Esko Public Schools

Original Adoption: 1995
Revised: 6/11/2012
Adopted: 6/19/2012

524 INTERNET ACCEPTABLE USE AND SAFETY POLICY

[Note: School districts are required by statute to have a policy addressing these issues.]

I. PURPOSE

The purpose of this policy is to set forth policies and guidelines for access to the district's electronic technologies, including electronic communications, the district's network and Internet social networking tools and to define the acceptable and safe uses of the Internet.

II. GENERAL STATEMENT OF POLICY

In making decisions regarding employee and student access to the district's computer network, electronic technologies and the Internet, including electronic communications, the school district considers its own stated educational mission, goals, and objectives. Electronic information research skills are now fundamental to preparation of citizens and future employees. Access to the district's computer network and to the Internet enables students and employees to explore libraries, databases, web pages, other online resources, and communicate with people globally. It is also essential in preparing our students to live and work in our society. The district expects its instructional staff will blend thoughtful and appropriate use of the district's computer network, educational technologies and the Internet in their curriculum, providing guidance to students.

When accessing the computer system or the Internet through wireless means the user will follow policies to ensure that authentication, confidentiality, availability and integrity are protected. This includes centralized oversight, configuration management and control of wireless devices by the district.

III. LIMITED EDUCATIONAL PURPOSE

The school district is providing students and employees with access to the district's electronic technologies and the Internet. The purpose of the system is more specific than providing students and employees with general access to the Internet. The district's network has a limited educational purpose, which includes use of the system for classroom activities, educational research, and professional or career development activities. Users are expected to use Internet access through the district network system to further educational and personal goals consistent with the mission of the school district and school policies. Computer networks, software, hardware, and applications are provided to support the instructional, administrative and informational needs of students and staff in the district. Uses which might be acceptable on a user's private personal account on another system may not be acceptable on this limited-purpose network.

IV. USE OF SYSTEM IS A PRIVILEGE

The use of the district's electronic technologies and access to the Internet is a privilege, not a right. All electronic technologies and all work product or communication by any person using any of the school district systems is the property of the Esko Public Schools. The school district reserves the right to confiscate, read, review, evaluate or otherwise determine the use and content of all hardware, software, and any work product or communication on any part of the school district network. This includes, but is not limited to, email, unauthorized or authorized software, files, pictures, and other content the user created. Users should not expect privacy in the contents of personal files on the district system.

V. UNACCEPTABLE USES

A. The following uses of the district's electronic technologies and Internet resources or accounts are considered unacceptable:

1. Users will not use the district's electronic technologies to access, review, upload, download, store, print, post, receive, transmit or distribute:

   a. pornographic, obscene or sexually explicit material or other visual depictions;

   b. obscene, abusive, profane, lewd, vulgar, rude, inflammatory, threatening, disrespectful, or sexually explicit language;

   c. materials that use language or images that are inappropriate in the education setting or disruptive to the educational process;

   d. information or materials that could cause damage or danger of disruption to the educational process;

   e. materials that use language or images that advocate violence or discrimination toward other people (hate literature) or that may constitute harassment or discrimination;

   f. Orders for personal shopping online during time designated as work time by the district;

   g. Storage of personal photos, videos, music or files not related to educational purposes for any length of time;

   h. Unlicensed software or applications.

2. Users will not use the district's electronic technologies to knowingly or recklessly post, transmit or distribute false or defamatory information about a person or organization, or to harass another person, or to engage in personal attacks, including prejudicial or discriminatory attacks. This is a definition of Cyberbullying.

3. Users will not use the district's electronic technologies to engage in any illegal act or violate any local, state or federal statute or law.

4. Users will not engage in computer hacking or other related activities.

5. Users will not use the district's electronic technologies to vandalize, damage or disable the property of another person or organization, will not make deliberate attempts to degrade or disrupt equipment, software or system performance by spreading computer viruses or by any other means, will not tamper with, modify or change the school district system software, hardware or wiring or take any action to violate the school district's security system, and will not use the district's electronic technologies in such a way as to disrupt the use of the system by other users.

6. Users will not use the district's electronic technologies to gain unauthorized access to information resources or to access another person's materials, information or files without the direct permission of that person. Users will not deliberately or knowingly delete a student or employee electronic file.

