BLOOMSBURG AREA SCHOOL DISTRICT
Policy Manual

Section: OPERATIONS

Title: COMPUTER AND INTERNET ACCESS AND USE

Date Adopted: March 17, 1997

Date Last Revised: 16 April 2012

815. COMPUTER AND INTERNET ACCESS AND USE

.1 The Bloomsburg Area School District requires each student and employee who receives a network and/or Internet account or accesses the Internet using district hardware to first read or discuss a description of the rights and responsibilities involved in gaining this access through the Bloomsburg Area School District.

.2 Any district student or employee may apply for an Internet account. To do so, the user and his or her parent/guardian, if appropriate, must complete an acceptable use agreement and application.

.21 The student acceptable use agreement requires a parent or guardian and a teacher signature, as well as a student signature, except in the case of elementary school students. Students should return the agreement to the person from whom he/she received it.

.22 Employees should return the contract to the office of the System Administrator.

.23 Applicants should retain a copy of the Terms and Conditions for their files.

.24 By signing these forms, Bloomsburg Area School District Network, Internet, and hardware users are agreeing to the terms and conditions set forth in the Terms and Conditions document.

.3 The reference to the BASD Network includes any and all networks that are constructed throughout the Bloomsburg Area School District.

.4 The Bloomsburg Area School District shall take precautions to restrict access to controversial materials. However, on a global network it is impossible to control all materials, and an industrious user may discover controversial information. We

firmly believe that the valuable information and interaction available on this worldwide network far outweighs the possibility that users may procure materials that are not consistent with the educational goals of the district. Users of the network who deliberately access inappropriate or illegal material will lose their Bloomsburg Area School District network privileges and may be subject to further disciplinary actions. Any instances involving child pornography will immediately be referred to law enforcement.

.5 The Bloomsburg Area School District recognizes the vast, diverse, and unique resources that the BASD Network and Internet Access offer to students, teachers, administrators, and staff, and how this service can promote educational excellence in schools by facilitating innovative resource sharing and communication.

.51 All uses of school technology and/or the BASD Network and the Internet should be in support of education and research, and consistent with the purposes of the Bloomsburg Area School District.

.52 The Internet will be used to support the district's curriculum, the educational community, projects between and among schools, communications, and research for district students, teachers, administrators, and staff.

.6 The Bloomsburg Area School District reserves the right to log BASD Network and Internet use, and to monitor fileserver space utilization by district users, while respecting the privacy right of both district users and other outside users. The school district reserves the right to remove a user account from the network to prevent further unauthorized or illegal activities. Authorized staff members are permitted to view student home directories that are stored on the BASD network.

.61 All data on the Bloomsburg Area School District's servers, PCs, laptops, or network is considered property of the Bloomsburg Area School District and can be accessed at any time necessary by the system administrator(s) and superintendent.

.7 Terms and Conditions

.71 Acceptable Use

The purpose of accessing the BASD Network and/or the Internet is to support education in and among the schools in the Bloomsburg Area School District, by providing access to unique resources and the opportunity for collaborative work. The use of an account must be in support of education, academic research, and consistent with the educational objectives of the school district. Use of other organizations' networks or computing resources, must comply with the rules appropriate for that network and is the responsibility of the user using that network or computer resource. Transmission of any material in violation of any U.S.

or state regulation is prohibited. This includes, but is not limited to: copyrighted, threatening, obscene, or pornographic material, or material protected by trade secret or property law.

Use for product advertisement, for-profit purposes or political lobbying is generally not consistent with the purposes, goals, and ideals of the district. Illegal activities are strictly prohibited. Hate mail, harassment, discriminatory remarks, and other antisocial communications on the BASD Network or Internet is prohibited.

