8630

RYE CITY SCHOOL DISTRICT

EMPLOYEE ACCEPTABLE USE OF TECHNOLOGY

The Rye City School District believes that the members of its educational community should be able to utilize every possible learning resource to maximize achievement and increase the probability for future success. Educators should be given opportunities to optimize student learning and teaching, employee performance and productivity.

The District considers access to a computer network, including the Internet, to be a powerful and valuable tool to enhance education, research and communication. Through the use of technology, faculty and staff may access extensive information resources, participate in global communication and utilize powerful tools for creating and learning across the curriculum.

To ensure the proper use of Technology, the Rye City District Acceptable Use Policy (AUP) contains the guidelines for access to and use of the Technology. All Users, which includes employees and contractors of the District, must review and agree to abide by the AUP annually.

User Responsibility and Compliance

1. The rules and obligations described in this AUP apply to all Users of the Rye City School District regardless of whether Users are employees, consultants or authorized visitors. It is each User's duty to use the systems responsibly, professionally, ethically, lawfully, and conduct his/her activities in support of District authorized activities.

2. This AUP shall be implemented and overseen by the District Technology Department personnel, administrators and selected vendors who are responsible for managing and protecting the school information technology systems.

3. Violations of this AUP can result in immediate withdrawal or suspension of access privileges to technology. The District reserves the right to advise law enforcement agencies if a suspected criminal offense has been committed.

4. The District reserves the right to modify, amend, or terminate any provision of this AUP at any time.

Acceptable Use of Technology Systems

1. **Acceptable Uses:** Users may only use technology in support of the educational goals and objectives of the District.

2. **Limit Personal Use:** Users are expected to limit personal communications through the Technology Systems, since these resources are finite and must be shared. Personal use that absorbs a large amount of system resources, or inhibits the responsibilities of the staff member to maintain job responsibilities, at the discretion of the District, may be restricted.

3. **Protect Confidential Use**
    a. Users with access to confidential information must be careful to protect such information from disclosure to unauthorized recipients. “Confidential Information” means any information concerning the District, its business, employees, students, or suppliers that is non-public and includes, but is not limited to, financial information, school plans, marketing plans, student identifiable information, software source and object code, outside contracts, and course materials. In order to prevent unauthorized individuals from viewing such information, Users should exercise proper judgment when sending Confidential Information via e-mail or forwarding e-mail strings containing Confidential Information.
    b. Users shall not invade the privacy of individuals or disclose Confidential Information about another individual or post identifying information, work or pictures without specific permission of the individual. If the individual is a student, permission must be granted by the parent or guardian in writing and all the school, state and federal laws, policies, guidelines must be followed.
    c. All Board policies regarding the confidentiality of student information and all state, federal and local laws regarding technology are to be upheld.
    d. Prior to publishing student work on the Internet, Users will verify that the permission form was signed by a parent or receive parental permission in writing.
    e. Users will obtain consent for recording or photographing others and describe the potential uses of such actions. See Media Release Permission Form.

4. **Use the Internet Cautiously**
    a. Users may access online services, use email and voicemail for school-related assignments, educational, administrative or other professional purposes.
    b. Users should exercise caution when browsing the Internet through the Technology Systems. In order to avoid receiving unsolicited email or email containing offensive content, Users should avoid posting their school email addresses or accounts on the Internet.
    c. The District will use commercial Internet blocking software to prevent receipt of inappropriate email or access to websites deemed inappropriate.
    d. Users are to avoid using the Internet for commercial purposes, financial gain, personal business, product advertisement, religious or political lobbying (including student body elections, union association elections or other communication)
    e. Official representation of the school or (i.e., Internet homepage or website) may be established within the guidelines of the District and comply with all aspects of the District policies and guidelines.
    f. Users are expected to abide by the generally accepted rules of Internet and network etiquette including but not limited to the following: be polite, use appropriate non-abusive language, use only language appropriate in a school setting, identify yourself.
    g. Teachers and IT staff will monitor the use of the Internet by students for grade level and cyber safety appropriate use.
    h. If an employee suspects inappropriate use by a student or another employee, these suspicions should be immediately reported to an administrator and/or the Technology Department.