7. Users will not use the district's electronic technologies to post private information in public access areas regarding private or confidential information about another person. Private or confidential information is defined by board policy, state law, and federal law.

    a. This paragraph does not prohibit the posting of employee contract information on school district webpages or communications between employees and other individuals when such communications are made for education-related purposes (i.e., communications with parents or other staff members related to students).

    b. This paragraph specifically prohibits the use of the district's electronic technologies to post private or confidential information about another individual, employee or student, on social networks.

8. Users must keep all account information and passwords on file with the designated school district official. Users will not attempt to gain unauthorized access to the district's electronic technologies or any other system through the district's electronic technologies, attempt to log in through another person's account, or use computer accounts, access codes or network identification other than those assigned to the user. If an employee's password is learned by another employee, the password should be changed immediately. An active terminal with access to private data must not be left unattended and must be protected by password protected screen savers. Messages and records on the school district system may not be encrypted without the permission of appropriate school authorities.

9. Users will not use the district's electronic technologies to violate copyright laws or usage licensing agreements, or otherwise to use another person's property without the person's prior approval or proper citation, including the downloading or exchanging of pirated software including freeware and shareware, or copying software to or from any school computer, and will not plagiarize works they find on the Internet or other information resources.

10. Users will not use the district's electronic technologies for conducting business, for unauthorized commercial purposes or for financial gain unrelated to the mission of the school district. Users will not use the district's electronic technologies to offer or provide goods or services or for product advertisement.

B. A student or employee engaging in the foregoing unacceptable uses of the Internet when off school district premises also may be in violation of this policy as well as other school district policies. Examples of such violations include, but are not limited to, situations where the school district system is compromised or if a school district employee or student is negatively impacted. If the school district receives a report of an unacceptable use originating from a non-school computer or resource, the school district may investigate such reports to the best of its ability. Students or employees may be subject to disciplinary action for such conduct, including, but not limited to, suspension or cancellation of the use or access to the school district computer system and the Internet and discipline under other appropriate school district policies, including suspension, expulsion, exclusion, or termination of employment.

C. If a user inadvertently accesses unacceptable materials or an unacceptable Internet site, the user shall immediately disclose the inadvertent access to an appropriate school district official. In the case of a school district employee, the immediate disclosure shall be to the employee's immediate supervisor and/or the building administrator. This disclosure may serve as a defense against an allegation that the user has intentionally violated this policy. In certain rare instances, a user also may access otherwise unacceptable materials if necessary to complete an assignment and if done with the prior approval of and with appropriate guidance from the appropriate teacher or, in the case of a school district employee, the building administrator.

D. Depending on the nature and degree of the violation and the number of previous violations, unacceptable use of the school district system or the Internet may result in one or more of the following consequences: suspension or cancellation of use or access privileges; payments for damages and repairs; discipline under other appropriate school district policies, including suspension, expulsion, exclusion or termination of employment; or civil or criminal liability under other applicable laws.

VI. FILTER

A. The Esko Public Schools seek to comply with both State of Minnesota Statues and federal Children's Internet Protection Act of 2001.

B. With respect to any of its computers with Internet access, the School District will monitor the online activities of minors and employ technology protection measures during any use of such computers by users. The technology protection measures utilized will block or filter Internet access to any visual depictions that are:

1. Obscene;

2. Child pornography; or

3. Harmful to minors.

C. The term "harmful to minors" means any picture, image, graphic image file, or other visual depiction that:

1. Taken as a whole and with respect to minors, appeals to a prurient interest in nudity, sex, or excretion; or

2. Depicts, describes, or represents, in a patently offensive way with respect to what is suitable for minors, an actual or simulated sexual act or sexual contact, actual or simulated normal or perverted sexual acts, or a lewd exhibition of the genitals; and

3. Taken as a whole, lacks serious literary, artistic, political, or scientific value as to minors.

D. An administrator, supervisor or other person authorized by the Superintendent may disable the technology protection measure, for use by an adult, to enable access for bona fide research or other lawful purposes.

VII. CONSISTENCY WITH OTHER SCHOOL POLICIES

Use of the district's electronic technologies and use of the Internet shall be consistent with school district policies and the educational mission, goals and objectives of the school district.

VIII. LIMITED EXPECTATION OF PRIVACY

A. By authorizing use of district's electronic technologies, the school district does not relinquish control over materials on the system or contained in files on the system. Users should not expect privacy in the contents of personal files on the school district system.

B. Routine maintenance and monitoring of the school district network may lead to a discovery that a user has violated this policy, another school district policy, or the law.

C. An individual investigation or search will be conducted if school authorities have a reasonable suspicion that the search will uncover a violation of law or school district policy.

