NEBO SCHOOL DISTRICT BOARD OF EDUCATION POLICIES AND PROCEDURES

SECTION: C – General School Administration
POLICY TITLE: Internet Safety and Computer Use
FILE NO.: CG
DATED: October 11, 2023

TABLE OF CONTENTS

1. PURPOSE AND PHILOSOPHY

1.1. Nebo School District provides computers, networks, email services, and filtered Internet access (together "network services") to support the educational mission of the School District and to enhance the curriculum and learning opportunities for students and employees for administrative, educational, communication, and research purposes. General rules and expectations for professional behavior and communication apply to the use of network services.

1.2. This policy outlines the requirements for receiving E-rate discounts under the Children's Internet Protection Act (CIPA), 47 U.S.C. 254, which requires the Board to adopt and enforce an internet safety policy. The policy must include provisions for educating students about appropriate online behavior, including cyberbullying and interacting with other people on social media. The policy must also include provisions for the operation of technology protection measures to protect against access to child pornography or other obscene visual depictions.

1.3. This policy is adopted to meet the requirements of UTAH CODE ANN. § 53G-7-1002, which requires the Board to adopt and enforce a policy to restrict access to internet or online sites that contain obscene material.

1.4. The intent of this Policy is to provide students and employees with general requirements for using network services. This policy may be supplemented by more specific administrative procedures, directives, and rules governing the day-to-day management and operation of the computer system.

2. SYSTEM FILTER

2.1. The District uses an Internet filtering system to assist in restricting access to Internet sites containing material that is obscene, pornographic, or harmful to minors. Even though the District takes reasonable efforts to block material that is obscene, pornographic, or harmful to minors, no filtering system or features will filter out all obscene, pornographic, harmful, or inappropriate material. It is the responsibility of the computer system user to maintain a high level of integrity to protect themselves and others from such inappropriate material. As used herein, references to the terms "obscene," "obscenity," "pornographic," "pornography," "child pornography", and "harmful to minors" are defined by applicable state and federal laws, regulations, and cases.

2.2. Users should report inadvertent access to inappropriate content to a teacher or administrator.

3. STUDENT USE

3.1. The Utah State Core Standards require students to become effective and efficient users of online resources. Students need access to email and the Internet to meet these requirements. Employees and volunteers assigned to supervise student use of computers must ensure compliance with this policy and/or applicable administrative procedures, directives, and rules. Although student use of network services at school will be supervised by school staff, the District cannot guarantee that students will not gain access to inappropriate material. The District encourages parents to have a discussion with their students about values and how those beliefs should guide student activities while using the District's network services.

3.2. Student access to network services is provided primarily for educational use. Occasional personal use is also permitted within the guidelines of this policy, Policy JDE, *Student Electronic Devices*, and all other applicable policies and laws.

4. EMPLOYEE USE

Employees are to utilize network services for the performance of job duties and professional or career development activities. Incidental personal use is permitted as long as such use does not interfere with: (a) the employee's job duties and performance; (b) computer system operations; and/or (c) other computer system users. "Incidental personal use" is defined as use by an individual employee for personal communication and information. Employees are reminded that such personal use must comply with this policy and all other applicable Board policies and administrative procedures, directives, and rules.

5. PROHIBITED USE

Each student, employee, or other network services user is responsible for his/her actions and activities involving use of network services and for his/her computer files, passwords, and accounts. General examples of unacceptable uses which are expressly prohibited include, but are not limited to, the following:

5.1. Any use that is illegal or in violation of Board policies and/or administrative procedures, directives, or rules, including, but not limited to, harassment; discrimination (i.e., race, color, gender, nationality, religion, age, or disability); defamation; violent or threatening communications and behavior; bullying; infringement of copyright or trademark laws; offering for sale, purchase, or use of any prohibited or illegal substances; etc.

5.2. Any use involving material that is obscene, pornographic, sexually explicit, sexually suggestive, or otherwise harmful.