5. **Network Use and Access**
    a. Network accounts are to be used only by the authorized owner of the account. Users shall not seek to learn, change or share their own or other Users’ passwords, modify other Users’ files or data, or misrepresent other Users of the network.
    b. All employees are to use the District technology to store only materials that are needed for the education and goals and objectives of the District.
    c. Access to online content via the network may be restricted in accordance with our policies and federal regulations, such as the Children’s Internet Protection Act (CIPA).
    d. Users are not to attempt to obtain access to restricted sites, servers, files, databases, or gain unauthorized access to other systems or bypass district filters and security by any means.
    e. The network may not be used to harass others, use abusive or obscene language, bully, annoy or otherwise offend another individual. Users may not send, save, view, or forward offensive content/messages that may include, but not limited to, pornographic, obscene, or sexually explicit

material, sexual comments, jokes or images that would violate school policies or guidelines. School policies, local, state and federal laws against harassment and discrimination apply.

f. Personal devices, including, but not limited to mobile devices, access points, or any other device that accesses the school network may only be used with the permission of the Technology Department.

6. **Wireless Access**
    a. Access to District network resources through wireless networks will be restricted based on the role of the User.
    b. To obtain wireless guest access, available at all buildings, the guest will be authenticated through a web-based authentication system.
    c. Staff using personal devices at school are required to have up-to-date virus protection before being connected to the network. The District is not responsible if a device is damaged in any way, misplaced, or stolen, and will not offer any restitution for loss. The District does not insure personal equipment nor will the District provide repairs or maintenance for it.

7. **Copyright Laws**
    a. Users may not use the Technology Systems in a manner that infringes upon the copyright rights of others. Copyright law protects the exclusive rights of images, music, text, audiovisual materials, software and photographs.
    b. The sharing, duplication, distribution, displaying, or performing of any copyright protected material without the permission of the copyright owner is strictly prohibited.
    c. If the copyright implicitly gives permission for educational use, the User must comply with all permissions and/or restrictions.
    d. Appropriate source documentation and permissions shall be followed whenever copyright electronic sources are reproduced.

8. **Software Licenses**
    a. The Technology Systems include software that is licensed from third parties. Users must use any licensed software or online subscriptions in accordance with the terms of the licensing agreement.
    b. Users may not reproduce or install any software that has not been properly authorized or purchased by the District.
    c. Users may not install personally owned or created software on District networks or computers.
    d. No User may modify, revise, recompile, disassemble, reverse engineer, or otherwise alter any software licensed to the District without prior written authorization from the software vendor.

9. Network Storage: Storage space on the Technology Systems is not an unlimited resource, and Users should take all possible steps to conserve the System's capability. Users should delete unnecessary or unwanted files on a regular basis from network servers, email and folders, and local hard drives. All files stored in the User's downloads folder will be removed on a weekly basis. Storage quotas are set on each User's storage network drives.

10. **District Website:** With regard to the District website and any official District web presence which is developed by, maintained by, or offered through third party vendors and open sources, the District is committed to compliance with the provisions of the Americans with Disabilities Act (ADA), Section 504 and Title II so that students, parents and members of the public with disabilities are able to independently acquire the same information, engage in the same interactions, and enjoy the same benefits and services within the same timeframe as those without disabilities, with substantially equivalent ease of use; and that they are not excluded from participation in, denied the benefits of, or otherwise subjected to discrimination in any District programs, services, and activities delivered online. All existing web content produced by the District, and new, updated and existing web content provided by third-party developers, will confirm to Web Content Accessibility Guidelines (WCAG) 2.0, Level AA conformance, or updated equivalents. See Website Accessibility Policy 4526.2 and Regulations 4526.2-R1/R2.

Inspection and Monitoring of Technology Systems - No Privacy Guarantee

1. Users of the District's computer network should not expect, nor does the District guarantee, privacy for electronic mail (e-mail) or any use of the District's computer network. The District reserves the right to access and view any material stored on District equipment or any material used in conjunction with the District's computer network.

2. Electronic communications (i.e. voice mail, email, Internet) should not be considered completely private and secure. Users should not, under any circumstances, transmit or reveal personal or confidential information about yourself or others, including but not limited to: home address, telephone number, password, social security number, credit card number, or confidential or sensitive information regarding students or staff.

3. The District Technology Department may access and review any information that Users create, store, send, or receive on the Technology Systems, including e-mail and instant messages with the permission of a building or district administrator for cause.

4. The District reserves the right to disable a computer account during periods of investigation and/or review and to gain access to the User's correspondence or files. Once an employee leaves the District, the Technology Department will disable all accounts immediately.

Security

1. **Security Threats**
    a. Users are expected to take reasonable safeguards against the transmission of security threats over the District network. This includes not opening or distributing infected files or programs and not opening files or programs of unknown or untrusted origin.
    b. If you believe a computer or mobile device you are using might be infected with a virus, please alert the Technology Department. Do not attempt to remove the virus yourself or download any programs to help remove the virus.
    c. Attempting to harm or destroy data of another User, another agency or the network by uploading, downloading, or creation of computer viruses is strictly prohibited.

