BALTIC SCHOOL DISTRICT'S INTERNET USER POLICY

(Please refer to the Parent/Student Handbooks for detailed information)

Users of the Internet are responsible for their actions in the use of the Internet. Users have to complete the required training before they have access to it. The District cannot guarantee that you will not encounter inappropriate or offensive material on the Internet. If offensive material would cause you embarrassment or other damage, you should not use the system.

INTERNET ETIQUETTE

All users of the school district's computers and networks are expected to abide by accepted rules of network etiquette. Breaches can result in harsh criticism by others on the Net and restricted access to some sources on the Internet. These rules of acceptable behavior are as follows:

1. Use of the school district's Internet access is a privilege, not a right.

2. Use of the school district's Internet is voluntary on the part of students, teachers, administration and the community.

3. Be polite and do not become abusive to others.

4. Use appropriate language. Swearing and the use of vulgarities will not be tolerated.

5. Do not reveal your personal address or phone number or that of other students or people.

6. The electronic mail (e-mail) is not guaranteed to be private. People who operate the system have access to the e-mail. Illegal activities may be reported to the authorities.

7. Communication and information accessible via the network should be assumed to be private property.

8. Focus on one subject per message and keep paragraphs and messages short and to the point.

9. Do not place unlawful information on any network system.

10. Abbreviate when possible. For an example: FYI (For Your Information).

11. Capitalize words only to highlight an important point or to distinguish a title or a heading. "Asterisks" surrounding a word can be used to make a stronger point.

12. Place your signature at the bottom of the e-mail. Your signature should include your name, position, affiliation, and Internet address.

INAPPROPRIATE USE

Inappropriate use includes, but is not limited to: intentional uses that violate the law, that are specifically named as violations in this policy, that violate the regulations of the school district or any other use that hampers the integrity or security of the school district's computer network or any computer networks connected to the Internet.

VIOLATION CONSEQUENCES

Transmission of any material in violation of any international, United States, or state law is prohibited. This includes, but is not limited to: copyright materials and threatening, harassing or obscene material.

Use of the school district Internet access for commercial "for profit" activities or product advertisements is prohibited. Vandalism and mischief while using the school district's Internet access is prohibited. Forgery of electronic mail messages, changing files belonging to users and downloading of any files into the school district's computers is prohibited.

Violations of the law, through the use of the school districts' Internet access may result in disciplinary action or litigation against the offender by proper authorities.

School disciplinary action, including suspension or expulsion, and/or appropriate legal action may be taken.

1. Preliminary determination – The school administrators with the assistance of the teacher will make the initial determination of a policy violation.

2. Student due process – Violations will be accorded due process as per school district policy.

3. Internet Access – The school administrator, as per school district policy disciplinary procedures, may deny, suspend, or revoke any Internet access as deemed appropriate.

Students who wish to use the computers and computer network of the Baltic School District including use of the Internet must sign, and have their parent/guardian sign, the agreement attached to this handbook and return the signed agreement to the school before they will be allowed access to the school computers and network.

BULLYING AND CYBER-BULLYING

Bullying and cyber-bullying are taken as very serious offenses by the Baltic School District. Students or staff who feel they are the target of bullying or cyber-bullying are encouraged to report the behavior to a school official. Information on the district anti-bullying and cyber-bullying guidelines can be found in the district policy handbook located on the school website.

TABLET POLICY, PROCEDURES, AND INFORMATION

The policies, procedures, and information within this document apply to all tablets used at Baltic High School, including any other device considered by the principal to come under this policy. Teachers may set additional requirements for computer use in their classroom.

1. **TABLET SPECIFICATIONS** - The tablet selected for use at the Baltic High School is the
2. **RECEIVING YOUR TABLET** - Tablets will be distributed each fall during “Student Registration & Tablet Orientation.” Parents & students must sign and return the Tablet Computer Protection plan and Student Pledge documents before the tablet can be issued to their child. The Tablet Computer Protection plan outlines three options for families to protect the tablet investment for the school district. Please review the Tablet Computer Protection plan included in this handbook. Tablets will be collected at the end of each school year for maintenance, cleaning, and software installations. Students will retain their original tablet each year while enrolled at BHS.
3. **TAKING CARE OF YOUR TABLET** - Students are responsible for the general care of the tablet they have been issued by the school. Tablets that are broken or fail to work properly must be taken to the technology Help Desk.

