with appropriate licenses and software deemed necessary for the execution

- of business and ministries at BELC. The approval of the Office and Business Manager is required for any software acquisition.
9. Staff – Anyone employed by BELC or acting in an official capacity appointed by the BELC Congregational Council.
 10. User – All persons who are granted access to BELC’s IT resources including staff, adult volunteers, BELC youth, and other individuals granted access according to the policy and the BELC Facility Use Policy.

POLICY

It is the policy of the Church that its IT resources are to be used only for the business of the Church and that personal use is prohibited except as allowed by this policy. Further, use of personal electronic devices for personal reasons while a staff member is being paid by BELC should be kept to minimum as judged by the Office and Business Manager and/or the pastors. Use of personal electronic devices by the congregation and visitors should not be disruptive to Church activities and shall only be used in a manner that is consistent with Christian principles. Use of personal electronic devices for illegal purposes by anyone is prohibited while on BELC premises, will not be tolerated, and will be reported if known.

The BELC Office and Business Manager in consultation with the pastor(s) shall determine who shall have access to BELC IT resources including temporary/permanent accounts, duration of access, and under what conditions (if different than the requirements of this policy). Access to personal and/or financial information shall be limited; individuals needing access to this information shall first secure the approval of the Office and Business Manager. Approval shall be based upon ‘need to know.’ The system protections (e.g. passwords) needed to assure the security of this information shall be determined and implemented by the BELC Office and Business Manager.

Privacy

BELC’s IT resources belong to the Church and as such, users should have no expectations of privacy in anything they create, store, send, or receive using these resources.

Waiver of Privacy Rights

Users expressly waive any right of privacy in anything they create, store, send, or receive using BELC IT resources, through the Internet, or any other computer network. Users of BELC IT resources consent to allowing the BELC Council President and/or Pastor or their designated representative to access and review all materials that users create, store, send, or receive on BELC computers or through the Internet or any other computer network. Users understand that BELC may use human or automated means to monitor use of its IT resources.

Prohibited Activities

Inappropriate or Unlawful Materials

Material that is fraudulent, harassing, embarrassing, lewd, sexually explicit, profane, obscene, intimidating, threatening or potentially violent, defamatory, racially offensive, inappropriate, or otherwise unlawful may not be sent by e-mail or any other form of electronic communication (such as bulletin board systems, newsgroups, chat groups) or displayed on or stored in BELC computers. Users may not use BELC IT resources for mass dissemination of any material outside of that which promotes and/or benefits the beliefs and missions of BELC.

Prohibited Uses

BELC IT resources may not be used for personal purposes (except as allowed by this policy), including personal email, storage of personal or commercial information, and any other activities not related to the business and ministries of BELC. BELC IT resources may not be used for receipt or distribution of inappropriate or unlawful material as defined above, participation in or accessing chat lines, chat groups or chat sites (unless directly related to BELC business or ministries), accessing any site which displays or distributes inappropriate or unlawful material as defined above, or any use which is unauthorized or unlawful. BELC IT resources may not be used for storage of databases or for services not related to the operations and ministries of BELC.

Misuse of Software

Users shall respect the copyrights, software licensing rules, property rights, and privacy. Users may not do any of the following: 1) copy BELC licensed software for use on their home computers unless otherwise allowed by the licensing agreement and the approval of the Office and Business Manager; 2) provide copies of BELC licensed software to any third person, or 3) install unauthorized software (including freeware and shareware) on any BELC computer or server. Any exceptions to these requirements must be first approved by the Office and Business Manager.

Communication of Confidential Information

Sending, transmitting, or otherwise disseminating restricted personal data or other confidential information of BELC is strictly prohibited. By exception as approved by the Office and Business Manager, these data may be transmitted if encrypted.

Security

BELC shall do everything practicable to protect personal identification information (e.g., birthdays, social security numbers, financial information, etc.). Procedures and/or processes shall be developed and followed that provides assurance that this information is protected from inappropriate disclosure.