2. **Security Controls**
    a. Users may access only those sections of the Technology Systems to which they have authorization. A User's ability to gain access to other computers or networks within the Technology Systems does not imply a right to such access, unless such access is specifically authorized. Users may not browse the Technology Systems in order to gain access to unauthorized areas.
    b. Users shall not connect to the Technology Systems by any means other than by those specifically defined by the School IT Staff or IT Management. Users may not disable security controls, such as access-management software, virus scanners, passwords, personal firewalls, and audit trails. Users may not attempt to discover security flaws. Tampering with any software protections or restrictions placed on computer applications, files or directories is strictly prohibited.
3. **Mobile Devices**
    a. The District may provide Users with mobile computers (laptops, iPads, tablets, e-readers, etc.) or other devices to promote learning outside of the classroom. Users should abide by the same acceptable use policies when using District devices off the District network as on the District network.
    b. Users are expected to treat these devices with extreme care and caution. Users should report any loss, damage, or malfunction to the Technology Department immediately. Users may be financially accountable for any damage resulting from negligence or misuse.
    c. Use of District-issued mobile devices off the school network may be monitored.

4. **Technology Equipment**
    a. Misuse of District property includes, but is not limited to, stealing or damaging equipment or software, knowingly running or installing computer viruses or password-cracking programs, attempting to circumvent installed data protection methods that are designed and constructed to provide secure data and information, attempting to interfere with the physical computer network/hardware, or attempting to degrade the performance or integrity of any school network or computer system.
    b. Users shall not degrade computer or network equipment, District-owned hardware, software or disrupt

system performance or waste finite network resources.

Logins and Passwords

1. **Login Accounts:** Each individual is issued a network account with a unique login name and password. Passwords must not be shared with any other staff member or student. Users are responsible for all transactions made using their Login. All Users are expected to either lock up or logoff the workstation when they are away from their work area. Users may not disguise their identity while using the Technology Systems.

2. **Password Security:** Users are responsible for safeguarding their Login password. Individual passwords should not be printed, stored online, posted on sticky notes, or shared with others. Users are prohibited from using or disclosing another User's password.

3. **Password Maintenance:** Passwords to District devices and applications may require regular reset and must adhere to the guidelines set for maximum security. If you feel your password has been compromised, please change it as soon as possible and notify the IT department or an administrator.

4. **Passwords Do Not Imply Privacy:** Users should have no expectation of privacy when using the Technology Systems. The fact that certain Users are granted access to password-protected areas of the Technology Systems does not imply that such Users retain any expectation of privacy in material created or received within the Technology Systems. The District reserves the right, without prior notice, to inspect, examine, audit, read, print, and monitor all data stored on the Technology Systems. The district has the ability and reserves the right to bypass individual user passwords and to monitor the use of such systems by staff. Therefore, staff should not expect to maintain personal privacy in the use of the system.

Use of District E-mail

1. All District staff will have an email account created by the Technology Department.
2. Users should check their email and manage the size of mailbox storage.
3. Users of District email systems are responsible for its appropriate use. All illegal or improper use of the electronic mail system, including but not limited to: offensive language or pictures, harassment, solicitation, gambling, violating copyright or intellectual property rights are prohibited.
4. Bulk posting to individuals or groups to overload the system (i.e., spamming or any similar actions) is prohibited, including but not limited to chain letters and pyramid schemes.
5. Do not open or forward email from a sender you do not recognize. Delete it immediately.
6. All email accounts remain the property of the District and can be searched at any time for cause.
7. Users may only use their assigned account and not give others access to it, or use another's email.
8. The broadcasting of any messages using the District's distribution list(s) is for school-related purposes only. Users are to consider the content of their email and the impact that it will have on recipients.
9. Staff and students should use their RCSD email accounts when communicating with one another.
10. Email content must never violate District policy.

Rye City School District Acceptable Use Policy Agreement

I understand and will abide by the provisions and conditions of the District's Acceptable Use Policy. I understand that any violations of the above provisions may result in disciplinary action, the revoking of my User account, and appropriate legal action. As a condition of network use I am obligated to report any use of the District technology systems in a manner inconsistent with or in violation of the Terms and Conditions listed above.

Employee Name: _____ **Employee Signature**: _____

Building: _____ **Date**: _____

Adoption Date: July 11, 2017