3.1 **GENERAL PRECAUTIONS**

- Food and beverages can damage your tablet. Students will be responsible for damages caused by food and beverage spills.
- Cords, cables, and removable storage devices must be inserted carefully into the tablet.
- Students should never carry their tablets while the screen is open, unless directed to do so by a teacher.
- Tablets must remain free of any writing, drawing, stickers, or labels that are not the property of the Baltic School District.
- Tablets must never be left in a vehicle or any unsupervised area. • Students are responsible for keeping their tablet's battery charged for school each day.
- The tablet stylus should not be shared with other students. Students are responsible for the stylus issued to them.

3.2 **CARRYING TABLETS** - The protective cases provided with tablets have sufficient padding to protect the tablet from normal treatment and provide a suitable means for carrying the computer within the school.

The guidelines below should be followed:

- Tablets should always be within the protective case when carried.
- Some carrying cases can hold other objects (such as folders and workbooks), but these must be kept to a minimum to avoid placing too much pressure and weight on the tablet screen.
- The tablet must be properly closed before placing it in the carrying case.

3.3 **SCREEN CARE** - The tablet screens can be damaged if subjected to rough treatment. The screens are particularly sensitive to damage from excessive pressure on the screen.

- Do not lean on the top of the tablet when it is closed.
- Do not place anything near the tablet that could put pressure on the screen. • Do not place anything in the carrying case that will press against the cover.
- Wiggling and excessively moving the screen will cause damage to the screen.
- Do not poke the screen.
- Do not place anything on the keyboard before closing the lid (e.g. pens, pencils, or disks).
- Clean the screen with a soft, dry cloth or anti-static cloth. Do not use commercial glass cleaners.
- Wrist jewelry and watches can scratch the screen.

4. **USING YOUR TABLET AT SCHOOL** - Tablets are intended for use at school each day. In addition to teacher expectations for tablet use, school messages, announcements, calendars, schedules, and the Student Handbook will be accessed using the tablet computer. Students must be responsible for bringing their tablets to all classes, unless specifically advised not to do so by their teacher.

4.1 **TABLETS LEFT AT HOME -** "Tablets left a home" is not an acceptable excuse for not submitting work. Repeat violations of this policy may result in disciplinary action.

4.2 **TABLET UNDERGOING REPAIR -** Loaner tablets may be issued to students when they leave their tablets for repair at the Help Desk. Students are responsible for the care of the loaner while in their possession.

4.3 **CHARGING YOUR TABLET'S BATTERY** - Tablets must be brought to school each day in a fully charged condition. Students need to charge their tablets each evening. Repeat violations of this policy will result in disciplinary action. In cases where use of the tablet has caused batteries to become discharged, students may be able to connect their computers to a power outlet in class with the teacher's permission.

4.4 **SCREENSAVERS**

- Inappropriate media may not be used as a screensaver.

- Presence of guns, weapons, pornographic materials, inappropriate language, alcohol, drug, and gang related symbols or pictures will result in disciplinary actions.

4.5 **SOUND** - Sound must be muted at all times unless permission is obtained from the teacher for instructional purposes. If teachers require headphones, they must be in your carrying cases at all times.

4.6 **PRINTING** - Students may use printers in classrooms, the library, and office area with teachers' permission during class or breaks.

5. **MANAGING YOUR FILES & SAVING YOUR WORK** - **SAVING TO MY DOCUMENTS AND/OR P: DRIVE**

- Students will be logging onto our network in order to back up their work.

- Students will have their own user account and folder on the network with ample space to back up any school-related work.

- The tablets will be set up with a My Documents folder in which students should save their work. My Documents will automatically save a copy of all student documents to the P: Drive on the High School server while they are on the High School network. When a student adds a document to the My Documents folder while working at home or away from school, that document will be copied automatically to the school server when the student logs onto the network at school. Additional folders in My Documents may be created or added by the student. All student work should be stored in one of the My Documents folders. Only files stored in My Documents will be automatically backed up and saved. Student work saved to a different location on the computer will not be saved to the high school server.

5.1 **SAVING DATA TO REMOVABLE STORAGE DEVICES** - Students should also backup all of their work at least once each week using removable file storage. Removable memory cards, flash drives may be purchased at a local retailer. It is the student's responsibility to ensure that work is not lost due to mechanical failure or accidental deletion. Computer malfunctions are not an acceptable excuse for not submitting work.