.72 Privileges

The use of the BASD Network and/or Internet is a privilege, and inappropriate use can result in the cancellation of those privileges. Each student who receives an account will take part in a discussion with an adult pertaining to the proper use of the Network and Internet. Based upon the acceptable use guidelines outlined in this policy, the System Administrator(s) and Technology Coordinator will deem what is inappropriate use of the BASD Network and/or Internet Access and may take appropriate action. The System Administrator(s), principals and assistant principals may suspend or close an account at any time as required. They must notify the user and, if appropriate, the parent/guardian in writing within two weeks of the reason for suspension or termination of an account. The administration, faculty, and staff of the district may also request the System Administrator(s) and/or Technology Coordinator to deny, revoke, or suspend specific user accounts. Students and employees whose accounts are denied, suspended or revoked may appeal that decision through existing school building and district-wide policies and procedures.

.73 Etiquette on the BASD Network and Internet

The user is expected to abide by the generally accepted rules of network etiquette. These include, but are not limited to, the following:

.731 Be polite. Do not write or send abusive or offensive messages to others, including hate mail or antisocial communications.

.732 Use appropriate language. Do not swear, use vulgarities, or inappropriate language.

.733 Do not reveal your personal address or phone number or those of student colleagues, teachers, and staff.

.734 Note that electronic mail (e-mail) is guaranteed to be not private. People who operate the system do have access to all mail. Messages relating to, or in support of illegal activities, will be

reported to the appropriate authorities. Users and their access may be monitored at any time. Prior consent of the user need not be obtained for such monitoring.

.735 Do not use the BASD Network and/or Internet in such a way that you would disrupt the use of the network by other users.

.736 All communications and information accessible via the BASD Network and/or Internet, should not be assumed to be private property.

.74 The Bloomsburg Area School District makes no warranties of any kind, whether expressed or implied for the service it is providing. The district will not be responsible for any damages that a user may suffer. This includes loss of data resulting from delays, non-deliveries, mis-deliveries, or service interruptions caused by its own negligence or user errors or omissions. Use of any information obtained via the BASD Network and/or Internet is at the user's own risk. The district specifically denies any responsibility for accuracy or quality of information obtained through its services.

.75 Security on any computer system is a high priority, especially when the system involves many users. If a user feels that he/she can identify a security problem through either the BASD Network and/or Internet Access, the user must notify a System Administrator or the principal or assistant principal immediately. Do not demonstrate the problem to others. Do not use another individual's account without written permission from that individual. Do not give your password to any other individual. Attempts to log in to the system as any user other than yourself may result in cancellation of user privileges. Attempts to login to either the Network and/or Internet as a System Administrator will result in immediate cancellation of the user's privileges. Any user identified as a security risk, or having a history of problems with other computer systems will be denied access to the BASD Network and/or Internet.

.76 Vandalism will result in cancellation of privileges. Vandalism is defined as, but not limited to, the following: any attempt to alter or destroy data of another user; any attempt to harm or destroy data on the Network and/or Internet, or any other networks that are connected to the BASD Network structure. This includes, but is not limited to, the uploading or creation of computer viruses, or the intentional misuse or vandalism of software or hardware.

.77 The district may occasionally require new registration and account information from the user in order to continue service. The user must notify either a System Administrator or the Technology Coordinator of any changes in his/her account information.

.78 All terms and conditions as stated in this document are applicable to the district Network and Internet Accesses provided by the district. These terms and conditions shall be governed and interpreted in accordance with all Pennsylvania and federal laws and regulations, as well as all CIPA requirements.

.79 Internet Safety Policy

.791 It is the policy of Bloomsburg Area School District to: (a) prevent district network access to or transmission of inappropriate material via the Internet, electronic mail, or other forms of direct electronic communications; (b) prevent unauthorized access and other unlawful online activity; (c) prevent unauthorized online disclosure, use, or dissemination of student personal information; (d) provide Internet safety education to students and (e) comply with the Federal Communications Commission's Children's Internet Protection Act (CIPA).

.792 Bloomsburg Area School District takes reasonable measures to ensure that students do not access material and content that is potentially harmful to minors. As required by CIPA, Bloomsburg Area School District utilizes a technology protection measure ("filter") that blocks access to material that is potentially harmful to minors. The filtering technology blocks Internet content and visual depictions including, but not limited to: pornography, child pornography, sexual acts or conduct, and other obscene material that may be deemed harmful to minors.

