Olathe Public Schools – Staff Responsible Use Policy (RUP)

I. Our Commitment to You and Technology

A. Technology is a powerful tool that enhances teaching and learning in Olathe Public Schools (the District). We provide you with various technologies to create engaging and impactful learning experiences for our students. This Responsible Use Policy (RUP) outlines our shared understanding of how to use these technologies effectively and responsibly.

B. Your access to and use of district-owned and personally owned technologies while on district property, at school-related activities, or while using the district network is a valuable privilege provided to support your professional responsibilities. We trust you to use these resources in a manner that aligns with our educational mission and professional standards.

C. What We Mean by "Technology":

For the purpose of this RUP, "technology" includes:

1. The district's network (both wired and wireless)
2. Servers
3. Computer workstations
4. Laptops
5. Mobile devices
6. Peripheral devices (like mice and keyboards)
7. Application databases
8. Online resources
9. Internet access
10. Email
11. Artificial intelligence (AI)
12. Any other technology the district provides or designates for staff and student use, including new technologies as they are adopted.

D. This RUP applies whenever you are using District technologies:

1. On or near school property
2. In school vehicles
3. At school-sponsored events and activities
4. Using district-owned technologies and resources off-campus

Our goal in providing these technologies is to support your professional work.

II. Olathe Public Schools: Our Responsibilities

A. The district is committed to supporting you in effectively using technology. Our responsibilities include:
    1. Helping you develop the skills needed to successfully use instructional and digital workplace technologies.
    2. Providing guidance and resources to understand the appropriate and responsible use of technologies.
    3. Supporting the integration of technology into district-approved curriculum and educational activities.
    4. Facilitating the use of instructional technologies within district-approved curriculum and educational activities.
B. To ensure the security of district information, including confidential files, email, staff personnel files, and other sensitive data, the district may need to limit access to certain technologies.
C. Please be aware that the district reserves the right to access staff digital files, messages, and account information on any district-owned technology or network access.
D. In compliance with the Children's Internet Protection Act (CIPA), the District educates staff and students about safe and appropriate online behavior, including the use of email and Web 2.0 resources (like social media). We also use filtering technologies and security measures to block access to inappropriate content that is illegal, harmful, or potentially offensive. While we strive to create a safe online environment, it's important to understand that completely preventing access to all inappropriate content is not always possible.
E. Ultimately, it is each staff member's responsibility to adhere to the guidelines for appropriate, responsible, and acceptable use. When uses of technology do not align with these expectations, the district will address the situation appropriately.

III. Your Rights and Responsibilities as Staff

A. Your use of technology is a valuable privilege intended to support your professional work here at Olathe Public Schools. To ensure we can all benefit from these resources, please comply with this RUP and all relevant Board of Education policies regarding technology use. In all your interactions with technology provided by or accessed through the District, your rights and responsibilities include:

1. **Respecting Privacy:** Always respect the privacy rights of students and other district personnel.
2. **Representing the District Professionally:** Understand that all your communications using district technologies reflect on the integrity, ethics, and good name of the District.
3. **Practicing Ethical Conduct:** Maintain ethical and acceptable standards of behavior, conduct, and courtesy, consistent with expectations in our schools and district settings.
4. **Complying with Laws and Policies:** Adhere to all local, state, and federal laws, Board of Education policies, and administrative and school guidelines, especially those related to copyrighted materials.
5. **Avoiding Unauthorized Access:** Do not attempt to gain or provide unauthorized access to school, district, other public, or private networks, technologies, or digital files for any reason.
6. **Following Procedures:** Comply with all related Board of Education policies, administrative guidelines, the Lines of Communication Matrix, and school operating procedures concerning acceptable and responsible use.
7. **Cooperating with Inquiries:** Fully cooperate with building and district administrators if an instance of inappropriate use is reported or suspected.
8. **Using District Technologies Appropriately:** Utilize district-provided technologies (as defined earlier) in accordance with all district policies and settings, as guided by current and future federal privacy and protection regulations.

IV. Guidelines for Utilizing District Technologies

A. When using technologies within the District, please:

1. **Practice Good Digital Citizenship:** Follow appropriate online etiquette and responsible digital behavior.

2. **Access Your Own Files:** Only access, open, view, modify, and/or delete your own personal digital files, educational work, email accounts, and passwords.
3. **Use Email Professionally:** Utilize your District email account for professional communication only.
4. **Manage Bandwidth Use:** Restrict your internet and bandwidth usage to activities that support professional responsibilities.
5. **Report Concerns Immediately:** Promptly report any threatening messages or inappropriate use/access of internet files/content to an administrator or supervisor.
6. **Communicate Respectfully:** Use all district technologies to communicate and collaborate with others in a kind and respectful manner.
7. **Act Ethically and Responsibly:** Take full responsibility for your actions and behave ethically, even when technology offers the freedom to act otherwise.
8. **Use Approved Wireless Access:** Only use the wireless network access provided by the district for staff and do not attempt to create unauthorized access points, such as personal VPNs, to any district-owned technologies.