5.2 **SAVING PERSONAL ITEMS** - All personal music, pictures, and videos must be stored in the media file on the C Drive or on removable storage devices.

6. **SOFTWARE ON TABLETS - ORIGINALLY INSTALLED SOFTWARE** - The software originally installed by BHS must remain on the tablet in usable condition and be easily accessible at all times. The tablet is supplied with Microsoft Windows 8 operating system and with additional software. Licensed software provided with all new tablets includes:

Adobe Acrobat Reader

Microsoft Internet Explorer

Microsoft Office 2013 including Word, Excel, Access, PowerPoint and Publisher

Microsoft PhotoStory

Microsoft Windows 8

Symantec Anti-Virus

Windows Media Player

Windows Movie Maker

From time to time, the school may add software applications for use in a particular course. The licenses for this software require that the software be deleted from tablets at the completion of the course.

6.1 **VIRUS PROTECTION** - The tablet has anti-virus protection software. This software will scan the hard drive and removable disks for known viruses on boot up. The virus software will be upgraded from the network. The school's storage server is also installed with virus protection software and hardware.

6.2 **INSPECTION** - Students may be selected at random to provide their tablet for inspection.

6.3 **PROCEDURE FOR RE-LOADING SOFTWARE** - If technical difficulties occur or illegal software is discovered, the hard drive will then be reformatted. Authorized software will be installed and the data files reinstated in My Documents. The school does not accept responsibility for the loss of any software deleted due to a re-format and re-image.

7. **ACCEPTABLE USE GUIDELINES** - **GENERAL GUIDELINES**

1) Students will have access to all available forms of electronic media and communication, which is in support of education and research and in support of the educational goals and objectives of the Baltic School District.

2) Students are responsible for their ethical and educational use of the technology resources of the Baltic School District.

3) Access to the Baltic School District technology resources is a privilege and not a right. Each employee, student and/or parent will be required to follow the Information Security, Acceptable Use, and CIPA Policy.

4) Transmission of any material that is in violation of any federal or state law is prohibited. This includes, but is not limited to the following: confidential information, copyrighted material, threatening or obscene material, and computer viruses.

5) Any attempt to alter data, the configuration of a computer, or the files of another user, without the consent of the individual, school administration, or technology administrator, will be considered an act of vandalism and subject to disciplinary action in accordance with the BHS Code of Conduct.

6) Hard drive passwords are forbidden. If used, students may be responsible for the cost of replacement hardware.

7) Teachers have a right to manage and/or restrict student use of the tablet, software, and internet within the confines of their class.

7.1 PRIVACY AND SAFETY

- Do not go into chat rooms or send chain letters without permission.

- Do not open, use, or change computer files that do not belong to you.

- Do not reveal your full name, phone number, home address, social security number, credit card numbers, password or passwords to other people.

- Remember that storage is not guaranteed to be private or confidential.

- If you inadvertently access a web site that contains obscene, pornographic or otherwise offensive material, notify a teacher, network administrator, or the principal immediately so that such sites can be blocked from further access. This is not merely a request; it is a responsibility.

7.2 LEGAL PROPRIETY

- Comply with trademark and copyright laws and all license agreements. Ignorance of the law is not immunity. If you are unsure, ask a teacher or parent.

- Plagiarism is a violation of the BHS Academic Policies and Procedures. Give credit to all sources used, whether quoted or summarized. This includes all forms of media on the Internet, such as graphics, movies, music, and text.

- Use or possession of hacking software is strictly prohibited and violators will face disciplinary action. Violation of applicable state or federal law, including the South Dakota Penal Code, Computer Crimes, will result in criminal prosecution or disciplinary action by the District.

7.3 E-MAIL

- The state of SD email and BlackBoard Learning are the only email approved for school use.

- Always use appropriate language.

- Do not transmit language/ material that is profane, obscene, abusive, or offensive to others.

- Do not send mass e-mails, chain letters, or spam.

- Students should maintain high integrity with regard to email content.

- No email use during class without permission. • BHS e-mail is subject to inspection by the school.

7.4 CONSEQUENCES(2010)

- The student in whose name a system account and/or computer hardware is issued will be responsible at all times for its appropriate use. Noncompliance with the policies of the Tablet Handbook or Information Security, Acceptable Use, and CIPA Policy will result in disciplinary action.