Passwords

Users are responsible for safe-guarding their passwords for access to BELC IT resources. Passwords should be changed at least annually. Individual passwords should be protected and only given to BELC computer support personnel when needed for work or set up on individual computers. Upon completion of the work by computer support personnel, the user should immediately change his/her password. Users are responsible for all transactions made on BELC IT resources using their assigned account and password. No user may access BELC IT resources using another user's password or account.

Use of passwords to gain access to BELC IT resources or to encode particular files or messages DOES NOT imply that users have an expectation of privacy in the material they create or receive on the computer system. BELC has system access that permits access to all material stored on networked IT resources.

To be most effective, passwords should be at least 8 characters long and should not be a word commonly found in the dictionary. It should not be a name of a family member, pet, or anything else that is commonly associated with the user, nor contain repeating groups, e.g. abcabc or runs, e.g. mnopqrs. The password should also contain at least two of the following categories: letters, numbers, and special characters.

BELC computers that are on and temporarily left unattended shall be protected, i.e. password protected locked-out.

Accessing Other User's Files

Users have the responsibility to protect the data that resides on their machines. Users are prohibited from accessing or attempting to access IT resources for which they do not have explicit authorization by means of user accounts, valid passwords, file permissions or other legitimate access and authentication methods. In addition, users may not alter or copy a file belonging to another user without permission from the owner of the file. Certain files on the BELC shared server are intended for general office use and may be copied and altered in the daily operations of the church.

Accessing Other Computers

A user's ability to connect to other non-public computer systems through the network or by a modem does not imply a right to connect to those systems or to make use of those systems unless specifically authorized by the operator of those systems.

Auto Lock-screen

Each BELC computer shall utilize an auto, password-protected lock-screen (e.g. screensaver) that automatically locks the machine out after 15 minutes of non-use.

Remote Access

With written approval by the Office and Business Manager, BELC staff may be allowed to utilize remote access to the BELC server and computers from off site locations for official business and ministry activities. Remote access is strictly limited to approved staff performing normal daily job-related activities.

Wireless access at the Church is intended for business purposes only. Wireless access will not be made available to the congregation or other groups using the facility for any purpose other than daily church business and ministry activities. Groups needing wireless access for approved activities may access the wireless if approved by the Office and Business Manager. Once the Group's approved activity has concluded, the Office and Business Manager will change the remote access password. The staff shall not store the remote access password on their computer system.

While accessing BELC's remote access services, users shall have valid (as determined by the Office and Business Manager) anti-virus and malware software on their electronic devices.

Computer Laboratory

The computer lab may be used by BELC members and Sunday School classes as needed for teaching Sunday School or for activities associated with BELC ministries and activities. The computer lab may not be used by unsupervised children. When children under the age of 18 are using the computer lab, adult supervision must be provided to monitor computer activities and follow BELC's Safe Sanctuary Policy. Once approved by the Office and Business Manager, groups outside of BELC may use the computer lab for sponsored ministries. Their use must comply with this policy. Adult supervision is required when the computers are in use by children and behavior must be consistent with the requirements contained in BELC's Safe Sanctuary Policy.

Personal Use of the Internet

Occasional personal use of BELC IT resources and Internet access by staff and other users is allowed as long as it does not interfere with staff productivity, pre-empt business activities, or consume more than a trivial amount of resources. In addition, personal use of the Internet is prohibited if:

- It materially interferes with the use of BELC IT resources by staff or interferes with ministry activities.
- Such use burdens BELC with additional costs.
- Such use interferes with the user's employment duties or other obligations to the Church.
- Such personal use includes any activity that is prohibited under this policy.

If personal usage is determined to be excessive or inappropriate by the Office and Business Manager in consultation with the pastor(s), then limitations of use will be imposed and/or disciplinary action taken.