D. Parents have the right at any time to investigate or review the contents of their child's files and email files. Parents have the right to request the termination of their child's individual account at any time.

E. School district employees should be aware that the school district retains the right at any time to investigate or review the contents of their files and email files. Employees will not provide access to their email accounts to non-employees. In addition, school district employees should be aware that data and other materials in files maintained on the school district network may be subject to review, disclosure or discovery under Minn. Stat. Ch. 13 (the Minnesota Government Data Practices Act).

In addition it is recommended that electronic mail sent by employees contain a confidentiality notice similar to the following:

Confidentiality Notice: If the information in this email relates to an individual or student, it may be private data under state or federal privacy laws. This e-mail message, including any attachments, is for the sole use of the intended recipient(s). Any unauthorized review, use, disclosure or distribution is prohibited. If you are not the intended recipient, please contact the sender by reply e-mail and destroy all copies of the original message.

F. The school district will cooperate fully with local, state and federal authorities in any investigation concerning or related to any illegal activities or activities not in compliance with school district policies conducted through the school district system.

IX. INTERNET USE AGREEMENT

A. The proper use of the Internet, and the educational value to be gained from proper Internet use, is the joint responsibility of students, parents and employees of the school district.

B. Your child will be granted access to the Internet unless a letter is submitted by a parent or guardian requesting that their student not be allowed to use internet resources. It should be understood that this may severely limit some of the educational activities your child is able to participate in. The letter must be signed by the parent or guardian and the school principal. This letter must be renewed annually.

C. Employees who terminate employment with the Esko Public School District will have any and all access to the school district network disabled or terminated on their last day of employment.

D. Students using social networking tools and curriculum content management software for a teacher's assignment are required to keep personal information as stated above out of their postings (see Section V.A.7)

E. Students using the district's educational technologies for social networking for a limited educational purpose must follow Policy, Bullying Prohibition.

X. LIMITATION ON SCHOOL DISTRICT LIABILITY

Use of the district's educational technologies is at the user's own risk. The system is provided on an "as is, as available" basis. The district will not be responsible for any damage users may suffer, including, but not limited to, loss, damage or unavailability of data stored on school district disks, tapes, drives or servers, or for delays or changes in or interruptions of service or misdeliveries or non-deliveries of information or materials, regardless of the cause. The school district is not responsible for the accuracy or quality of any advice or information obtained through or stored on the school district system. The school district will not be responsible for financial obligations arising through unauthorized use of the school district system or the Internet.

XI. DISTRICT WEB PRESENCE

The district website was established to provide a learning experience for employees and students and to provide a venue for communications with parents and the community.

A. The district will establish and maintain a website. The website will include information regarding the district, its schools, district curriculum, extracurricular activities and community education. All website content will support and promote he district's mission, goals and strategic direction.

B. The district's website will provide parents with a web portal to grades, attendance, and resources.

C. The district webmaster will be responsible for maintaining the district website and monitoring district web activity.

D. The district encourages all teachers to establish a web page, using district format, that supports their classroom instruction. The teacher is responsible for maintaining their own web page on the district web site.

E. Departments and noninstructional programs sponsored by the district may also create web pages to support their departments or programs. These web pages must be approved by the district administration. Each department or program must appoint a person to maintain the web page.

XII. USER NOTIFICATION

A. All users shall be notified of the school district policies relating to Internet use and access.

B. This notification shall include the following:

1. Notification that Internet use is subject to compliance with school district policies.

2. Disclaimers limiting the school district's liability relative to:

    a. Information stored on school district disks, drives or servers.

    b. Information retrieved through school district computers, networks or online resources.

    c. Personal property used to access school district computers, networks or online resources.

    d. Unauthorized financial obligations resulting from use of school district resources/accounts to access the Internet.

3. A description of the privacy rights and limitations of school sponsored/managed Internet accounts.

4. Notification that, even though the school district may use technical means to limit student Internet access, these limits do not provide a foolproof means for enforcing the provisions of this acceptable use policy.

5. Annual presentation by district personnel or outside law enforcement sources of appropriate on line behavior. The information presented will be age appropriate for all students in grades K-12. This will include information on social networking, chat rooms and cyber bullying as well as other on line resources students may encounter while on the internet.

6. Notification that goods and services purchased over the Internet may potentially result in unwanted financial obligations and that any financial obligation incurred by a student or school employee through the Internet is the sole responsibility of the school employee, student and/or the the student's parent(s) or guardian(s).

