BEREA COLLEGE INFORMATION SYSTEMS & SERVICES
NETWORK USAGE GUIDELINES

The following guidelines are of a general nature and clarify the Computer and Network Policy. The guidelines address common situations but are not meant to be exhaustive. Questions about acceptable use of Berea College computing and network resources should be directed to the Information Systems and Services department.

1. Computer and Network Policy applies to all users and usage of College owned computers and data and voice networks.

   a. The policy applies apply to all host computer systems, personal computers, software, data sets, and other resources which may be accessed by users of the Berea College data or voice communications network
   b. All network users, including Berea College faculty, staff, students or contractors or other parties are expected to comply as was agreed by their signature on the application for a network/e-mail account.
   c. By logging in to the network, a user consents to these guidelines and all other IS&S policies and procedures implemented under the Computer and Network Policy.

2. Limited personal use of computer and network resources is allowed, but priority is given to usage for College business and academic pursuits.

   a. Users of the Berea College data or voice network may access the Internet or make phone calls for personal purposes but the College is not responsible for the security and privacy of data or messages transmitted for such purposes.
   b. The College does not guarantee availability, reliability or capacity of Internet or voice connection for personal usage.
   c. Users may store a limited amount of personal data and documents not related to their work or study on a personal computer. If storage is overloaded, users may be asked to remove such personal data and documents.
   d. Users assume full responsibility for the legality of any personal data and documents stored.
   e. Users are cautioned that Internet surfing, the display of videos or the use of audio materials on a personal computer during work time is likely to distract from efficient work and may be outside the bounds of their department's acceptable practices.

3. Users of computer and network resources will abide by community decency standards, copyright restrictions and other legal requirements.

   a. Users may not utilize e-mail mailing lists, classified ads or other mass communications resources to advertise or sell regulated goods such as pharmaceuticals or firearms.
   b. Users may not utilize e-mail mailing lists, classified ads or other mass communications resources to harass, belittle or coerce other individuals or classes of persons.
   c. Users may not utilize e-mail, phone calls or other communications resources to harass or coerce another individual.
   d. Users may not utilize peer-to-peer upload/download software or services to obtain or distribute copyrighted material not specifically authorized to the service.

4. Users may not modify the campus network wiring or configuration.

    a. Network hubs, switches or wireless routers may not be added to an existing port.
    b. Personal computers may not be configured to serve as routers or gateways to other networks, internal or external to Berea College.
    c. Network names of computers, printers and other network attached devices may not be changed.
    d. Network wires may not be cut, spliced or moved from their installed location.

5. Users may not engage in activities which degrade network performance or which interfere with other users' access to computer and network resources.

    a. Intentional spreading or creation of computer viruses is prohibited.
    b. Overloading network services by using hacking tools, e-mail spamming or other means are prohibited.
    c. Overloading network storage areas with personal or unnecessary data is prohibited.
    d. Initiation or propagation of e-mail chain letters is prohibited.

6. Users may not attempt to circumvent system security or information protection mechanisms.

    a. Use of hacking techniques to uncover security loopholes or to circumvent network security and gain access to folders, databases, hardware, or other material on the network to which one is not authorized is will not be tolerated.
    b. Any network user found to have hacking software or paraphernalia installed on a computer connected to the campus data network will face immediate suspension of network access privileges and may be subject to further disciplinary action.
    c. Any attempt to guess other user's passwords, access codes or encryption keys is forbidden.