Prohibited technology resources activities include, but are not limited to, the following: Computer Tablet Violations:

a) Sending, accessing, uploading, downloading, or distributing offensive, profane, threatening, pornographic, obscene, or sexually explicit materials.

b) Using email, games, and other technology resources during class or during other inappropriate time without permission.

c) Downloading or transmitting multi-player game, music or video files using the school network.

d) Vandalizing, damaging, or disabling technology property of the school.

e) Accessing another individual's materials, information, or files without permission.

f) Using the network or internet for commercial, political campaign, or financial gain purposes.

g) Releasing files, home address, personal phone numbers, passwords, or other vital accessing information to others.

h) Promoting or soliciting for illegal activities.

i) Attempting to repair, remove, or install hardware components reserved for authorized service technician.

j) Violating copyright or other protected material laws.

k) Subscribing to mailing lists, mass e-mail messages, games, or other services that generate several messages that can slow the system and waste other users' time and access.

l) Intentionally wasting school resources.

Consequences:

1st Offense 2 weeks computer tablet suspension or resource suspension (email, internet, etc.)

2nd Offense: 4 week computer tablet suspension or resource suspension (email, internet, etc.)

3rd Offense: Tablet suspended for remainder of the semester or not less than 4 weeks.

Computer Network Violations:

a) Attempting to log on to the Internet or network (servers, routers, switches, printers, projectors, firewall) as a system administrator.

b) Accessing or attempting to access other privileged accounts; attempting to exceed user rights, attempting to gain administrative rights.

c) Bypassing or attempting to circumvent Baltic Schools security protocols (firewalls, proxy servers, etc).
d) Sending, accessing, uploading, downloading or distributing pornographic or sexually explicit materials.
e) Installing, enabling, launching, or creating programs that interfere with the performance of the network, Internet, or hardware technology resources.

f) Creating, uploading, or transmitting computer viruses.

g) Attempting to defeat computer or network security.

h) Attempting to download freeware, software, public domain software or other executable and/or installable software.

i) Using tools or techniques to circumvent or bypass current security configurations (hacking). Consequences may Include:

Suspension of tablet computer

Suspension with possible long term suspension or recommended expulsion from school

Possible referral to law enforcement authorities

Electronic mail, network usage, and all stored files shall not be considered confidential and may be monitored at any time by designated District staff to ensure appropriate use. The District cooperates fully with local, state or federal officials in any investigation concerning or relating to violations of computer crime laws. Contents of e-mail and network communications are governed by the South Dakota Open Records Act; proper authorities will be given access to their content.

8. **PROTECTING & STORING YOUR TABLET COMPUTER - TABLET IDENTIFICATION**

Student tablets will be labeled in the manner specified by the school. Tablets can be identified in the following ways:

-Record of serial number

-Individual User account name and password

8.1 **PASSWORD PROTECTION** - Students are expected to use and keep their logon password confidential to protect information stored on their tablets. Disciplinary action may result due to actions of an unauthorized user.

8.2 **STORING YOUR TABLET** - When students are not monitoring tablets, they should be stored in their lockers with the lock securely fastened. Nothing should be placed on top of the tablet, when stored in the locker. Students are encouraged to take their tablets home every day after school, regardless of whether or not they are needed.

Tablets should not be stored in a student's vehicle at school or at home.

8.3 **Tablets Left in Unsupervised Areas**

Under no circumstances should tablets be left in unsupervised areas. Any computer left unsupervised is in danger of being stolen. Unsupervised tablets will be confiscated by staff and taken to the Principal's Office. Disciplinary action may be taken for leaving your tablet in an unsupervised location.

9. **REPAIRING OR REPLACING YOUR TABLET COMPUTER 9.1 MANUFACTURER WARRANTY** - This coverage is purchased by the Baltic School District as part of the purchase price of the equipment. The manufacturer warrants the tablets to be free from defects in materials and workmanship. This 4 year limited warranty covers normal use, mechanical breakdown or faulty construction and will not provide replacement parts necessary to repair the tablet or tablet replacement. The Manufacturer warranty

does not warrant against damage caused by misuse, abuse, accidents or computer viruses. Please report all tablet problems to the Technology Help Desk.

9.2 **ACCIDENTAL DAMAGE PROTECTION** - The Baltic School District no Accidental Damage Protection for school computers. Accidental damage will be covered by the school's insurance program and a fine based on the type of damage. Please report all tablet problems to the technology Help Desk.