.793 Bloomsburg Area School District provides instruction to minors on the topics of Internet Safety and appropriate online behavior. Internet Safety education topics include, but are not limited to: online behavior and ethics, social networking safety, chat room safety, cyberbullying awareness and response and other online privacy and security issues.

.8 Electronic records shall be maintained in accordance with the Bloomsburg Area School District Records Management Policy.

Bloomsburg Area School District
Acceptable Use of Internet Guidelines

1. Introduction

The Bloomsburg Area School District Board of Directors requires that all users of the Bloomsburg Area School District network read and agree to the terms set forth in the "Acceptable Use of Internet" policy before signing the "Acceptable Use of Internet Agreement." Failure to comply with the terms of this agreement could result in the cancellation of the user's account and/or computer usage privileges. Students will also need signed parental permission to use the Internet.

The goal of the Bloomsburg Area School District (BASD) network is to promote educational excellence by facilitating resource sharing, innovation, and communication that is consistent with the district's curriculum, policies and mission. The BASD network is to be used to promote the exchange of information for educational purposes. Non-educational activities are prohibited.

The smooth operation of the BASD network relies upon the proper conduct of the end users who must adhere to strict guidelines. The end users are responsible for the manner in which they access or transmit information through the BASD network and the Internet. The BASD network is to be used for educational purposes, such as daily operations, classroom activities, professional or career development, and administrative applications. This policy is intended to provide the guidelines and responsibilities of the end user in regards to acceptable use of the BASD network.

2. Authority

The electronic information available to students and staff via the BASD network does not imply endorsement by the BASD, nor does the BASD guarantee the accuracy of information received. The BASD will not be responsible for any information lost, damaged, or unavailable when using the network, or for any information that is retrieved from the Internet. The BASD shall not be responsible for any unauthorized charges or fees resulting from access to the Internet.

The Internet is a vast global network connecting a great number of computers around the world and therefore inappropriate materials, including those that may be profane, pornographic, or otherwise offensive, may be accessed through the network. The BASD has technology in place to block out this inappropriate material, but due to the increasing size of the Internet, it is impossible to completely block out all inappropriate material. Accessing these and similar types of resources will be considered an unacceptable use of school resources and will result in suspension of network privileges and/or disciplinary action as outlined in appropriate discipline policies.

BASD reserves the right to monitor and log network use as well as restrict storage space and bandwidth utilization. The use of the BASD network is a privilege and not a right. Inappropriate, unauthorized, and illegal use will result in cancellation of those privileges and appropriate disciplinary action. Excess e-mail or files taking up an inordinate amount of fileserver disk space may be removed by system administrators, after a reasonable time and after notification to the user.

3. Netiquette

Users are expected to abide by the rules of network etiquette. These include (but are not limited to) the following:

- Be polite. Do not get abusive in your messages to others.
- Use appropriate language. Do not swear or use vulgarities or any other inappropriate language. Illegal activities are strictly forbidden.
- Do not reveal your personal address, network password, or phone numbers of students or colleagues.
- Do not use the network to threaten, curse, or intimidate others.
- Note that electronic mail and network folders are not guaranteed to be private. Building and system administrators reserve the right to review all system content. Messages relating to, or in support of, illegal activities may be reported to authorities.
- Do not use the network in such a way that you would disrupt the use of the network by other users.

4. Guidelines

It is essential for each user on the network to recognize his/her responsibility in having access to vast services, systems, and people. The user is ultimately responsible for actions in accessing network services. Users of the network must abide by the following rules. The following operational activities and behaviors are as prohibited:

1. The BASD network may not be used for: (a) private, commercial, for-profit, or business (except where such activities are otherwise permitted or authorized under appropriate school policies); (b) unauthorized fundraising; (c) advertising; or (d) unauthorized use of the BASD name.
2. Product advertisements and political lobbying or organizing is prohibited.
3. Use of the BASD network to access obscene or pornographic material is expressly prohibited.
4. Sending offensive or objectionable materials to recipients is expressly prohibited.
5. Using programs that harass BASD network users or infiltrate a computing system and/or damage the software components is expressly prohibited.
6. Use of the BASD network for hate mail, harassment, discriminatory remarks, offensive and/or inflammatory communications, or to transmit offensive or objectionable material to recipients is prohibited.
7. Use of the BASD network to transmit inappropriate, rude, vulgar, lewd, profane, inflammatory, threatening and disrespectful language is prohibited.

