A/MPolicy 524: INTERNET ACCEPTABLE USE AND SAFETY POLICY

[Note: BrightWorks is 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 BrightWorks computer system and acceptable and safe use of the Internet, including electronic communications.

II. GENERAL STATEMENT OF POLICY

In making decisions regarding employee access to BrightWorks computer system and the Internet, including electronic communications, BrightWorks 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 BrightWorks computer system and to the Internet enables employees to explore thousands of libraries, databases, bulletin boards, and other resources while exchanging messages with people around the world. BrightWorks expects that staff will blend thoughtful use of BrightWorks computer system and the Internet throughout their work.

III. LIMITED PURPOSE

BrightWorks is providing employees with access to BrightWorks computer system, which includes Internet access. The purpose of the system is more specific than providing employees with general access to the Internet. BrightWorks system 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 BrightWorks system to further educational and personal goals consistent with the mission of BrightWorks policies. 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 BrightWorks system and access to use of the Internet is a privilege, not a right. Depending on the nature and degree of the violation and the number of previous violations, unacceptable use of BrightWorks 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 BrightWorks policies, including suspension, exclusion, or termination of employment; or civil or criminal liability under other applicable laws.

V. UNACCEPTABLE USES

A. While not an exhaustive list, the following uses of BrightWorks system and Internet resources or accounts are considered unacceptable:

1. Users will not use BrightWorks system to access, review, upload, download, store, print, post, receive, transmit, or distribute:

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

harmful;
b. obscene, abusive, profane, lewd, vulgar, rude, inflammatory, threatening, disrespectful, or sexually explicit language;
c. materials that use language or images that are inappropriate for the professional setting of an employee;
d. information or materials that could cause damage or danger of disruption to the professional setting of an employee; and
e. materials that use language or images that advocate violence or discrimination toward other people (hate literature) or that may constitute harassment or discrimination.

2. Users will not use the BrightWorks system 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.

3. Users will not use the BrightWorks system to engage in any illegal act or violate any local, state, or federal statute or law.

4. Users will not use the BrightWorks 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 BrightWorks system software, hardware, or wiring or take any action to violate the BrightWorks' security system, and will not use the BrightWorks system in such a way as to disrupt the use of the system by other users.

5. Users will not use the BrightWorks system to gain unauthorized access to information resources or to access another person's materials, information, or files without the implied or direct permission of that person.

6. Users will not use the BrightWorks system to post private information about another person, personal contact information about themselves or other persons, or other personally identifiable information, including, but not limited to, addresses, telephone numbers, school addresses, work addresses, identification numbers, account numbers, access codes or passwords, labeled photographs, or other information that would make the individual's identity easily traceable, and will not repost a message that was sent to the user privately without permission of the person who sent the message. [Note: BrightWorks should consider the impact of this paragraph on present practices and procedures, including, but not limited to, practices pertaining to employee communications, and student/employee use of social networking websites. Depending upon BrightWorks policies and practices, BrightWorks may wish to add one or more of the following clarifying paragraphs.]

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

b. Employees creating or posting BrightWorks-related web pages may include personal contact information about themselves on a webpage. However, employees may not post personal contact information or other personally identifiable information unless:

(1) such information is classified by the BrightWorks as directory information

and verification is made that the BrightWorks has not received notice from an employee eligible that such information is not to be designated as directory information in accordance with Policy 515; or

(2) such information is not classified by BrightWorks as directory information but written consent for release of the information to be posted has been obtained from an employee. In addition, prior to posting any personal contact or personally identifiable information on a BrightWorks-related webpage, employees shall obtain written approval of the content of the postings from the Executive Director.

c. These prohibitions specifically prohibit a user from utilizing the BrightWorks system to post personal information about a user or another individual on social networks, including, but not limited to, social networks such as "Facebook," "Twitter," "Instagram," "Snapchat," "TikTok," "Reddit," and similar websites or applications.

7. Users will not attempt to gain unauthorized access to the BrightWorks system or any other system through the BrightWorks 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. Messages and records on the BrightWorks system may not be encrypted without the permission of appropriate BrightWorks authorities.

8. Users will not use the BrightWorks 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 BrightWorks computer, and will not plagiarize works they find on the Internet.