7. Users must respect institutional data confidentiality and others' privacy.

    a. Unauthorized monitoring of electronic communications is forbidden.
    b. Attempts to gain unauthorized access to private information will be treated as violations of privacy, even if the information is publicly available through authorized means.
    c. Searching through directories to find unprotected information is a violation.
    d. Special access to information or other special computing privileges are to be used in performance of official duties only. Information obtained through special privileges is to be treated as confidential.
    e. As it relates to sensitive college data maintained on college-owned computers the following applies:
        1. **Computers/Laptops:** IS&S is responsible for the disposal of all College-owned computers, laptops and similar devices. Drives on these computers are wiped to DoD-3 standard before the unit is sold or sent to recycling.
        2. **CD's/DVD's:** Standard practice is to shred CD's and DVD's using standard paper shredders with built in capacity to shred this media. IS&S maintains such a shredder for this purpose.
        3. **External Hard Drives:** External hard drives including USB drives should be wiped to DoD-3 standards before disposal. Free software is available to do this such as CCleaner at http://www.piriform.com/ccleaner.

8. Users are responsible for all actions initiated from their login ID(s).

   a. Each user is assigned a personal login ID with a unique name associated with their College student or employee records.
   b. Users should not share access to their personal login ID with others.
   c. In some situations, a user may also be issued a non-standard ID which can be used on specific computers for a particular function. The owner of a non-standard ID may share that ID with others, but he or she is responsible for all activity that occurs in sessions logged in under that ID.
   d. Passwords must be chosen in such a way that they cannot be easily guessed. Network software will enforce a minimum level of password complexity.
   e. Workstations should be logged off or locked when left unattended.
   f. Users may set up network sharing on a personal computer issued for their use in order to provide other users access to data or other resources. However, individuals are responsible for the content and legality of any information they choose to share.
   g. Users should avoid storing on paper on in computer files their passwords or other information that could be used to gain access to other campus computing resources.
   h. Network storage is provided to each individual user and to many groups such as employees in a department or students enrolled in a class. Network storage may be used only to store material associated with a user’s work or study.
   i. Network software will enforce storage size limits on network storage resources. Users are responsible for managing their stored data and documents within these size restrictions.

9. Users must comply with software licensing terms.

   a. Software licensed to Berea College may not be installed on a computer not owned by Berea College.
   b. Personal computer users may not install copyright protected software not licensed to the College on a College owned computer.
   c. Personal computer users may install public domain or open source software on their computer, but are cautioned that installing such software may disrupt the efficient operation of the computer. If the computer requires service such software may be removed.

10. Access to network resources is provided only to those officially associated with Berea College.

    a. Withdrawn student accounts and stored data and documents will be deleted immediately upon receipt by IS&S of official notification of the change in status.
    b. Graduated student accounts and stored data and documents will be deleted between two and four weeks after their graduation.
    c. Faculty, staff or contractor accounts will be disabled or deleted when a user ceases official association with Berea College. All data and documents stored on personal computers or personal network folders will be deleted or copied to another location at the discretion of the departing individual’s supervisor.
    d. When faculty, staff or contractors are assigned a new position and/or responsibilities within Berea College, access associated with the former position will be revoked and access associated with the new position must be requested.
    e. No services will be provided to outside organizations or agencies that would normally be provided by other public or private agencies within the geographical areas of the

campus without the prior approval of the campus president or authorized vice president designee.

11. Information Systems and Services manages all network resources.

    a. Only Information Systems and Services personnel or those authorized by the Chief Information Officer may be given physical access to College network servers, switches, routers and other equipment.
    b. Individual departments may operate a server connected to the campus network only with explicit permission from Information Systems and Services. Application for such permission is by letter to the Chief Information Officer. An application letter needs to include the need, use, and information content of the server and needs to identify a Berea College faculty or staff member who will be ultimately responsible for the use, maintenance and content of the server.
    c. IS&S system administrators may access user's files for the maintenance of networks and computer and storage systems (e.g., to create backup copies of data).
    d. IS&S system administrators will not intentionally inspect the contents of data files or e-mail messages or disclose such contents to any person other than the owner, sender, or an intended recipient without the consent of the owner, sender, or an intended recipient unless required to do so by law or to investigate complaints regarding files or documents alleged to contain material contrary to Berea College policies or applicable laws.

Issued August 9, 2001

Revised January 27, 2013 by John Lympany