7. Notification that the collection, creation, reception, maintenance and dissemination of data via the Internet, including electronic communications, is governed by Policy 406, Public and Private Personnel Data, and Policy 515, Protection and Privacy of Pupil Records.

8. Notification that, should the user violate the school district's acceptable use policy, the user's access privileges may be revoked, school disciplinary action may be taken and/or appropriate legal action may be taken.

9. Notification that all provisions of the acceptable use policy are subordinate to local, state and federal laws.

XIII. PARENTS' RESPONSIBILITY; NOTIFICATION OF STUDENT INTERNET USE

A. Outside of school, parents bear responsibility for the same guidance of Internet use as they exercise with information sources such as television, telephones, radio, movies and other possibly offensive media. Parents are responsible for monitoring their student's use of the school district system and of the Internet if the student is accessing the school district system from home or a remote location.

B. Parents should understand that their students will be using school district resources/accounts to access the Internet. Information provided to parents/guardians will include:

1. A section in elementary and high school student handbooks.

2. A statement that the school district's acceptable use policy is available for parental review, in print or online.

3. Internet Tips for Parents; Addendum A

XIII. IMPLEMENTATION; POLICY REVIEW

A. The school district administration may develop appropriate user notification forms, guidelines and procedures necessary to implement this policy for submission to the school board for approval. Upon approval by the school board, such guidelines, forms and procedures shall be an addendum to this policy.

B. The administration shall revise the user notifications, including student and parent notifications, if necessary, to reflect the adoption of these guidelines and procedures.

C. The school district Internet policies and procedures are available for review by all parents, guardians, staff and members of the community.

D. Because of the rapid changes in the development of the Internet, the school board shall conduct an annual review of this policy.

Legal References:
15 U.S.C. § 6501 *et seq.* (Children's Online Privacy Protection Act)
17 U.S.C. § 101 *et seq.* (Copyrights)
20 U.S.C. § 6701 *et seq.* (Enhancing Education through Technology Act of 2001)
47 U.S.C. § 254 (Children's Internet Protection Act of 2000 (CIPA))
47 C.F.R. § 54.520 (FCC rules implementing CIPA)
Minn. Stat. §§ 125B.15 (Internet Access for Students)
Minn. Stat. § 125B.26 (Telecommunications/Internet Access Equity Aid)
United States v. American Library Association, 123 S.Ct. 2297 (2003)

Cross References: MSBA/MASA Model Policy 403 (Discipline, Suspension, and Dismissal of School District Employees)

MSBA/MASA Model Policy 406 (Public and Private Personnel Data)
MSBA/MASA Model Policy 505 (Distribution of Nonschool-Sponsored Materials on School Premises by Students and Employees)
MSBA/MASA Model Policy 506 (Student Discipline)
MSBA/MASA Model Policy 515 (Protection and Privacy of Pupil Records)
MSBA/MASA Model Policy 519 (Interviews of Students by Outside Agencies)
MSBA/MASA Model Policy 521 (Student Disability Nondiscrimination)
MSBA/MASA Model Policy 522 (Student Sex Nondiscrimination)
MSBA/MASA Model Policy 603 (Curriculum Development)
MSBA/MASA Model Policy 604 (Instructional Curriculum)
MSBA/MASA Model Policy 606 (Textbooks and Instructional Materials)
MSBA/MASA Model Policy 806 (Crisis Management Policy)
MSBA/MASA Model Policy 904 (Distribution of Materials on School District Property by Nonschool Persons)
MSBA/MASA Model Policy 604 (Instructional Curriculum)
MSBA/MASA Model Policy 606 (Textbooks and Instructional Materials)
MSBA/MASA Model Policy 804 (Bomb Threats)
MSBA/MASA Model Policy 904 (Distribution of Materials on School District Property by Nonschool Persons)

