

Introduction:

The Norwood Public Schools is committed to providing a safe, productive, and ethical digital learning environment for all students and staff. This Responsible Use Policy (RUP) outlines the expectations for using the district's technology resources, including user accounts, computers, networks, internet access, software, and digital tools. This policy applies to all users, whether accessing district resources on school property or remotely.

I. General Principles:

- **Educational Purpose:** All technology use must be directly related to educational activities, administrative tasks, or authorized district business.
- **Respect and Responsibility:** Users must demonstrate respect for themselves, others, and district resources.
- **Ethical Conduct:** Users must adhere to ethical standards, including copyright law, intellectual property rights, and academic integrity.
- **Security and Privacy:** Users are responsible for protecting their accounts and respecting the privacy of others.
- **Compliance:** Users must comply with all applicable laws, district policies, and this RUP.

II. Student Use:

- **A. Acceptable Use:**
 - Using district-provided devices and networks for assigned schoolwork, research, and approved educational activities.
 - Accessing approved educational websites and applications.
 - Communicating with teachers and classmates in a respectful and appropriate manner.
 - Saving and storing school-related files in designated locations.
- **B. Unacceptable Use:**
 - Accessing or distributing inappropriate content, including pornography, hate speech, or violent material.
 - Cyberbullying, harassment, threats, or any form of online abuse, including account impersonation and the creation of fake content for malicious purposes.
 - Unauthorized access to networks, systems, user accounts, or data.
 - Malicious destruction, theft, or vandalism of devices, networks, systems, user accounts or data.
 - Downloading or installing unauthorized software or applications.
 - Engaging in online gambling, illegal activities, or activities that violate school rules.
 - Plagiarism, cheating or any form of academic dishonesty.
 - Sharing personal information without consent.
 - Circumventing security/compliance or filtering measures on any hardware or software system used in the Norwood Public Schools.

- **C. Social Media:**
 - Students must use social media responsibly and ethically.
 - Posting or sharing content that is defamatory, harassing, or violates the privacy of others is prohibited.
 - Students should be aware that their online behavior can have negative real-world consequences.
 - Students are prohibited from creating social media accounts that impersonate the district, school, staff, or other students.
- **D. Generative AI:**
 - Generative AI tools may be used for educational purposes with teacher guidance and approval.
 - Students may only use AI tools that have been approved by the district and have a student data policy agreement in place.
 - Using AI to generate content that violates academic integrity or school policies or other policies in this RUP is prohibited.
 - Students should be aware that AI generated content can be inaccurate, and should be used responsibly.
- **E. Use of Digital Tools and Websites:**
 - Various digital tools may be used for educational purposes with teacher guidance and approval.
 - Students may only use their NPS accounts to log into digital tools that have been approved by the district and/or have a data privacy agreement in place, unless the school has obtained parent/guardian permission.
 - Using any digital tools or internet resources to gain an unfair advantage in assignments, assessments or other academic evaluations without the permission of the teacher is prohibited.
 - Presenting someone else's work, ideas, or digital content as one's own is prohibited. This includes copying and pasting from online sources without citation, failing to paraphrase appropriately, or submitting work done by another individual or with the unauthorized assistance of digital tools.
- **F. Data Privacy:**
 - Students should understand that their online activity may be monitored by the Norwood Public Schools for safety and security purposes and therefore there should be no expectation of privacy when using them..
 - The district will take reasonable measures to protect student data.
 - Students should not share their passwords or personal information with others.
- **G. Parental Consent for Google Workspace Additional Services (Students Under 18):**
 - The Norwood Public Schools utilizes Google Workspace for Education, which includes core services essential for educational purposes. These core services are fundamental to our instructional program and may include, but are not limited to: Google Classroom, Drive, Docs, Sheets, Slides, and Gmail.
 - In addition to the core services, some optional Google Workspace additional services may offer enhanced functionality. These additional services may include,

but are not limited to YouTube, Google Earth, Google Groups, Google Photos, Google Maps and more.

- For students under 18 years of age, parental consent is required for the use of these Google Workspace additional services. By signing the student handbook acknowledgement form, parents/guardians are providing consent for their child to use both the Google Workspace core and additional services.
 - Information about the specific Google Workspace core and additional services, including their privacy implications, is available at the following link: [Google Workspace Additional Services Information](#)
 - Parents/guardians who do not wish for their child to utilize the Google Workspace additional services must contact their child's school principal. The school will then ensure the student has access to the core services only, and will work with the student to provide alternative methods for any educational need that the additional services fulfill.
- **H. Consequences:**
 - Violations of this RUP may result in disciplinary action, including loss of technology privileges, possible suspension or other consequences.

III. Staff Use:

- **A. Acceptable Use:**
 - Using district-provided devices and networks for instructional, administrative, and professional development purposes.
 - Accessing approved educational and professional websites and applications.
 - Communicating with students, parents, and colleagues in a professional and respectful manner.
 - Using district resources to enhance student learning and improve educational outcomes.
- **B. Unacceptable Use:**
 - Accessing or distributing inappropriate content.
 - Cyberbullying, harassment, or discrimination.
 - Unauthorized access to networks, systems, or data.
 - Downloading or installing unauthorized software or applications.
 - Using district resources for personal gain or commercial purposes.
 - Violating copyright law or intellectual property rights.
 - Circumventing security/compliance or filtering measures on any hardware or software system used in the Norwood Public Schools.
- **C. Social Media and Communication:**
 - Staff members must maintain professional conduct on social media, especially when representing the district.
 - Posting or sharing content that is defamatory, harassing, or violates the privacy of students, colleagues, or the district is prohibited.

- Staff should not communicate with students on personal accounts, including personal social media accounts. All communication with students and families must be done through school-approved means.
- This policy regarding social media is to be followed in conjunction with school committee policy [JNDD Policy on Social Media](#)
- **D. Generative AI:**
 - Staff can use Generative AI tools to enhance teaching and administrative tasks.
 - Staff may only use AI tools that have been approved by the district and have a student data policy agreement in place.
 - Staff must verify the accuracy of AI-generated content before using it.
 - Staff must adhere to copyright and intellectual property laws when using AI-generated materials.
 - Staff should ensure that the use of AI tools complies with student privacy regulations.
- **E. Data Privacy:**
 - Staff members are responsible for protecting student and district data.
 - Confidential information should be handled with care and stored securely.
 - Staff members must comply with all applicable data privacy laws and regulations, including FERPA, COPPA, HIPAA and state-specific laws.
 - Staff should report any data breaches or potential security risks immediately.
- **F. Consequences:**
 - Violations of this RUP may result in disciplinary action, including warnings, suspension, or termination.

IV. Monitoring and Enforcement:

- The district reserves the right to monitor technology and NPS account use to ensure compliance with this RUP.
- Violations of this RUP will be investigated and addressed according to district policies.
- The district may implement security measures to protect its networks and data.

V. Policy Review:

- This RUP will be reviewed and updated periodically to reflect changes in technology and best practices.

VI. Parent/Guardian Acknowledgement (Student RUP):

- Parents/guardians are required to review and acknowledge this RUP through the district's student handbooks.
- By signing the acknowledgement, parents/guardians agree to support the district's efforts to promote responsible technology use.

VII. Staff Acknowledgement:

- Staff are required to review and acknowledge this RUP annually.