Acceptable Use Policy

Network Access and Computer Hardware/Software

Rights and Obligations

Purpose:

To establish guidelines for County-owned hardware and software, computer network access and usage, Internet and email usage, and security and privacy for users of the Blount Count Schools Local and Wide Area Networks.

Objectives:

- Ensure the protection of proprietary, personal, privileged, or otherwise sensitive data and resources that may be processed in any manner by the County Schools, or any agent for the County Schools.
- Provide uninterrupted network resources to users.
- Ensure proper usage of networked information, hardware, and software offered by the Blount County Schools networks.
- Maintain security of and access to networked data and resources on an authorized basis.
- Secure email from unauthorized access.
- Protect the confidentiality and integrity of files and programs from unauthorized users.
- Inform users there is no expectation of privacy in their use of County-owned hardware, software, or computer network access and usage.
- Provide Internet and email access to the users of the Blount County Schools networks.

Scope:

This Acceptable Use Policy applies to all individuals who have been provided access rights to the Blount County Schools networks, County Schools provided email, and/or Internet. The scope does not include County Schools phone systems, fax machines, non-networked copiers, County Schools issued cell phones or pagers unless those services are delivered over the County's network.

Use and Prohibitions:

1. Network Resources

County School employees, students, and vendors, and other governmental agencies may be authorized to access county network resources to perform business or educational functions with, or on behalf of the County Schools. Users must be acting within the scope of their employment or contractual relationship with the County Schools and must agree to abide by the terms of this agreement as evidenced by his/her signature.

Prohibitions

- Sending or sharing with unauthorized persons any information that is confidential by law, rule or regulation.
- Installing software or hardware that has not been inspected and authorized by the Technology Department.
- Attaching any device that has not been authorized by the Technology Department.
- Attaching non-county owned computers without written permission from the Technology Department.
- Using network resources to play or download games, music or videos that are not in support of business or educational functions.
- Leaving workstation unattended without engaging password protection for the keyboard or workstation.
- Utilizing unauthorized peer-to-peer networking or peer-to-peer file sharing.
- Using network resources for or in support of unlawful activities as defined by federal, state, and local law.
- Utilizing network resources for activities that violate conduct policies established by the Board of Education or the user's Department.

1. Email

Email is provided to expedite and improve communications among network users.

Prohibitions

- Sending unsolicited junk email, advertising, items-for-sale postings, or chain letters (e.g. "spam") to any users of the network.
- Knowingly ending any material that contains viruses, Trojan horses, worms, time bombs, cancel bots, or any other harmful or deleterious programs.
- Sending copyrighted materials via email that is either not within the fair use guidelines or without prior

permission from the author or publisher.

- Sending or receiving communications that violate conduct policies established by the Board of Education or the user's department.
- Sending confidential material to an unauthorized recipient, or sending confidential e-mail without the proper security standards (including encryption if necessary) being met.

Email created, sent or received in conjunction with the transaction of official business are public records in accordance with T.C.A 10-7-401 through 10-7-404, and the rules of the County Public Records Commission. A public record is defined as follows:

"*Public record(s)" or "county record(s)" means* All documents, papers, records, books, and books of account in all county offices, including, but not limited to, the county clerk, the county register, the county trustee, the sheriff, the county assessor, the county executive and county commissioners, if any; The pleadings, documents, and other papers filed with the clerks of all courts, including the courts of record, general sessions courts, and former courts of justices of the peace, and the minute books and other records of these courts; and The minutes and records of the county legislative body*(T.C.A. 10-7-403).*

County Schools records are open to public inspection unless they are protected by County, State or Federal law, rule, or regulation. Because a court could interpret county records to include draft letters, working drafts of reports, and what are intended to be casual comments, be aware that anything sent as electronic mail could be made available to the public

1. Internet Access

Internet access is provided to network users to assist them in performing the duties and responsibilities associated with their positions.

Prohibitions

- Using the Internet to access non-County Schools provided web email services.
- Using unapproved Instant Messaging or Internet Relay Chat (IRC).
- Using the Internet for broadcast audio for non-business use.
- Utilizing unauthorized peer-to-peer networking or peer-to-peer file sharing.

- Using the Internet when it violates any federal, state or local law.

STATEMENT OF CONSEQUENCES

Noncompliance with this policy may constitute a legal risk to the Board of Education, an organizational risk to Blount County Schools in terms of potential harm to employees or citizen security, or a security risk to the Blount County Schools Network Operations and the user community, and/or a potential personal liability. The presence of unauthorized data in the County Schools network could lead to liability on the part of the Board of Education as well as the individuals responsible for obtaining it.

STATEMENT OF ENFORCEMENT

Noncompliance with this policy may result in the following immediate actions.

1. Written notification will be sent to the non-complying employee, the Department Head and to the Director of Schools to identify the user and the nature of the noncompliance as “cause”. In the case of a vendor, the vendor will be notified.
2. User access may be terminated immediately by the Supervisor of Technology, and the user may be subject to subsequent review and action as determined by the Director of Schools.