Addendum I

Internet Tips for Parents

- Become more computer literate so you can learn how to block objectionable material.
- Keep the computer in a common area in your home, where youcan watch and monitor your child.
- Monitor your child's email by sharing an email account.
- Make your child's favorite sites easy to find by bookmarking them.
- Take time to go online with your child so he or she can develop healthy online behavior.
- Block dangerous or threatening sites, such as private chat rooms, with safety features provided by your ISP (Internet Service Provider) or install a filtering solution.
- Be aware and inform your child that anything posted on the Internet is there forever. Also, anytime they post something on a blog, they are revealing their email address.
- Be on the lookout for any unfamiliar charges to our credit card and /or phone bills, which could indicate online activity involving your child.
- Be sure you are aware of any Internet access your child has away from home. Find out if safety features are in place at your child's school, after-school center, friends' homes, or any place where he or she could use a computer without your supervision.
- Don't ever dismiss your child's concerns while online. If your child reports feeling uncomfortable about an online exchange, take him or her seriously.
- Immediately forward copies of any obscene or threatening messages you or your child receives to your Internet service provider.
- Call the National Center for Missing and Exploited Children at (800) 843-5678 if you are aware of the transmission, use, or viewing of child pornography online. Contact your local law enforcement agency or the FBI if your child has received child pornography via the Internet.
- Many sites use "cookies", devices that track specific information about the user, such as name, email address, and shopping preferences. Cookies can be disabled. Ask your Internet service provider for more information.

Rules for Your Child

- Never trade personal photographs in the mail or scanned photographs over the Internet.
- Never reveal personal information, such as address, phone number, or school name or location.
- Use only a screen name and change it often.
- Never agree to meet anyone from a chat room in person.
- Never respond to a threatening email or message.
- Always tell apparent about any communication or conversation that was scary or made you uncomfortable.

Source: www.edgewave.com

Internet Policy Summary

This is a summary of the Esko Public Schools District Policy relating to acceptable use of the school district computer system and the Internet.

- The use of the school district system and access to use of the Internet is a privilege, not a right.
- There is no guarantee of privacy when using any school technology.
- Users will not use the school district system to access, review, upload, download, store, print, post, or distribute pornographic, obscene, illegal or sexually explicit material.
- Users will not use the school district system to transmit or receive illegal, obscene, abusive, profane, lewd, vulgar, rude, inflammatory, threatening, disrespectful, or sexually explicit language.
- Users will not use the school district system to access, review, upload, download, store, print, post, or distribute materials that use language or images that are inappropriate in the educational setting or disruptive to the educational process and will not post information or materials that could cause damage or danger of disruption.
- Users will not use the school district system to access, review, upload, download, store, print, post, or distribute materials that use language or images that advocate violence or discrimination toward other people or that may constitute harassment or discrimination.
- Users will not use the school district system to knowingly or recklessly post false or defamatory information about a person or organization, or to harass another person, or to engage in personal attacks, including prejudicial or discriminatory attacks, including cyberbullying.
- Users will not use the school district system to engage in any illegal act or violate any local, state or federal statute or law.
- Users will not use the school district system to vandalize, damage or disable the property of another person or organization, will not make deliberate attempts to degrade or disrupt equipment, software or system performance by spreading computer viruses or by any other means, will not tamper with, modify or change the school district system software, hardware or wiring or take any action to violate the school district system's security in such a way as to disrupt the use of the system by other users, this includes anything that would be considered computer hacking.
- Users will not use the school district system to gain unauthorized access to information resources or to access another person's materials, information or files without the direct permission of that person.
- Users will not use the school district system to post private information about another person or to post personal contact information about themselves or other persons including, but not limited to, addresses, telephone numbers, school addresses, identification numbers, account numbers, access codes or passwords, and will not repost a message without permission of the person who sent the message.
- Users will not attempt to gain unauthorized access to the school district system or any other system through the school district system, attempt to log in through

another person's account, or use computer accounts, access codes or network identification other than those assigned to the user.

- Users will not use the school district system to violate copyright laws or usage licensing agreements, or otherwise to use another person's property without the person's prior approval or proper citation, including the downloading or exchanging of pirated software or copying software to or from any school computer, and will not plagiarize works they find on the Internet.
- Users will not use the school district system for the conduct of a personal business, for unauthorized commercial purposes or for financial gain unrelated to the mission of the school district. Users will not use the school district system to offer or provide goods or services or for product advertisement. Users will not use the school district system to purchase goods or services for personal use during working hours.
- Use of the school district computer system and use of the Internet shall be consistent with school district policies and the mission of the school district.
- Violation of Internet Use Policy will be addressed through existing disciplinary Policy.

This is a summary of POLICY 524 – INTERNET ACCEPTABLE USE POLICY. For a full copy, please contact the Esko Public Schools District Office at 879-2969.

Addendum III – (Policy #524 Internet Use Policy)

Wireless Policy Summary

Ad hoc wireless connection – connection of a computer or peripheral to a network to communicate with each other without the use of a wireless router or a router and a wireless access point; typically used for smaller networks, such as a home network.