5.3. Any inappropriate communications with students, minors, employees, or anyone else that is obscene, profane, lewd, vulgar, belligerent, inflammatory, or threatening.

5.4. Use for private financial gain, or commercial, advertising, or solicitation purposes that is inconsistent with section 4.

5.5. Use as a forum to solicit, proselytize, advocate, or communicate the views of an individual or a non- District sponsored organization; to solicit membership in or support of any non- District sponsored organization; or to raise funds for any non- District sponsored purpose, whether for profit or not for profit that is inconsistent with section 4.

5.6. Any communication that represents personal views as those of the District or that could be misinterpreted as such.

5.7. Any unauthorized attempt to bypass the District's Internet filtering systems and features, including VPN technologies.

5.8. Any malicious use or disruption of the network services or breach of security features.

5.9. Any physical or electronic vandalism to the computer system or equipment.

5.10. Failing to report a known breach of computer security or violations of this policy to the school principal or other appropriate administrator.

5.11. Any attempt to delete, erase, or otherwise conceal any information stored on a District computer that violates Board policies and/or administrative procedures, directives, and rules.

5.12. Using the network services to gain unauthorized access to other computers, computer systems or user accounts, or to attempt to gain such unauthorized access.

5.13. Any use involving damaging, dangerous, or disruptive material.

5.14. Any use involving personal or generalized attacks or harassment, or to communicate false or defamatory information.

5.15. Any use of technology to disrupt class or that takes oneself or others off-task, including lab time.

5.16. Any use for political purposes as described in UTAH CODE ANN. § 20A-11-1203, including to influence a ballot proposition, initiative, or referendum; to influence a person to either vote or refrain from voting for or against any particular candidate, judge, or ballot proposition; or to solicit a campaign contribution. Utah law imposes a civil fine against a person who sends an email using the email system of a public entity for a political purpose, to advocate for or against a ballot proposition, or to solicit a campaign contribution. Thus, employees may not use their Nebo email address to send or forward such emails. Employees who violate this provision may be subject to a fine by the lieutenant governor of $250 for the first offense and $1,000 for each subsequent offense. UTAH CODE ANN. § 20A-11-1205.

The foregoing list provides general guidelines and examples of prohibited uses for illustrative purposes but does not attempt to state all required or prohibited activities by network services users. Students, employees, and other users who have questions regarding whether a particular activity or use is acceptable should seek further guidance from the school's principal or other appropriate administrator.

6. INSTRUCTION

Students shall be instructed in appropriate online behavior, including online safety, interacting with other individuals on social networking websites and in chat rooms, and regarding cyber-bullying awareness and response. This instruction will be included in the curriculum for elementary Keyboarding and required junior high and high school CTE courses.

7. NO EXPECTATION OF PRIVACY

The District retains control, custody, and supervision over all network services owned, licensed, or leased by the District. The District reserves the right to monitor all network services activity by

students, employees, and other users. Students, employees, and other users have no expectation of privacy in their use of the District's network services and equipment.

8. STUDENT RECORDS

Employees and other network services users are expected to use appropriate judgment and caution in communications concerning students and staff to ensure that personally identifiable information remains confidential. Employees and others with access to student records may not use, release, or share these records, except as authorized by federal and state law.

9. NO DISCLOSURE OF PERSONAL INFORMATION

For personal safety purposes in using network services, users are advised not to disclose personal information such as home addresses, home telephone numbers, social security numbers, etc.

10. INDEMNIFICATION

10.1. All network services users shall be responsible for any and all claims, losses, damages, or costs (including attorneys' fees) associated with their use of the network services, including, but not limited to, illegal uses (copyright and trademark violations, defamation, discrimination, harassment, etc.); violations of this policy and/or applicable administrative procedures, directives, and rules; etc., and shall hold harmless and indemnify the District and its employees and agents from such claims, losses, damages, and costs.

10.2. The District assumes no responsibility for any unauthorized charges made by network services users, including, but not limited to, credit card charges, subscriptions, long distance telephone charges, equipment and line costs, etc., and users shall hold harmless and indemnify the District and its employees and agents from such unauthorized charges.