8. Use of the BASD network to impersonate or misrepresent other users, or the use of anonymity, pseudonyms, encryption, or other technology to avoid detection or identification is prohibited.

5. **Software and Hardware**

Users are expected to abide by the rules of the "Software and Hardware" section of this policy.

1. BASD computers are configured and maintained for educational and administrative purposes only and should not be viewed as the personal equipment of the user; therefore, the right is reserved to restrict configuration and installation of software and hardware on all school computers.
2. Any software installed on BASD computers must be licensed in accordance with the law. A separate license must be purchased for each computer upon which the software is installed. A copy of all licenses must be forwarded to technology department staff before installation.
3. Users may not make unauthorized copies of copyrighted software.
4. Users may not install any unauthorized games, programs, files, or other electronic media on school computers.
5. Users may not move or remove equipment or install/configure hardware or software without authorization by technology department staff.
6. Users may not physically damage or destroy hardware, alter or destroy data of another user, harm or destroy data on the network and/or the Internet by the introduction of worms or viruses, or any other networks that are connected to the BASD network structure. Vandalism, including theft of computer components, will result in monetary damages paid by the perpetrator, as well as disciplinary action according to school policy.

6. System Security

Users are expected to abide by the rules of the "Systems Security" section of this policy.

1. Users may not give others access (via password or other means) to computing resources to which they are not entitled.

2. Users' passwords should be a combination of letters, numbers, and symbols.

3. Users may not use a computer that has been logged in under another student or employee's name. Use of the network to intentionally obtain or modify files, passwords, and data belonging to other users is prohibited, as is impersonation of another user, anonymity, and pseudonyms.

4. Users may not modify technology resources, utilities, and/or configurations, or change the restrictions associated with their accounts, or attempt to breach any technology resources security system, whether with malicious intent or not.

5. Users may not engage in malicious hacking, i.e. deliberately breaking into a system to alter or damage it for the purpose of gaining illegitimate access to resources or information.

6. Users may not create, implement, or host their own servers or services using school resources.

7. Administrative or office computers should be utilized for their intended functions and should not be available to other users for general or personal use.

8. The district will educate minors about appropriate online behavior. This includes interacting with other individuals on social networking Web sites, in chat rooms, and cyber-bullying awareness and response.

7. Privacy

1. Users are responsible for the use of their individual account and should take all reasonable precautions to prevent others from being able to see their account, including logging off when away from the computer, especially if the computer is in an educational or insecure workplace setting. Unless authorized, users should not provide their password to another person. In the event that a user's password/login is used by another in violation of the BASD "Acceptable Use of the Internet" policy, both parties will be subject to consequences which may include, but are not limited to, the loss of network privileges, as well as possible disciplinary action as outlined in appropriate district policies.

2. Users may not read, execute, modify, or delete any file belonging to someone else without explicit permission from the owner, even if the file is unprotected.

3. An authorized system administrator may remove or alter as necessary user files that threaten to interfere with the operation of the network, or as needed for system maintenance such as files infected with a virus, unauthorized programs that have adverse effects to the infrastructure, or files containing copyright infringements. The system administrator should make every effort to notify the user prior to such action to give the user opportunity to remove such files him/herself. It is recognized that there may be special cases where the threat to the effectiveness of system resources is so immediate that prior notification is not possible.

4. Users are responsible for creating backup copies of critical files.

5. The use of personal (non-school) computers and or hardware (printers, etc.) on the network will not be supported. Personal computers should be registered with the technology department and include appropriate serial numbers and ownership information. BASD is not liable for any damage done to personal computers. BASD-owned hardware components may not be installed in a personal computer.

6. Users have no expectation of privacy in their e-mail messages and/or files that are contained with the BASD network. The BASD may intercept or access files and or e-mails at any time for any reason.

7. The district may occasionally require new registration and account information from users, in order to continue service. Users must notify either a system administrator or the technology coordinator of any changes in his/her account information.

