Book	Policy Manual
Section	800 Operations
Title	Responsible Use of Digital Technology
Code	815
Status	Active
Adopted	August 15, 2007
Last Revised	November 18, 2020

Objective

BLaST Intermediate Unit 17 recognizes the value of using online computer resources and networks to gather information, promote communications and enhance student learning. In working to achieve its mission and vision, the Intermediate Unit also recognizes the need for responsible, ethical use of these resources in the delivery of curriculum, professional development, instruction and the business operations of the Intermediate Unit. This policy establishes the parameters in which guidelines and procedures for students, staff and community are to function.

Provisions

All uses of Intermediate Unit network facilities are intended to support and advance the educational mission of the Intermediate Unit. It is the policy of the Intermediate Unit to prevent user access over its computer network to inappropriate materials via the Internet; prevent unauthorized access and other unlawful online activity; prevent unauthorized online disclosure, use, or dissemination of personal identification information of minors; and comply with the Children's Internet Protection Act [Pub. L. No. 106-554 and 47 USC 254(h)].[1]

The Intermediate Unit will provide:

1. The software and hardware necessary to make the networks function effectively and efficiently.
2. Educational materials and training for network use as appropriate.
3. Appropriate staffing to administer, operate and support the Intermediate Unit systems.

The Intermediate Unit will develop and communicate:

1. Changes as appropriate.
2. Policies and procedures regarding use as appropriate.
3. Policies and procedures that protect the rights of users and their property and ensures the legal use of all software and protected materials (i.e. copyright, etc.)

The Intermediate Unit will:

1. Secure its networks and computing systems in reasonable and cost effective ways while making them accessible for authorized and legitimate use.

2. Maintain its networks and computing systems to ensure reliable, efficient and effective use.

3. Inform users of expected standards of conduct and disciplinary measures for not adhering to them.

4. To the extent practical, use technology protection measures (or "Internet filters") to block or filter Internet, or other forms of electronic communications, access to inappropriate information. Specifically, as required by the Children's Internet Protection Act, blocking shall be applied to visual depiction of material deemed obscene or child pornography, or to any material deemed harmful to minors. Subject to staff supervision, technology protection measures may be disabled or, in the case of minors, minimized only for bona fide research or other lawful purposes. The use of Intermediate Unit networks and computing systems is a privilege that requires users to adhere to the policies and procedures established by the Intermediate Unit. Violations will result in disciplinary action in accordance with Intermediate Unit discipline policies and may include loss of privileges or appropriate legal action.

The responsibility of the user is to:

1. Adhere to all applicable state and federal laws.

2. Adhere to all Intermediate Unit policies, procedures and guidelines.

3. Use Intermediate Unit networks and computing systems to further the mission of the Intermediate Unit and promote a positive learning environment.

4. Respect the rights of others and their work at all times.

5. Not disrupt the use or operation of Intermediate Unit networks or computing systems.

6. Not hold the Intermediate Unit liable for lost or disrupted information or services.

Use of Social Media

Social media are online applications, services, and practices that allow users to connect to each other and to create, share, and collaborate on content.

BLaST Intermediate Unit 17 recognizes the importance of open exchange and learning between the Intermediate Unit and its many constituents. We recognize the two-way communication available through social media — blogging, social websites, and networking — as an important arena for interaction and collaboration, to learn from and connect with others using these communications tools.

Where appropriate, the Intermediate Unit supports the use of social media by employees in pursuit of instructional and educational goals. The Intermediate Unit may use social media to connect with students, parents, faculty, staff, alumni, colleagues, other educators, and more. Please refer to the Intermediate Unit’s Social Media Guidelines (attached) for guidance on using social media effectively, safely, and within Intermediate Unit policy.

In the best interests of our Intermediate Unit and our community, Intermediate Unit staff and students who administer or use official social media sites on behalf of the Intermediate Unit must adhere to all existing policies, especially Policy 249 Anti-Bullying and Anti-Cyber Bullying and Policy 814 Copyright Materials, as well as the Professional Code of Conduct for Educators (Chapter 235).[2][3]

Educational Network Guidelines

The Intermediate Unit strives to provide the most up-to-date technologies and information possible, recognizing their potential to enhance learning. However, network use involves many ethical questions and issues. Parents and guardians are urged to contact the Intermediate Unit to discuss any policies and procedures that may be unclear to them, as well as the proper and ethical use of networks before approving their use by a child.