Internet Safety

BELC will attempt to employ reasonable filtering and/or blocking software to restrict access to Internet sites containing child pornography, obscene depictions, or other materials harmful to minors and/or inappropriate for a church and business environment. However, no software is foolproof, and there is still a risk that an internet user may be exposed to a site containing such materials. Protections will also include active adult supervision and age appropriate guidance to Internet access. If an inappropriate site is encountered by a minor, adults will ensure the site is left immediately or the computer is shut down immediately. If an adult encounters an inappropriate site, the adult will leave the site immediately.

The anti-virus, malware, and other internet protection devices, systems, and software must be kept in a state that protects both the computer and the BELC server at all times, i.e. these protections shall not be turned off by the user.

Personal information of members of Bethlehem or individuals using Bethlehem computers will not be posted online unless it is used with permission by the individual for Bethlehem business purposes.

Users of Bethlehem computers will not visit recreational chat rooms and/or arrange meetings with anyone they have met on the Internet.

E-mail

Staff and congregational officers will be issued a BELC e-mail account. E-mail accounts may be issued to volunteer positions on a case-by-case basis. Requests for e-mail accounts for non-staff individuals must be approved by the Office and Business Manager.

E-mail access will be terminated when the employee or individual terminates their association with BELC.

E-mail users are expected to remember that e-mail sent from the BELC e-mail accounts reflects on the church. BELC expects individuals to comply with normal standards of professional and personal courtesy and conduct.

Individuals at BELC using BELC e-mail are allowed to use e-mail to further the BELC vision, mission, and core values. Types of activities that are acceptable include:

- Communicating with fellow employees, members of the congregation, members of the community, and others associated with the ongoing ministries of BELC.
- Acquiring or sharing information necessary or related to the ongoing ministries of BELC.
- Participating in professional development activities.

The BELC e-mail systems and services are not to be used for purposes that could be expected to strain storage or bandwidth. E-mail use shall not interfere with others' use of the BELC e-mail system and service. The following activities are deemed inappropriate uses of BELC e-mail systems and services and are prohibited:

- Use of e-mail for illegal or unlawful purposes, including, but not limited to, copyright infringement, obscenity, libel, slander, fraud, defamation, plagiarism, harassment, intimidation, forgery, impersonation, soliciting, and computer tampering.
- Use of BELC e-mail systems and services for unsolicited mass mailings, non-BELC activity, political campaigning, dissemination of chain letters, and use by unauthorized non-employees.
- Viewing, copying, altering, or deletion of e-mail files belonging to other individuals without authorized permission.
- Opening e-mail attachments or clicking on links from unknown or unsigned sources. Attachments and links are a primary source of computer viruses and should be treated with utmost caution.
- Setting a configuration or default setting to automatically forward all e-mail to an external destination without prior approval from BELC's Office and Business Manager.
- Sharing e-mail account passwords or attempting to obtain another person's e-mail account password.
- Excessive personal use of BELC e-mail resources. Limited personal use for communication with family and friends is allowed as long as it does not interfere with staff productivity, pre-empt any business activity, or consume more than a trivial amount of resources.

Miscellaneous

Compliance with Applicable Laws and Licenses

When using Bethlehem IT resources, users must comply with all software licenses; copyrights; and all state and federal laws governing intellectual property and online activities.

Computer Availability

Bethlehem IT resources are made available primarily for the daily business activities of the church. IT resources are also made available for Sunday School purposes under the direct supervision of adults. Bethlehem does not guarantee access to computers and reserves the right to remove access to IT resources at anytime.

Backup

There shall be at least two backups of important computer files as determined by the BELC Office and Business Manager. At least one backup shall be stored in a different location, with sufficient separation to prevent loss and/or damage of both the original and the backup due to the same event (e.g., fire at the Church). The backup shall be kept in a safe and secure location, and the location shall be recorded in the Church Office.

Backups shall be updated at appropriate intervals to ensure continuity of operations should the original files be lost or damaged. Backup frequency may be determined based upon the frequency and importance of changes.

Violations/Consequences

Staff who violate this policy shall be subject to discipline, up to and including suspension or termination as defined in the BELC Staffing Handbook. If it's determined that a violation of this policy has occurred, the Congregation Council will investigate and review any allegations to determine appropriate consequences. The proper authorities (i.e. law enforcement) shall be notified as soon as possible should any illegal activities (real or suspected) involving BELC IT resource be discovered.