8. All terms and conditions as stated in this document are applicable to the district network and Internet accesses provided by the district. These terms and

conditions shall be governed and interpreted in accordance with all Pennsylvania and federal laws and regulations, as well as all CIPA requirements.

8. E-mail

1. BASD e-mail is to be used for educational purposes or district- related business.
2. BASD e-mail is not to be used for personal advertisement or business, or to forward chain letters or other mass mailings that are not school related.
3. Users may not repost a message that was sent to them privately without the permission of the person who sent them the message.
4. Excess e-mail or files taking up an inordinate amount of fileserver disk space may be removed by system administrators, after a reasonable time and after notification to the user.
5. Users may not post private information about another person.
6. Network users have no privacy expectation in their e-mail messages. The school may intercept or access stored communication at any time for any reason.
7. Users may not use vulgar, abusive, profane or other offensive language in BASD e-mail.
8. Users may not discuss illegal activities on BASD e-mail.

9. Inappropriate Access to Material

1. Users may not use, attempt to use, or direct the use of the school Internet system to access material that is profane or obscene (pornography), that advocates illegal acts, or that advocates violence or discrimination toward other people (hate literature).
2. If a user inadvertently accesses such information, he or she must immediately disclose the inadvertent access in a manner specified by his or her teacher or building administrator. This will protect users against an allegation that they have intentionally violated the "Acceptable Use of Internet" policy.

10. Protection

1. The district has a software filter in place which blocks access to Web sites which may contain visual depictions and text that are obscene, contain child pornography, and are harmful to minors with respect to use by minors. As with any software filter, there are no guarantees that the filters will block 100% of the offensive material all the time.
2. An Internet usage log will be maintained and online activities of users may be monitored.
3. Students are prohibited from unauthorized disclosure or dissemination of personal identification, including but not limited, to the student's first name or last name, address, phone number, picture, or e-mail address.
4. School district employees are prohibited from the unauthorized disclosure or dissemination of information about students' records, including but not limited to, the student's first or last name, address, phone number, picture, or e-mail address.

5. Routine maintenance of the system may lead to the discovery that the user is in violation of the BASD "Acceptable Use of Internet" policy, the discipline policy, or the law.
6. An individual search may be conducted if there is reasonable suspicion that a user has violated the law or school district policies. The nature of the investigation will be reasonable and in the context of the alleged violation.
7. The expression, publication, or distribution of obscene, libelous, or slanderous materials, or materials which encourage students to commit unlawful acts, violate lawful district regulations, or cause material and substantial disruption of the orderly operation of his/her school, are prohibited.
8. When using the Internet for class activities, teachers will select material that is appropriate for the age of the students and that is relevant to the course objectives. Teachers will preview the materials and sites they require. Teachers will provide guidelines and lists of resources to assist their students in their research activities. Teachers will assist their students in developing the skills to ascertain the truthfulness of information and to distinguish fact from opinion.
9. Internet downloads will be restricted to those files that have an educational purpose within the guidelines of the curriculum or in accordance with the requirements of one's job position.

11. Chat Rooms and Other Direct Electronic Communications

1. Students are prohibited from access to chat rooms, Internet e-mail, or instant messaging software, services, and servers outside of the BASD Network.
2. Teachers may utilize online chats and instant messaging for educational purposes only. Students may observe these activities, but may not be the administrator of such activities.

12. Copyright Issues

1. Users will be subject to the Federal Copyright Law. The U.S. Copyright Law grants authors certain exclusive rights of reproduction, adaptation, distribution, performance, display, attribution and integrity to their creations, including works of literature, photographs, music, software, film, and video. Violations of copyright laws include, but are not limited to, the making of unauthorized copies of any copyrighted material (such as commercial software, text, graphic images, and audio and video recordings), distributing copyrighted materials over computer networks or through other means, and framing other Web site material and representing it as one's own.
2. Users may not plagiarize. Teachers will instruct students in appropriate research and citation practices.