The Intermediate Unit will educate students annually on network etiquette and other online behavior, including:

1. Interaction with other individuals on social networking web sites and in chat rooms.
2. Cyberbullying awareness and response.

All uses of the Intermediate Unit network facilities are intended to support and advance the Intermediate Unit's educational mission/vision or other purposes as deemed appropriate by the Intermediate Unit's Board of Directors.

Access accounts for networks in the Intermediate Unit are governed by the policies and procedures established by the Intermediate Unit. Individuals applying for and accepting a User ID are making a commitment to adhere to those policies and to conduct themselves according to the highest standards.

Use Guidelines

Access to inappropriate material as defined by school policy and by the Children's Internet Protection Act is prohibited. To the extent practical, steps shall be taken to promote the safety and security of users of the Intermediate Unit's online computer network with using electronic mail, chat rooms, video conferencing, livestreaming (Policy 815.1), or other forms of direct electronic communications.[4]

Generation and/or transmission of any material in violation of any federal, state, or Intermediate Unit regulation is prohibited. This includes, but is not limited to: violation of copyrights; using other protected materials without permission of the author; using threatening, obscene or racist language or material: unauthorized access, including so-called "hacking," unauthorized disclosure, use, and dissemination of personal identification information regarding minors.

Network administrators and supervising staff members have the discretion to determine inappropriate use. Violations may result in loss of privileges pursuant to IU discipline procedures and/or legal action.

These guidelines will be revised and updated as needed.

User IDs

Computer network accounts assigned to individuals consist of a unique User ID code and password combination. Users are not permitted to share accounts or passwords. Directory of services may also be securely connected to other Single Sign-On authentication services or other Federation/SAML authentication services to access platforms which use one set of credentials to access. Employees should understand that the security of multiple applications utilize one set of credentials.

Accounts will provide access to electronic mail, information and news, access to databases and web sites. All accounts will be issued for limited time frames. Accounts will be reviewed and extended as needed.

Security

Users will be responsible for keeping individual accounts secure by keeping passwords secret and by using the client software provided by IU servers. The Intermediate Unit has installed several security measures to ensure appropriate usage.

Any user(s) that has a history of computer misuse may be denied access to an account. Use of encryption technology must be done with prior approval by the network administrator.

Users, who believe they have identified a security problem, must notify an appropriate authority with the details of the problem as soon as possible.

Supervision and Monitoring

It shall be the responsibility of all members of the Intermediate Unit staff to supervise and monitor usage of the online computer network and access to the Internet in accordance with this policy and the Children's Internet Protection Act.

Procedures for disabling or otherwise modifying any technology protection measures shall be the responsibility of the Director of Management Information Services or designated representative.

Liability

The BLaST Intermediate Unit does not guarantee service nor is it responsible for damaged or incorrect data. Use of any information obtained on the Internet or other network services must be undertaken at the individual's own risk.

The Intermediate Unit shall not be held liable for the actions of individuals who choose to violate the acceptable uses of the network. In addition, each user and/or user's parent(s) or guardian(s) shall indemnify the Intermediate Unit and hold it harmless from and against any damage, liability, loss, or deficiency arising out of or resulting from the user's use and/or misuse of the network.

Vandalism

Vandalism includes any attempt to harm any hardware or software, or the data of another user of the network. This includes, but is not limited to the uploading or creation of viruses, worms or trojans. Unauthorized attempted entry to any computer system is grounds for cancellation of a user's account, and could be referred to the appropriate legal authorities. Physical harm may include physical damage to IU-issued technology by students or staff.

Privacy

Email is not guaranteed to be secure. The user should assume that communications sent via a network should be thought of as communications sent via post card. The IU provides no facilities for secure communications. In addition, the IU may access e-mail and/or files stored in user accounts where there is reason to suspect misuse.