9.3 **INTENTIONAL OR NEGLIGENT DAMAGE** - Students are expected to keep the tablet in good condition. Failure to do so will result in fines as specified below:

Fee Chart:

- Cost Lost or intentionally damaged stylus $29.00
- Keyboard Replacement $45.00
- All damaged screen repairs and major case damages will be repaired over the summer. Broken screens will not be replaced during the school year. A student's computer will not be repaired/replaced until the fine is paid.
- Broken screen: accidental A student who has broken their screen will receive a an older model replacement laptop until their fine is paid and computer repaired. Students may continue to use a touchscreen computer with cracked screen if it is still functional.
    - $50.00 first occurrence
    - $100 second occurrence
    - 3 rd occurrence will be the actual cost ($380)
- Broken screen: non-accidental such as a computer that was thrown or a student who was observed by staff abusing the computer. (Actual cost ($380)
- Broken chassis $20-$200.00
- Damaged/lost power cord $40 (A/C adapter).00
- Rubber bumpers/pads $ .50 each
- Lost carrying case $30.00
- Damaged carrying case $10-$20.00
- Damaged/lost secondary battery $120.00
- Damaged/lost primary battery $60.00
- Tablet replacement $400.00
- Additional fees may be assessed depending upon tablet condition

9.4 **SCHOOL DISTRICT PROTECTION** - School District Protection is available for students and parents to cover tablet replacement in the event of theft, loss, or accidental damage by fire. The protection cost is $25.00 annually for each tablet with a maximum cost of $50.00 per family and includes a $200.00 additional charge for each claim.

9.5 **CLAIMS -** All insurance claims must be reported to the principal's office. In instances of theft, loss, or fire, students or parents must file a police or fire report and bring a copy of the report to the principal's office before a tablet can be repaired or replaced with School District Protection. Fraudulent reporting of theft, loss, or accidental damage by fire will be turned over to the police and insurance company for prosecution. A student making a false report will also be subject to disciplinary action. The District will work with the Minnehaha Sheriff's Department to alert pawnshops and police departments in the area to be aware of this District owned equipment.

10. **TABLET TECHNICAL SUPPORT** - The Technology Help Desk coordinates the repair work for tablets. Services provided include the following:

- Filing trouble tickets for hardware maintenance and repairs;

- Battery exchanges and charges and distribution of loaner batteries;

- Distribution of loaner tablets;

- Password identification;

- User account support;

- Operating system or software configuration support;

- Re-imaging hard drives;

- Updates and software installations;

- Coordination of warranty repair;

- Oversee suspended tablet privileges. Information Security, Acceptable Use and CIPA Policy Baltic School District

Mission Statement

The mission of the Baltic School District: "Preparing Students to be Successful in Life."

A. **PURPOSE** The purpose of this document serves to create an environment at Baltic School District that will help protect all teachers, students, and staff members from information security threats that could compromise privacy, productivity, intellectual property rights, and district financial records. This policy recognizes the vital role information plays in the school district's educational, teacher, student, and staff privacy and financial records, and the importance of taking the appropriate steps in protecting information in all forms. As information is shared within internal networks (school networks) and external networks, (Internet), a committed effort must be made to protect this information. This policy serves to protect information resources from threats from both within and outside the school's networks by setting forth responsibilities, guidelines and practices that will help the school district prevent, deter, detect, respond to and promote an environment of secure distribution of information.

B. **SCOPE** This policy is applicable to all students, teachers, staff, contractors, consultants, student teachers, interns, temporary employees, guests, board members and other members of Baltic School District. This policy also applies to those individuals or groups affiliated with third parties, who access Baltic School District network and computer resources.

II. **PHILOSOPHY** The philosophy underlying this policy is to support the Baltic School District Mission Statement by protecting its network resources, student and teacher records, and financial records. The policy serves to reinforce policies regarding access to its network resources, acceptable use policies, copyright policies, license agreements, and other forms of intellectual properties. All members associated with Baltic School District share in the responsibility for protecting information resources to which they have access. Individuals using the Baltic School District information resources will need adequate information, training and other resources to exercise their responsibility

III. **RESPONSIBILITIES** All members of Baltic School District share in the responsibility for protecting the information resources to which they have been given access. These information resources include but are not limited to, individual computer platforms, server platforms and server resources, printer servers and other net workable devices that must be protected from internal and external threats. To aid in the defense of these resources from diverse internal and external threats, several guidelines and procedures must be implemented.