13. District Web Site

1. BASD employees may not officially or unofficially represent the district on non-school Web sites. BASD is not liable for information posted on a non-BASD site.
2. Groups associated with the BASD, including but not limited to, booster clubs, parent organizations, band associations, or other associations representing school

activities, may not establish Web sites representing a school district affiliated group without review by the network director of technology before it is posted.
3. The BASD Web site was created with the intent of presenting information about each school or class activities or for educational purposes. Teachers are responsible for the content created by their students. Student-created Web pages will be posted at the discretion of and by the network director of technology or his/her designee.
4. Schools and classes may establish Web pages that present information about the school or class activities or for educational purposes. Teachers are responsible for the content created by their students. Student-created Web pages will be posted at the discretion of the network director of technology or his/her designee.
5. With the approval of the network director of technology, extracurricular organizations may establish Web pages. Advisors to the activities will be responsible for the content. Material presented on the organization web page must relate specifically to organizational activities. Disclaimers may be required stating that: "Opinions expressed on this page shall not be attributed to the BASD." The network director of technology or his/her designee will post organizational web pages, unless otherwise stipulated by the network director of technology.
6. Users will not have access to posting information on the authorized BASD Web site, unless otherwise stipulated by the network director of technology.
7. Any links occurring on school Web pages must be done in accordance with the law and must be linked to sites that have an educational purpose. When links are used on a BASD Web page, a reference must be made that states that "BASD is not responsible for the information contained on linked sites."
8. The network director of technology reserves the right to edit or remove any material posted to the authorized district Web site.
9. Advertising for commercial, political, or religious purposes is prohibited on BASD Web pages.
10. Threats or intimidating statements made in reference to persons within or outside the BASD are prohibited from being posted on any BASD Web page or resource.

14. Student Confidentiality

Information electronically published on the BASD network, including but not limited to, the BASD World Wide Web pages, shall be subject to the following guidelines:

1. Published documents or video conferences may not include a child's phone number, street address or box number, or names of other family members.
2. Documents or video conferences may not include information which indicates the physical location of a student at a given time other than the attendance at a particular school or participation in school activities.
3. Digital photographs and/or published video material must be limited to students with signed parental release forms.

4. Electronic records shall be maintained in accordance with the district's "Records Management" policy.

15. Sanctions

1. Students and employees must be aware that violations of this policy or unlawful use of the computers, wireless laptops, Personal Digital Assistants (PDAs), the Internet, and BASD network will result in disciplinary action.
2. Any user of the network will be held financially responsible for damages to BASD equipment, systems, and software due to deliberate acts of vandalism.
3. General rules for behavior and communications apply when using the network and the Internet, in addition to the policies. Loss of access and other disciplinary actions may result from inappropriate use. For example, disciplinary action may be taken for inappropriate language or behavior in using the computers, wireless laptops, Personal Digital Assistants (PDAs), the BASD network, or online services.
4. Loss of use of the BASD network, district computers, and/or Internet access could disciplinary actions; however, this policy incorporates all other relevant school policies, such as, but not limited to, the student and professional employee discipline, copyright, property, Web site development, bullying, curriculum, sexual harassment, and terrorist threat policies. Violations as described in this policy may be reported to the appropriate legal authorities, such as the Internet service provider, and local, state, and federal law enforcement.

16. Safety

To the greatest extent possible, users of the network will be protected from harassment or unwanted or unsolicited communication. Any network user who receives threatening or unwelcome communications shall immediately bring them to the attention of a teacher or administrator. Network users shall not reveal personal addresses or telephone numbers to others users on the network.

17. Definitions

BASD Network: All necessary components that affect the network's operation, including computers, copper and fiber cabling, wireless communications and links, equipment closets and enclosures, network electronics, telephone lines, printers and other peripherals, storage media, and other computers and/or networks to which the BASD network may be connected, such as the Internet or those of other institutions.

E-mail: Electronic mail. Mail composed and transmitted on a computer system or network.

Hardware: The physical components of a computer system-the computer, plotters, printers, terminals, digitizers, keyboards, mice, and so on.

Internet (Web): A network of servers linked together by a common protocol, allowing access to millions of hypertext resources. It is also known as www., W3, and the World Wide Web.