Network Etiquette

Users of Intermediate Unit networks and computer systems are expected to follow accepted network etiquette procedures at all times.

Social Media Guidelines

Use of Social Media -

Social media are online applications, services, and practices that allow users to connect to each other and to create, share, and collaborate on content. BLaST Intermediate Unit recognizes the importance of open exchange and learning between the IU and its many constituents. We recognize the two-way communication available through social media—blogging, social websites, and networking—as an important arena for interaction and collaboration, to learn from and connect with others using these communications tools.

Where appropriate, the IU supports the use of social media by employees in pursuit of instructional and educational goals. The organization may use social media to connect with students, parents, faculty, staff, colleagues, other educators, and for marketing goods and services. The guidelines below are to be used for guidance on using social media effectively, safely, and within the IU’s policy.

In the best interests of our IU and the community, staff and/or students who administer or use social media sites on behalf of the IU must adhere to all existing policies, especially Policy 249 Anti-Harassment and Anti-bullying and Policy 814 Copyright Materials, as well as the Professional Code of Conduct (Chapter 235). Generally speaking, social media refers to the digital tools that we use to interact among each other, to create, share and exchange information, ideas, and media in online

virtual networks. Specifically, examples of social media include commonly used tools such as Facebook, Twitter, Pinterest, Flickr, and LinkedIn. These are just a few examples of social media; these and all other examples of social media fall under the application guidelines.[2][3]

Who needs to apply? Apply if you want to use social media on behalf of the Intermediate Unit programs and services: Employees/volunteers who wish to create, administer, or use a social media platform on behalf of the IU, or one of its programs or services, must apply for permission.

If staff are asking students to use social media, web-based tools and applications, these tools and applications must appear on the 'IU 17 Approved for General Use List' published on the IU website. This list includes a training video that provides orientation of safe and effective use which should be viewed by the staff prior to student use.

If an application/tool does not appear on the 'IU 17 Approved for General Use List,' then staff should apply for the consideration of adding the application/tool to the list by submitting a 'Request for Application Approval Form' found on the IU website. When this electronic form is submitted, it will be reviewed by the Director of Technology and/or designee. When approval is granted, the application/tool will be added to the approved listing and notice will be provided to staff.

Personal use of social media by employees/volunteers: Application is not needed, but it is important to remember that each staff member is personally responsible for the content he/she publishes on any form of social media. This is especially important if you identify yourself as an employee of the Intermediate Unit.

Although the official policies and guidelines discussed previously apply to those uses of social media in a person's capacity as an employee of the IU, it is important to remember that each staff member is personally responsible for the content he or she publishes on any form of social media.

1. There should be clear and definite differentiation between a staff member’s personal and professional social media use.

2. When identifying oneself as an employee of the Intermediate Unit, either directly or as part of a user profile, an employee should conduct himself according to the IU’s On-Line Acceptable Use Policy, Anti-harassment Policy, and Professional Code of Conduct (Chapter 235).

3. Further, employees must comply with confidentiality obligations imposed by law, including HIPPA and FERPA (Family Educational Rights and Privacy Act).

4. Employees are prohibited from becoming “friends” with or interacting with students on their personal social networking sites. Concerns expressed by a parent or guardian will be investigated with diligence by the IU and may result in disciplinary action, if appropriate.

5. Under no circumstances may the employee use the IU logo, or other images associated with the IU in personal social media pages without express written consent of the organization.

6. Employees should not use the IU’s name to promote or endorse any opinion, product, cause, or political party or candidate.

7. The use of images or photographs of students on a personal blog, photo sharing site, or social networking web page are absolutely prohibited.

8. Under no circumstances should employees discuss situations involving employee or student discipline on their blog or social networking site.

9. Social networking sites may not be used for non-professional purposes during working hours.

Legal

1. 47 U.S.C. 254
2. Pol. 249
3. Pol. 814
4. Pol. 815.1

47 CFR 54.520

Pol. 103

Pol. 104

815Attachmt.docx (14 KB)