A. **ACCESS CONTROLS** Individuals will be granted access privileges (user account) to Baltic School District information resources upon request and upon agreeing with the terms and conditions of this policy and by signing an "Acceptable Usage Agreement." Individual's accessing or attempting to access other privileged accounts is strictly prohibited. Individuals attempting to exceed their user rights without explicit approval of Baltic School District administrators are strictly prohibited. Examples of exceeding user rights include, but are not limited to: attempting to gain 63 administrative rights and gaining exclusive rights to confidential information (see section f). Violations and abuse of user accounts will be subject to disciplinary procedures, (see section five). Technology resources are provided for academic and work related purposes; any other use may result in loss of access. Recreational browsing of the Internet or recreational uses of technology resources is prohibited. The district protects confidentiality of records through permissions on servers, secure communications to record keeping databases located on the Dakota Digital Network and firewalls located both on the district end and state end. Baltic School District makes no warranties of any kind, whether expressed or implied, for the service it is providing. Baltic School District will not be responsible for any damages suffered by users. This includes loss of data resulting from delays, non-deliveries, mis-deliveries, or service interruptions caused by its own negligence or errors or omissions by users. Use of any information obtained via Baltic School District is at the risk of the user. Baltic School District specifically denies any responsibility for the accuracy or quality of information obtained through its services.

B. **PASSWORDS** Password sharing is explicitly prohibited. A person's password is confidential and is not to be shared with any other person. If an individual's password has been compromised or has been believed to be compromised, the individual is strongly encouraged to report the incident to Baltic School District administrators. A new password will be assigned to the individual. A person's password should never be documented by Baltic School District administrators or by the person possessing the password.

C. **SOFTWARE DOWNLOADS/SOFTWARE INSTALLATION** Downloading of Freeware, Shareware, public-domain software or other executable and/or installable software is explicitly prohibited unless deemed "educational" and appropriate by Baltic School District administrators. Baltic School District administrators reserve the right to determine "educational software." Teachers and staff members must request from Baltic School District administrators explicit permission to download any software. Executable software includes, but not limited to, binary form and script(s) (i.e., Java scripts, Visual Basic scripts). Software installation by students, teachers, and Baltic staff is explicitly prohibited. Individuals wishing to have software packages installed on any platform must seek the approval of Baltic School District administrators. Baltic School District purchases licenses and site licenses for all software installed on computers. Baltic School District does not allow any software to be copied or leave the Baltic School

District premises. Any data located on Baltic School District hardware and within the physical buildings is under control of the district.

D. **E-MAIL/CHATTING AND OTHER COMMUNICATIONS** Students are prohibited from accessing or possessing e-mail accounts without prior consent of Baltic School District administrators. Examples of e-mail services include, but are not limited to the following, MSN, and Yahoo. Baltic School District administrators will determine whether a student is granted e-mail privileges. Teachers and staff members of Baltic School District must abide by the State of South Dakota K -12 Data Center policies. Personal communication software (chatting programs) is explicitly prohibited without prior consent of Baltic School District administrators. Examples of chatting software includes, but is not limited to MIRC, MSN Messenger, web based chatting software/scripts.

E. **ACCEPTABLE USAGE** Any person or persons requesting access to Baltic School District information resources must sign and date an "Acceptable Usage Agreement." This agreement must state that the person or persons requesting Baltic School District information resources will abide by the guidelines and procedures set forth in this document. Failure to comply with these guidelines and procedures will be cause for disciplinary action as outlined in section five of this document. Using tools and/or techniques to circumvent or bypass current security configurations ("hacking") will be considered a violation of this policy and will be subject to disciplinary procedures as outlined in 64 section five. Hacking tools are explicitly prohibited. Any unlawful activities are strictly prohibited and the offender will be prosecuted in accordance with the state laws. Cryptographic software is prohibited by all individuals. All documents and files (binary or text forms) are to remain in their natural format. Examples of cryptographic software include, but are not limited to PGP, PC Guardian. Baltic School District reserves the right to determine what deems cryptographic software. Exceptions include DDN Campus, staff email and any web based encrypted communications (SSL) staff may be using for school records. Bypassing Baltic School District security protocols i.e., firewalls, proxy servers, etc., is explicitly prohibited. Individuals attempting to circumvent current security protocols using software (binary or non-binary form) will be subject to disciplinary action.