B. **Responsible Use of Artificial Intelligence (AI)**
1. **Human-in-the-Loop:** Retain human oversight and critical judgement when using AI with students. Use AI as a teaching companion and thought partner, rather than a direct substitute for your expertise.
2. **Ensure Data Privacy:** Maintain the confidentiality and security of student, family, and employee information by strictly prohibiting the input of any personally identifiable information (PII) into AI tools or platforms.
3. **Bias Awareness:** Be aware that AI can amplify societal biases. Cultivate critical evaluation and analyze AI outputs for bias before sharing with students.
4. **Equitable Access:** Ensure access for all, regardless of background or ability. When designing instruction that may require the use of AI or other technologies, staff will utilize district-approved and/or purchased tools for student assignments.
5. **Understand AI:** Develop a critical understanding of the capabilities and limitations of AI tools before and during their use with students and reflect on their impact on learning.

V. Unacceptable and Inappropriate Uses of Technology

A. The following actions are considered examples of unacceptable and inappropriate uses of technology and will be treated as violations of Board of Education policy and administrative guidelines. Violations may lead to disciplinary action, including temporary or permanent loss of technology access.

1. **Failure to Report Misuse:** Not reporting any misuse or breach of information technology to the OPS Chief Technology Officer or designee.
2. **Misuse of Confidential Information:** Obtaining confidential information about a student or employee for non-school-related activities or sharing such information for non-school-related purposes.
3. **Unauthorized Access to Student Data:** Accessing or obtaining student educational information without a legitimate educational interest.
4. **Malicious Code:** Creating, copying, knowingly distributing, or posting any type of malicious software (malware) to any district-owned technologies.
5. **Impersonation and Unauthorized Sharing:** Sending or posting digital messages (email, social media, etc.) using someone else's name or sharing another individual's personal information without their consent.
6. **Policy Violations in Communication:** Sending messages that are inconsistent with Board of Education policies or administrative guidelines.
7. **Discriminatory or Harmful Content:** Sending messages that are sexist, racist, discriminatory, inflammatory, or hurtful.
8. **Inappropriate Messages:** Sending inappropriate messages through any digital technology.
9. **Obscene or Inappropriate Content:** Sending messages, downloading files, or accessing websites that knowingly contain obscene language, graphics, pictures, or any inappropriate content, including anything encoded/encrypted or attached to messages.
10. **Non-Professional Online Chat:** Engaging in online chat sessions that are not directly related to professional responsibilities.
11. **Sharing Accounts:** Lending your account ID or password to anyone.
12. **False Online Presence:** Creating any social networking site or presence while pretending to be another staff member.

13. **Harassment and Bullying:** Using obscene, harassing, bullying, or abusive language in any digital or non-digital format.
14. **Manipulative Media:** Recording or distributing media online with the intention of manipulating or embarrassing others (staff or students).
15. **Bypassing Security:** Disabling or attempting to disable any district filtering, monitoring, or security system on any district technology.
16. **Copyright Infringement:** Violating copyright laws.
17. **Unauthorized Network Administration Access:** Attempting to log in to any district network (wired or wireless) as a network administrator without proper authorization.
18. **Data Vandalism:** Vandalizing or destroying data belonging to another user (student or staff member).
19. **Plagiarism:** Presenting the work of others as your own in digital or non-digital school assignments.
20. **General Policy Violations:** Using technologies in any way that violates school rules, administrative guidelines, Olathe Public Schools Board of Education policies, or local, state, or federal law.
21. **Unauthorized Wireless Networks:** Accessing non-OPS wireless networks with district-issued laptops while on campus (including personal hotspots).
22. **Unauthorized Devices on Network:** Attempting to connect non-authorized devices, including personal laptops, phones, or tablets, to the OPS wired or wireless network.
23. **Emergency Communication/Moving Phones (E911 Compliance):** To comply with federal E911 regulations (Ray Baum Act), which require accurate location information for emergency services, no district-owned phone or communication device shall be moved without prior approval and assistance from the Olathe Public Schools Technology Division.
24. **Managing District Technology Assets:** For effective management, security, and support, any relocation of district-owned technology, such as computers, printer, phones, and other equipment, requires advance approval and coordination with the Olathe Public Schools Technology Division.

VI. Consequences of Unacceptable and Inappropriate Use

A. Staff members who violate this RUP, related administrative guidelines, or Olathe Public Schools Board of Education policies regarding Staff Responsible Use of Technologies will face appropriate disciplinary measures, up to and including immediate termination.