Wireless access point (WAP) –spread spectrum radiofrequency wireless device or technology that provides a common connection point for devices in a wireless network. A WAP uses transmit and receive antennas instead of plug in connector ports for access by multiple users of the wireless network. A WAP can be connected to the wired network to bridge between the campus backbone and a wireless network.

Wireless client – hardware and software that is installed in a desktop, laptop, handheld, portable, or other computing device to allow it to communicate with a WAP, providing an interface to a wireless network.

Wireless network or wireless local area network (WLAN) – type of computer network spanning a relatively small area (e.g., a single building or group of buildings) that uses high frequency radio waves rather than wire to communicate between nodes (e.g., computer, printer, wired network).

1. Ad hoc wireless connections are not permitted on any device connected to the schools wired or wireless network infrastructure. These types of connections are inherently insecure and pose a risk to the district's computing environment. IT will periodically perform network scans for unregistered WAPs. Only access points purchased by ISD 99 or those that are pre-registered and are found to be in compliance and meet ISD 99 security specifications and are configured by IT with the appropriate security settings are permitted on the district network. If any other access points are identified, they will be immediately disconnected from the network. Failure to comply with this item will result in disciplinary action by administration.

2. As with access to the school wired network, access to the school wireless network or to Internet services through independent WAPs must require user authentication and authorization for all faculty, staff, and students.

3. ISD 99 standard virus protection software, intrusion detection, auditing, and monitoring mechanisms will be used on all district owned wireless equipment as necessary.

4. Any unauthorized use of the school wireless network is prohibited. Unauthorized uses include: attempts to sniff or capture wireless data, attempts to disrupt or jam the wireless network, altering a wireless client media access control (MAC) address to attempt to evade security, attempts to break into or gain unauthorized access to any computers or systems from a wireless connection, installing a personal WAP on the network, mass emailing (spamming) on the wireless network, running servers on the wireless network, or any type of denial of service attack using the wireless network.

5. In an emergency situation, IT is authorized to take whatever reasonable steps are necessary, including denial of network access, to protect the integrity and security of the ISD 99 data network and systems, safeguard the safety of district community members and property, and protect ISD 99 from liability.

6. All ISD 99 wireless network users must use equipment registered, approved, and/or acquired by Esko Public School.

7. Users must obtain approval prior to use of the district Wireless Network from the District Technology Coordinator to assure network compatibility. Students or staff wishing to use personal equipment on the network must first have it approved by the Technology Coordinator and building administrator to see that it meets minimum standards for use on the network. Once approved, a list of approved equipment will be kept in the District Office.

8. Users must report damaged, lost or stolen ISD 99 wireless network equipment to the District Technology Coordinator by the next business day. Fiscal responsibility will be determined by administrative staff.

9. All District owned equipment, (laptops, desktop computers, digital cameras, projectors etc.) whether used on the wireless network or not, shall be for school use. Equipment shall remain in the building unless the user of the equipment needs it for school related purposes, such as workshops or presentations outside the building. Users must notify district technology staff or a building administrator and complete a property removal form before taking equipment out of the building. Failure to comply with this item will result in disciplinary action by administration that will follow the District's Discipline Policy #403.

ESKO PUBLIC SCHOOLS ISD 99
PROPERTY REMOVAL REQUEST

Complete three copies. Retain one each for employee, supervisor and one for technology department.

NAME: _____

EQUIPMENT: Quantity: _____ _____ _____

Laptop ☐ TV ☐ VCR ☐ Video Equip. ☐ Computer ☐ Other:_____

MAKE:_____ MODEL:_____ S#_____

APPROX. VALUE:_____

DATE PICKED UP:_____ TIME:_____ AM ☐ PM ☐

EQUIPMENT CONDITION: OK ☐ DAMAGED ☐

As a condition of removal, the employee expressly agrees to release, discharge, save and hold harmless Esko Public Schools ISD 99 from any and all claims for injury or death of persons or damage to property caused through use of said removed property. The employee is responsible for the safe handling, loss or damage to the removed equipment.

EMPLOYEE'S SIGNATURE:_____ DATE:_____

APPROVED BY:_____ TITLE:_____

TO BE COMPLETED WHEN PROPERTY IS RETURNED

DATE:_____ EQUIPMENT CONDITION: No Damage ☐ Damaged ☐

REPLACEMENT VALUE:_____

CHECKED BY:_____ TITLE:_____