F**. PHYSICAL ABUSE** The intentional and unauthorized alteration, damage, destruction or theft of computer hardware, software, data, or related equipment clearly is a violation of Baltic School District policy Examples of damage and/or destruction of hardware devices (i.e. computers, printers, etc.) include, but are not limited to the following;

• Writing and/or drawing on computer hardware, • Inserting items into a floppy drive other than a floppy disk,

• Inserting items into a CD drive other than CD disk,

• Inserting items into the 6-in-1 media card reader

Violations involving physical abuses of network devices will be subject to disciplinary action. Users have an obligation to report physical damage or theft that they see committed by others to Baltic School District administrators.

IV. **CHILDREN'S INTERNET PROTECTION ACT** The Children's Internet Protection Act was put in place to help control and limit access to unacceptable, vulgar, illegal, and offensive content in public places like schools and libraries.

A. **FILTERING** Baltic School District runs filters on all Internet connections to help prevent access to pornographic, obscene, and any other content that may be harmful to minors. Baltic School District staff will be present to supervise and make certain students are not going to any harmful content. The filtering content is updated on a constant basis to assure that recent harmful content is being blocked.

B. **ACCESS BY MINORS TO HARMFUL CONTENT** - Since filters are not perfect, staff are instructed to supervise the computers the students are using to assure no harmful content is accessed. In the case harmful content is accidentally accessed, students are to immediately report the incident to the staff member that is in the presence of the computer, and the staff member is to report the harmful content to the network administrator or technology coordinator so that the content can be manually blocked. If a minor purposefully tries accessing or gets access to harmful content, that minor's privileges can be taken away for computer and Internet access. Other consequences will be determined by the administrator for the violation. The harmful content will then be manually blocked if the filter missed it.

C. UNAUTHORIZED ACCESS - Using tools and/or techniques to circumvent or bypass current security configurations ("hacking") will be considered a violation of this policy and will be subject to disciplinary procedures as outlined in section five. Hacking tools are explicitly prohibited. Any unlawful activities are strictly prohibited and the offender will be prosecuted in accordance with state law.

D. E-MAIL/CHATTING AND OTHER COMMUNICATIONS Students are prohibited from accessing or possessing e-mail accounts without prior consent of Baltic School District administrators. Examples of e-mail services include, but are not limited to the following, MSN, and Yahoo. Baltic School District administrators will determine whether a student is granted e-mail privileges. Personal communication software (chatting programs) is explicitly prohibited without prior consent of Baltic School District administrators.

Examples of chatting software includes, but is not limited to MIRC, MSN Messenger, web based chatting software/scripts. If a student needs access to email, the student can be assigned an unidentifiable email address from the state.

E. UNAUTHORIZED DISCLOSURE - Unauthorized disclosure, use, and dissemination of personal identification information regarding minors is strictly prohibited. Staff should take all precautions necessary to insure students' identification safety. This may include logging out of the computer when the staff member is not in the presence of students or other practices to ensure that student data is kept secure.

V. ENFORCEMENT - Violations of the policy will be handled consistent with Baltic School District disciplinary procedures applicable to the relevant person or persons. Baltic School District administrators may suspend, block or restrict access to network resources. Student violations may be subject to warnings, suspend, block or restrict access to network resources, detention, and suspension of school activities and/or suspended from school. Teachers and staff members may be subject to warnings, suspend, block or restrict access to network resources and/or employment dismissal. Violations of state and federal laws will result in legal prosecution.

Examples of these laws include but not limited to, Cyber Law's, Federal Communities Laws, Federal Wire Tap Laws, Homeland Security Act, National Information Infrastructure Protection Act of 1996, Computer Fraud and Abuse Act, Electronic Communications Privacy Act, Children's Online Privacy Protection Act, Digital Millennium Copyright Act. Individuals violating local, state and federal laws will be subject to disciplinary and/or legal action. Any individual accessing information on external networks, Internet, that is not deemed "educational" for class exercises will be subjected to disciplinary action.