9. Users will not use the BrightWorks system for conducting business, for unauthorized commercial purposes, or for financial gain unrelated to the mission of BrightWorks. Users will not use the BrightWorks system to offer or provide goods or services or for product advertisement. Users will not use the BrightWorks system to purchase goods or services for personal use without authorization from the appropriate BrightWorks official.

10. Users will not use the BrightWorks system to engage in bullying or cyberbullying in violation of the BrightWorks Bullying Prohibition Policy. This prohibition includes using any technology or other electronic communication off BrightWorks premises to the extent that the BrightWorks environment is substantially and materially disrupted.

B. BrightWorks has a special interest in regulating off-campus speech that materially involves substantial disorder or invasion of the rights of others. An employee engaging in the foregoing

unacceptable uses of the Internet when off BrightWorks premises also may be in violation of this policy as well as other BrightWorks policies. Examples of such violations may include, but are not limited to, serious or severe bullying or harassment targeting particular individuals. If BrightWorks receives a report of an unacceptable use originating from a non-BrightWorks computer or resource, BrightWorks may investigate such reports to the best of its ability. Employees may be subject to disciplinary action for such conduct, including, but not limited to, suspension or cancellation of the use or access to BrightWorks computer system and the Internet and discipline under other appropriate BrightWorks policies, including suspension, 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 the immediate supervisor and IT Systems Manager. In the case of a BrightWorks employee, the immediate disclosure shall be to the employee's immediate supervisor. 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 BrightWorks Executive Director.

VI. FILTER

[Note: Pursuant to state law, BrightWorks is required to restrict access to inappropriate materials on computers with Internet access. BrightWorks seeking technology revenue pursuant to Minnesota Statutes section 125B.26 or certain federal funding, such as e-rate discounts, for purposes of Internet access and connection services and/or receive funds to purchase Internet accessible computers are subject to the federal Children's Internet Protection Act, effective in 2001. BrightWorks is required to comply with additional standards in restricting possible access to inappropriate materials. Therefore, BrightWorks should select one of the following alternative sections depending upon whether BrightWorks is seeking such funding and the type of funding sought.]

All computers equipped with Internet access and available for use at each BrightWorks site will be equipped to restrict, by use of available software filtering technology or other effective methods, all employee access to materials that are reasonably believed to be obscene, child pornography or harmful to minors under state or federal law. Software filtering technology shall be narrowly tailored and shall not discriminate based on viewpoint.

VII. CONSISTENCY WITH OTHER POLICIES

Use of BrightWorks computer system and use of the Internet shall be consistent with BrightWorks policies and the mission of BrightWorks.

VIII. LIMITED EXPECTATION OF PRIVACY

A. By authorizing use of the BrightWorks system, BrightWorks does not relinquish control over materials on the system or contained in files on the system. Users should expect only limited privacy in the contents of personal files on the system.

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

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

D. BrightWorks employees should be aware that BrightWorks retains the right at any time to investigate or review the contents of their files, instant messaging records, and email files. In addition, BrightWorks employees should be aware that data and other materials in files maintained on the BrightWorks system may be subject to review, disclosure or discovery under Minnesota Statutes Chapter 13 (Minnesota Government Data Practices Act).

E. BrightWorks 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 BrightWorks policies conducted through the BrightWorks 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 responsibility of BrightWorks employees.

B. BrightWorks Computer, Equipment, Network, Internet and Email Guidelines for Acceptable Use for employees must be read and signed by the user. The form must then be filed at BrightWorks.

X. LIMITATION ON BrightWorks LIABILITY

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

XI. USER NOTIFICATION

A. All users shall be notified of BrightWorks policies relating to Internet use.

B. This notification shall include the following:

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

2. Disclaimers limiting BrightWorks's liability relative to:

a. Information stored on BrightWorks hard drives, solid state drives, cloud drives and servers.

Adopted April 19, 2023

b. Information retrieved through BrightWorks computers, networks, or online resources.

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

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

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

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

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

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

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

XII. IMPLEMENTATION; POLICY REVIEW

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

B. The Executive Director shall revise the user notifications, if necessary, to reflect the adoption of these guidelines and procedures.