Software: Written coded commands that tell a computer what tasks to perform. For example, Word, PhotoShop, Excel, and Access are all software programs.

Users: Any one person who may have access to the BASD network. This may include, but is not limited to administrators, guests, school board members, students, support staff, and teachers.

BLOOMSBURG AREA SCHOOL DISTRICT
LAPTOP POLICY

Bloomsburg Area School District Staff must read, understand and agree to abide by this policy before receiving or checking out a Laptop. Abuse of this privilege may result in suspension of laptop privileges.

By receiving this laptop you accept responsibility for safeguarding it while it is signed out to you. Please take the following precautions:

- When leaving your workspace overnight, store your laptop in a locked drawer or cabinet.
- If you have a private office, close and lock the door if you leave during the day.
- If you take your laptop home, be sure to lock all doors when you go out. If you have a home security system, be sure it is on when you leave.
- If you are staying in a hotel, lock your laptop in a safe if your room has one. If no safe is available, lock your laptop in a suitcase when you go out.
- Keep laptop in your sight when going through airport checkpoints. Many travelers find it helpful to tape their business card to their laptops. This will help you identify your laptop in airport security.
- If you are traveling by car, lock your laptop in the trunk when you park.
- Do not use the computer in locations that might increase likelihood of damage.
- Keep food and drinks away from the computer.

If the laptop is damaged or stolen despite your having followed the guidelines listed above, it will be replaced with another laptop. If the laptop is damaged or stolen and the above procedures were not followed, either your department will assume responsibility for the insurance deductible or the employee may be responsible for the prorated cost of the laptop (first year: 100%; second year, 75%; third year, 50%; fourth year, 25%). Users are encouraged to check their home insurance policies regarding coverage. The School District will evaluate the circumstances of the theft or loss to determine if the required reimbursement should be waived.

Acceptable Use

The use of laptops, including off-site use, is strictly regulated by the School District's Acceptable Use Policy, Guidelines, and Procedures.

Virus, Hacking, and Security Protection

To ensure that virus protection and other security patches are current, laptops must be connected to the School's network and left on over night at least once a week. In the case of a significant security alert, users may be contacted by e-mail and/or voicemail, to bring in their laptops to the helpdesk to ensure proper security is enabled on the laptop.

Data Security

The following describes certain steps you should take to ensure that Data on your laptop remains Secure.

- Turn off your computer whenever you will not be using it for several hours.

- Do not open email attachments unless you are expecting them from a specific sender.
  E-mail headers can be changed or simulated, so even if you think the mail came from a friend, don't click on or open the attachment until you verify that the sender actually sent it.

- Don't let just anyone use your computer. You are responsible for all use of your computer. Do not make it easily accessible to strangers.

- Use screensaver passwords. And system passwords whenever possible.

- Use secure passwords. The security designs of some systems, such as the Bloomsburg's e-mail system, require you to enter a password. The object of having a password is to prevent others from posing as you or accessing your data. Therefore, select a password that will be familiar only to you.

- Don't download software from the Internet of unknown origin and/or unknown security.
  Some software (including screensavers) can include features that make your computer vulnerable or allow access to your personal data without your knowledge or permission.

- Make back-ups. You should regularly back up all work that you do on your computer.

- Double check and think twice about your work before sharing, printing, or transferring it anywhere else.
  Incidents have occurred recently in which data has been transferred inadvertently to non-secure sites and made public. Think twice-or consult with another person-

before sharing sensitive data. Confirm that sites to which you are sending data are themselves secure.

Bloomsburg has in place appropriate technical and security measures to prevent unauthorized or unlawful access to or accidental loss of or destruction or damage to personal data. These measures ensure an appropriate level of security in relation to the risks inherent in the processing and the nature of the personal data to be protected. Securely held personal data will only be accessible by select authorized members of staff within the District. Those members of staff with access to personal data are aware of their responsibility to protect the security of the data and have been given relevant training. Access to this information is controlled through data networks that use technologies such as password protection to limit access to authorized users. You are responsible to notify the technology department of any breech of data that may occur on your laptop.

_____

Printed Name

_____

Signature & Date