VII. Best Practices for District-Issued Device Usage

A. We encourage you to help students actively engage with technology to process new information and demonstrate their learning. To support this, please remember to:

1. **Bring Your Device:** Bring your district-issued device(s) to school regularly.
2. **Use Appropriate Software:** Avoid using software and services that may not be suitable for the teaching and learning goals of a specific course or subject.
3. **Protect Your Credentials:** Do not share or ask for usernames, PINs, or passwords with others.
4. **Data Management and Backup:** While the district provides storage, we encourage staff to routinely back up their professional and instructional resources to personal storage solutions as needed, understanding that the district is not responsible for the security or accessibility of such personal storage and that **no student Personal Identifying Information or data should be moved to personal storage**.

B. District-Issued Device Maintenance

1. **Restart Regularly:** Restart your district-issued device (e.g., Surface Pro) on a weekly basis.
2. **Clearing Browsing History:** Routinely clear your cache/browsing history to improve device performance.
3. **Report Repairs Promptly:** Report any needed repairs (e.g., cracked screen, trackpad issues, missing keys, bent corners) to your building technician in a timely manner.

C. Power Management and Energy Saving

1. To extend your device's battery life when not plugged in:
    a. Close unused applications.
    b. Lower the keyboard backlight.
    c. Reduce display brightness.
    d. Turn off Wi-Fi if not needed.
    e. Turn off Bluetooth if not in use.

f. Shorten the time before your computer goes to sleep.

D. Transporting District-Issued Devices Safely

1. Always close the keyboard and kickstand when carrying your device.
2. Avoid dropping your device, especially when open.
3. Protect your device from extreme temperatures (hot or cold).
4. Do not squeeze the device between heavy objects.

E. What to Avoid

1. **Personal Use of School Email:** Avoid using your District email address for personal purposes, such as subscriptions and coupons.
2. **Secondary Accounts:** Do not create secondary accounts on your district-issued laptop (e.g., for friends, family, or parental controls).
3. **Unauthorized Operating Systems:** Do not install operating systems other than those installed by the OPS Tech Department (e.g., Linux, Virtual Machines).
4. **Unauthorized File-Sharing Software:** Avoid installing or using unauthorized third-party multi-node file-sharing software (e.g., Dropbox, Torch, BitTorrent, Transmission).
5. **Using Personal Devices Instead:** Please use your district-issued device as your primary work device.
6. **Network Congestion:** Avoid sending chain emails, inappropriate broadcast messages, or any other information that could overload the network.
7. **Commercial Use:** District technologies should not be used for commercial purposes. The school district is not responsible for any financial obligations resulting from district-issued devices, technology, or internet access (including cryptocurrency-related activities).
8. **Unauthorized Security Software:** Do not install third-party firewalls, anonymizers, or proxies.

VIII. Violations of Responsible and Acceptable Use: Examples

The following examples illustrate serious violations that threaten the safety and security of the school's network, infrastructure, students, staff, and the wider community. These are not exhaustive but highlight key areas of concern:

A. **Privacy, Property, & Community**

1. Accessing or deleting the OPS administrative account.
2. Vandalizing or disassembling district-issued devices or other network resources (including defacing, engraving, coloring, painting, etching, marking, removing keys, or deforming the device).
3. Accessing laptops, accounts, and files of others without permission (including browsing someone else's computer, accessing their online accounts without their knowledge, or impersonating someone online).
4. Recording, filming, or photographing teachers, staff, or students in violation of the law, without permission, or without authority. If permission is granted, the recorded material must be used respectfully and responsibly. Sharing or publicly posting captured material without further permission is not permitted.
5. Using district-issued devices, applications, or the school network (in or out of school) for self-gain or to harass, disparage, or intimidate any person or the school itself.
6. Sending or posting messages that harm the reputation of OPS using your school email address or other identifiers created by OPS.

B. **Illegal Activity**

1. Installing or distributing unlicensed or illegal software.
2. Using the network to support illegal activities, businesses, or gambling. The school district is not responsible for any financial obligations resulting from school-provided technology or internet access related to such activities.

C. **Network Access Violations**

1. Accessing, creating, or storing sexually explicit, violent, obscene, or unlawful material.
2. Attempting to bypass OPS network security or impair network functionality, including using VPNs or remote login tools (e.g., GoToMyPC, LogMeIn) to circumvent network protocols.
3. Attempting to bypass restrictions set by network administrators.
4. Using a computer to distribute inappropriate or illegal material (text, audio, images, or video).

5. Providing billable services to others using your laptop or OPS network resources.
6. Connecting personal routers, wireless access points, smart speakers, and printers to the district network.
7. Creating a wired or wireless network without the explicit approval of the Technology Department.