C. BrightWorks Internet policies and procedures are available for review by all staff and members of the community.

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

Legal References: Minn. Stat. Ch. 13 (Minnesota Government Data Practices Act

15 U.S.C. § 6501 et seq. (Children's Online Privacy Protection Act)

17 U.S.C. § 101 et seq. (Copyrights)

Adopted April 19, 2023

20 U.S.C. § 1232g (Family Educational Rights and Privacy Act)

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. § 121A.031 (School Student Bullying Policy)

Minn. Stat. § 125B.15 (Internet Access for Students)

Minn. Stat. § 125B.26 (Telecommunications/Internet Access Equity Act)

Mahanoy Area Sch. Dist. v. B.L., 594 U.S. ___ , 141 S. Ct. 2038 (2021)

Tinker v. Des Moines Indep. Cmty. Sch. Dist., 393 U.S. 503 (1969)

United States v. Amer. Library Assoc., 539 U.S. 1942003)

Sagehorn v. Indep. Sch. Dist. No. 728, 122 F.Supp.2d 842 (D. Minn. 2015)

R.S. v. Minnewaska Area Sch. Dist. No. 2149, 894 F.Supp.2d 1128 (D. Minn. 2012)

Tatro v. Univ. of Minnesota, 800 N.W.2d 811 (Minn. App. 2011), aff'd on other grounds 816 N.W.2d 509 (Minn. 2012)

S.J.W. v. Lee's Summit R-7 Sch. Dist., 696 F.3d 771 (8th Cir. 2012)

Parents, Families and Friends of Lesbians and Gays, Inc. v. Camdenton R-III Sch. Dist., 853 F.Supp.2d 888 (W.D. Mo. 2012)

M.T. v. Cent. York Sch. Dist., 937 A.2d 538 (Pa. Commw. Ct. 2007)

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 Non School-Sponsored Materials on School Premises by Students and Employees)

MSBA/MASA Model Policy 506 (Student Discipline)

MSBA/MASA Model Policy 514 (Bullying Prohibition Policy)

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 (Title IX Sex Nondiscrimination Grievance Procedures and Process)

MSBA/MASA Model Policy 603 (Curriculum Development)

Adopted April 19, 2023

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)

Adopted April 19, 2023

BrightWorks Policies and Practices, Equipment

From Policy List: Equipment

Equipment Provided

BrightWorks provides copy machines/printers, computers, Internet access and appropriate communication and peripheral equipment for the sole purpose of aiding employees in activities directly related to the requirements of their position.

Equipment Purchases

The IT Systems Manager must approve purchases of communication, peripheral, and technology equipment in excess of $100.00. The Executive Director or the Executive Director's designee must approve purchases of consumable or other products for which grant-based resources are used.

Use of Equipment

BrightWorks neither supports nor endorses the use of any equipment for any purpose other than official business of the organization. Employees are cautioned that electronically transmitted material is subject to BrightWorks sexual harassment and hostile work environment policies. In addition, transmissions outside of BrightWorks offices may expose the employee and/or the organization to significant consequences. Text messaging and emailing while operating a motorized vehicle while on BrightWorks business are prohibited.

See BrightWorks Computer, Equipment, Network, Internet and Email Guidelines for Acceptable Use which is included in the addenda of this policy manual.

Use of Personally Owned Electronic Equipment

Reimbursement of or use of personally-owned electronic equipment such as cell phones, computers, etc., will be allowed only in case of emergency, or if common use of such items has been approved by the Executive Director.

Adopted April 19, 2023

BrightWorks Computer, Equipment, Network, Internet and Email Guidelines for Acceptable Use

OVERVIEW

Use Technology Resources responsibly:

- Use resources only for authorized purposes to support the mission and goals of BrightWorks.
- Protect your username/user ID, equipment, and system from unauthorized use. You are responsible for all activities on your username/user ID, accounts, and computer system.
- Access only information that is your own, that is shared on the BrightWorks networks, or information you are authorized to access.
- Use only legal versions of copyrighted software in compliance with vendor license requirements.
- Be aware of your use of shared resources. Refrain from monopolizing systems, overloading the network with excessive data, wasting disk space, printer paper, or other resources.

Do NOT use Technology Resources for unacceptable purposes, including:

- Use of another person's system, username/user ID, password, files, or data without permission.
- Activities undertaken to purposely harm BrightWorks computer and data systems or network security.
- Use of BrightWorks systems for commercial or political purposes.
- Use of any BrightWorks computer or the computer networks to violate any United States or Minnesota state law or regulation.
- Wasteful use of computing resources; or network resources, for example, by sending unsolicited mass mailings.
- Use of BrightWorks systems or networks for personal gain; for example, by selling access to your username/user ID or to BrightWorks systems, accounts, or networks.