10.3. The District makes no warranties of any kind, either expressed or implied, that the network services will be error-free or without defect. The District will not be responsible for any damage users may suffer, including, but not limited to, loss of data or interruptions of service. The District is not responsible for the accuracy or quality of the information obtained through or stored on the computer system.

11. REVOCATION OF USE

Access and use of the network services is a privilege and not a right. This privilege may be revoked at any time for failure to comply with the terms and conditions of this policy and/or applicable administrative procedures, directives, and rules.

12. STUDENT VIOLATIONS AND DISCIPLINE

12.1. Any student who violates this policy and/or applicable administrative procedures, directives, and rules governing the use of network services may be subject to disciplinary action, such as losing computer use privileges, suspension, and expulsion. Illegal uses by students of School District computers may also result in referral to law enforcement authorities.

12.2. Disciplinary action may be taken against a student for violation of this policy consistent with Board policies and administrative procedures. Students are entitled to due process and may appeal disciplinary action as provided in Policy JD, *Student Conduct and Discipline*.

13. EMPLOYEE VIOLATIONS AND DISCIPLINE

13.1. Any employee who violates this policy and/or applicable administrative procedures, directives, and rules governing the use of network services may be subject to disciplinary action, up to and including termination. Professionally licensed employees may be referred to the Utah Professional Practices Advisory Commission (UPPAC), along with any and all evidence, for investigation and possible disciplinary action against professional licensing. Illegal uses of network services will also result in referral to law enforcement authorities.

13.2. Disciplinary action may be taken against an employee for violation of this policy consistent with Policy GCPD, *Employee Discipline, Administrative Leave, and Orderly Termination*, as well as administrative procedures, and procedures set forth in the Certified Employee Handbook, Classified Employee Handbook, or Management Team Handbook as applicable. Employees are entitled to due process and may appeal the disciplinary action imposed by following the procedures set forth in the applicable employee handbook.

14. ACCEPTABLE USE AGREEMENTS

14.1. Annually, each employee authorized to access the network services must agree to the "Employee Acceptable Use Agreement" stating that they have read the Agreement and this policy, and that they agree to comply with the terms and conditions set forth therein. The "Employee Acceptable Use Agreement" will be retained by the District.

14.2. Each school year, every student authorized to access the network services must verify that they have read this policy and that they agree to comply with it.

15. NOTICE

Notice of the availability of this policy shall be posted in a conspicuous place within each school.

16. BOARD REVIEW

As required by UTAH CODE ANN. § 53G-7-1003, the Board shall review this policy at least every three (3) years.

EXHIBITS
None

REFERENCES
Children's Internet Protection Act (CIPA), Pub. L. No. 106-554, § XVII, 114 Stat. 2763, 335–352 (codified as amended in scattered sections of 20 U.S.C. and 47 U.S.C. § 254); 47 CFR 54.520.
UTAH CODE ANN. § 53G-7-1001 et seq.
Nebo School District Policy GCPD, *Employee Discipline, Administrative Leave, and Orderly Termination*
Nebo School District Policy JD, *Student Conduct and Discipline*
Nebo School District Policy JDE, *Student Electronic Devices*
Certified Employee Handbook
Classified Employee Handbook
Management Team Handbook

FORMS
Nebo School District Employee Acceptable Use Agreement

HISTORY
Revised: 11 October 2023: title changed from *Computer, Email, and Internet Use* to *Internet Safety and Computer Use*; added reference to legal requirements under CIPA and Utah law; clarified certain prohibitions on personal and political use; modified acceptable use requirements; made technical changes.
Technical Change: 21 November 2022 – district administration added new logo to policy and all forms.
Revised: 13 February 2019 –updated consistent with current terminology and practices, including student take-home devices; removed reference to filter on email; made technical changes.
Revised: 8 February 2012 –permitted incidental personal use; added section on instruction; made technical changes.
Revised: 14 May 2008 – updated to new format.
Adopted or revised: 10 July 2002.