VI. RESOURCES - Information supporting this policy is listed below. This policy was developed in conjunction with the information provided from these sources listed below and the Department of Defense guidelines. • State of South Dakota K-12 Data Center http://www.k12.sd.us/ • Digital Dakota Network http://www.ddnnet.net/ • Children's Internet Protection Act http://www.ifea.net/cipa.html • Digital Millennium Copyright Act http://www.gseis.ucla.edu/iclp/dmcal.htm • Homeland Security Act http://www.whitehouse.gov/deptofhomeland/analysis/ • Computer Fraud and Abuse Act http://www.cpsr.org/cpsr/privacy/crime/fraud.act.txt

VII. **VOCABULARY AND DEFINITIONS -** Malicious Code: Malicious code includes all and any programs (including macros and scripts) which are deliberately coded in order to cause an unexpected (and usually, unwanted) event on a user's PC. Virus: A program which, when executed, can add itself to other program, without permission, and in such a way that the infected program, when executed, can add itself to other programs. Trojan Horse: A type of virus that masquerades or hides itself in a legitimate program, but does something other than what was intended. Worms: A type of virus which can replicate itself and send itself to other computers without permission. Hacker: An individual which attempts to circumvent established security protocols to gain unauthorized access to information systems and/or resources. Hacking Tools: Tools and/or techniques that are used by hackers to gain unauthorized access to information systems and/ or resources. Password: A set of alphanumeric characters that a user requires to enter into a computer before accessing its resources. Freeware: Copyrighted software that has no monetary value. The software is free to use and has no "expiration date." 66 Shareware: Copyrighted software that is free to use within a predefined time period. Once the time has expired the software will no longer function unless the user pays for continual use or registers the software for continual use.

TABLET COMPUTER PROTECTION - The Baltic School District recognizes that with the implementation of the tablet initiative there is a need to protect the investment by both the District and the Student/Parent. The following outlines the various areas of protection: warranty, accidental damage protection and insurance.

MANUFACTURER WARRANTY: This coverage is purchased by the Baltic School District as part of the purchase price of the equipment. The manufacturer warrants the tablets to be free from defects in materials and workmanship. This limited warranty covers normal use, mechanical breakdown or faulty construction and will not provide replacement parts necessary to repair the tablet or tablet replacement. The Manufacturer warranty does not warrant against damage caused by misuse, abuse, accidents or computer viruses.

INSURANCE FOR THEFT, LOSS OR FIRE: Tablets that are stolen, lost or damaged by fire are not covered by the protection outlined above. SCHOOL DISTRICT PROTECTION: Each student will pay the school district an annual protection payment for coverage of theft, loss or damage by fire in the amount of $30. The $30 payment is non-refundable. This protection coverage has a $200.00 additional charge per occurrence for a high school Fujitsu computer or $100 additional charge for a middle school HP computer. This annual coverage begins upon receipt of the payment and ends at the conclusion of each school year. Damage fees will be assessed for up to $50 for a broken screen or broken case on any computer. Families who find the fee to be a hardship may apply for reduction or exemption by contacting marsha.polzin@k12.sd.us.

ADDITIONAL INFORMATION: In cases of theft, vandalism and other criminal acts, a police report, or in the case of fire, a fire report MUST be filed by the student or parent for the protection coverage to take place. A copy of the police/fire report must be provided to the principal's office. The additional charges are the responsibility of the student/parent and must be paid before the tablet can be repaired or replaced.

INTENTIONAL DAMAGE: Students/Parents are responsible for full payment of intentional damages to tablets. Warranty, Accidental Damage Protection, or School District Tablet Protection DOES NOT cover intentional damage of the tablets. Students will be assessed for intentional damage up to the full cost of replacement.

STUDENT PLEDGE FOR TABLET USE

1. I will take good care of my tablet and know that I will be issued the same tablet each year.

2. I will never leave the tablet unattended.

3. I will never loan out my tablet to other individuals.

4. I will know where my tablet is at all times.

5. I will charge my tablet's battery daily.

6. I will keep food and beverages away from my tablet since they may cause damage to the computer.

7. I will not disassemble any part of my tablet or attempt any repairs.

8. I will protect my tablet by only carrying it while in the bag provided or an approved case.

9. I will use my tablet computer in ways that are appropriate and educational.

10. I will not place decorations (such as stickers, markers, etc.) on the District tablet.

11. I understand that my tablet is subject to inspection at any time without notice and remains the property of the Baltic School District.

12. I will follow the policies outlined in the Tablet Handbook and the Use of Technology Resources Policy while at school, as well as outside the school day.

13. I will file a police report in case of theft, vandalism, and other acts covered by insurance.

14. I will be responsible for all damage or loss caused by neglect or abuse. 67

15. I agree to pay for the replacement of my power cords, battery, stylus, or tablet case in the event any of these items are lost or stolen.

16. I agree to return the District tablet, power cords, and carrying case in good working condition.