PRIVILEGES

The use of any BrightWorks computer, computer system, technology equipment, or networks by any person (employee or authorized user) is a privilege, not a right. Inappropriate use will result in restriction or removal of those privileges. BrightWorks reserves the right to terminate, suspend, or limit computer, technology equipment, or network access at any time.

Privacy: Computers and technology equipment belonging to BrightWorks are considered

shared resources. Nothing saved on a BrightWorks computer is guaranteed to be private or secure from other authorized users. Email in BrightWorks-licensed Microsoft Outlook and Google and instant messaging in Microsoft Teams is not guaranteed to be private. The IT Systems Manager has access to all email and instant messaging and reserves the right to monitor the use of all data, accounts, files, and devices on BrightWorks networks.

ACCEPTABLE USE

The use of any BrightWorks computer, equipment, computer networks, and Internet must be consistent with the policies and procedures of BrightWorks.

Authorized Users Only: BrightWorks computers and other technology equipment are not for use by family members, friends, or unauthorized users at any time.

Network and Internet Access: BrightWorks provides staff members and other authorized users with access to the networks, which includes Internet access for activities related to BrightWorks and its organizational mission and goals. Uses that might be acceptable on a user's private, personal account on another system may not be acceptable on these networks.

Legal Uses Only: Employees must not use any BrightWorks computer, computer networks, accounts, or technology equipment to violate any United States or Minnesota state law or regulation. For example, employees must not use illegal copies of copyrighted software, applications, or materials on BrightWorks systems. In addition, employees must not use BrightWorks technology to harass or intimidate others.

Technology Losses: BrightWorks cannot be held responsible for any lost data, files, resources, or damages incurred through the use of BrightWorks computers, technology equipment, or computer networks.

Damages to Computers and Technology Equipment: Users will report all damage promptly to the IT Systems Manager. The cost of repair or replacement for damage from inappropriate use will be the responsibility of the user.

SECURITY

Users of BrightWorks computers and computer networks agree not to violate or attempt to violate system security or intentionally interfere with performance of BrightWorks networks.

User Accounts and Passwords: Users agree not to access another person's accounts, files or passwords. Do not use another individual's computer or any BrightWorks-related accounts without express consent. Do not give your passwords to any other individual, except as required by the IT Systems Manager to troubleshoot and diagnose system malfunctions.

Downloads: Downloading of applications, programs, games, Internet browser add-ins, messaging services, videos, music, and other data files requires prior approval from the IT Systems Manager.

Connection to the Network: Personal (non BrightWorks-supported) and guest devices are not allowed on BrightWorks internal networks at any time. Personal and guest devices are allowed only on the BrightWorks-Guest, ME-Community, and BrightWorks Training Room WiFi networks.

Reporting Suspected Security Breaches: If you identify a security problem on BrightWorks networks, system, computers, or technology equipment, or accounts, you are obligated to immediately notify the IT Systems Manager.

BrightWorks EMPLOYEE AGREEMENT

BrightWorks considers any violation of BrightWorks Computer, Equipment, Network, Internet and Email Guidelines for Acceptable Use to be a serious offense and reserves the right to copy and examine any files or information residing on all BrightWorks computers, mobile devices, technology equipment, networks, and BrightWorks systems. Inappropriate use will result in restriction or removal of privileges. BrightWorks reserves the right to terminate, suspend, or limit computer or network access at any time.

I acknowledge that while I am working for BrightWorks, I will take proper care of all company technology equipment and accounts that I am entrusted with. I further understand that upon resignation/termination, I will return all BrightWorks technology equipment and that the technology equipment will be returned in proper working order. I understand I may be held financially responsible for lost or damaged technology equipment. This agreement includes, but is not limited to, laptops, tablets, cell phones, printers, monitors, accounts, and other equipment. I understand that failure to return equipment will be considered theft and may lead to criminal prosecution by BrightWorks.

By signing below I confirm that I have read, understand, and agree to abide by BrightWorks Computer, Equipment, Network, Internet and Email Guidelines for Acceptable Use outlined in this document.

Signature: _____

Name (please print): _____

Date: _____

Adopted April 19, 2023

BrightWorks

*Equipment provided to employee on first day:

*All items are included in the BrightWorks Technology Database in FileMaker

Adopted April 19, 2023