Other users (e.g., volunteers) who violate this policy will be banned from using BELC IT resources.

If requested, the Office and Business Manager in consultation with the pastor(s) shall determine if/when access is provided to any staff or volunteer who has previously violated the provisions of this policy.

Breach of confidentiality or inappropriate release of personal information shall require formal notification to those affected.

ATTACHMENTS

1. Computer, Internet, E-mail, and Digital Network Use Agreement
2. BELC Computer User Responsibilities

Revision	Revision Date	Review Date	Summary of Revisions
0	6/8/93	NA	<i>Policy on Computer Use</i>
1	11/2011	2013	<ol style="list-style-type: none">1. Incorporates <i>BELC Policy on Computer, Internet, E-Mail, and Digital Network Usage</i>, Revision 0, 18 October 2010 [DRAFT].2. Replaces <i>Policy on Computer Backup</i>, Revised 4/93.

Attachment 1

Bethlehem Evangelical Lutheran Church Computer, Internet, E-mail, and Digital Network Use Agreement

Each staff, volunteer, or other approved user of Bethlehem information technology resources must sign this agreement as a condition for using Bethlehem's information technology resources. Please read this agreement and the BELC Policy on Computer, Internet, E-mail, and Digital Network Usage carefully before signing this agreement. If you have any questions about these documents, please contact the Pastor or BELC's Office and Business Manager.

I hereby acknowledge that I have been given a copy of Bethlehem Evangelical Lutheran Church's Policy on Computer, Internet, E-mail, and Digital Network Usage, that I have read and understand the terms therein, and have read, understood, and initialed the User Computer Responsibilities form that follows.

I understand that Bethlehem Evangelical Lutheran Church may access and monitor my use of BELC information technology resources, including my use of the Internet, e-mail and downloaded material, without prior notice to me. I further understand that should I violate this policy, my BELC information technology resource privileges may be revoked and disciplinary action/dismissal, and/or legal action may be taken against me.

Employee/Volunteer Signature _____

Employee/Volunteer Name (Print) _____

Date _____

BELC Computer User Responsibilities

Responsibilities	Initial
1. Offices shall be locked except during office hours to protect computers from unauthorized access.	_____
2. Computers shall not be left unattended and logged in without password protection including an auto lock screen that activates after 15 minutes. Passwords shall not be physically kept in the vicinity of a computer (e.g. in a desk drawer, posted under the keyboard, etc. The password shall comply with the requirements listed in the policy. A compromised password shall be reported to the Office and Business Manager immediately.	_____
3. Visitors and unfamiliar people will be challenged if found using BELC computer resources and the Office and Business Manager immediately notified. In addition, the Office and Business Manager shall be immediately notified when any computing or communications devices are compromised.	_____
4. Users shall maintain physical control over BELC IT resources and notify the Office and Business Manager immediately if a unit is lost or stolen.	_____
5. Non-BELC computing devices shall not be connected to the BELC network, nor shall computing devices already connected to the BELC network be reconfigured without prior notification and permission of the Office and Business Manager.	_____
6. No software shall be installed or removed from a BELC computer without prior written approval of the Office and Business Manager.	_____
7. Data on a BELC computer shall be protected and is the responsibility of the computer user.	_____
8. Users shall not use BELC IT resources for any illegal activity, gambling, or to violate the laws or regulations of the United States, any state or local jurisdiction, or any other nation.	_____
9. Only limited personal use of BELC IT resources is allowed without permission of the Office and Business Manager.	_____
10. Users shall not access, display, distribute, edit, or record sexually explicit material using BELC IT resources.	_____
11. User shall not use BELC IT resources to override or circumvent any security mechanism (e.g. turn off anti-virus or malware) belonging to BELC or any other government agency, organization, or company.	_____
12. Offsite access of BELC IT resources is prohibited without written permission of the Office and Business Manager.	_____