Employee Technology Acceptable Use Policy and Code of Conduct

I. INTRODUCTION

In accord with RSA 194:3-d, (I) the purpose of the Acceptable Use Procedures is to provide the procedures, rules, guidelines, and the code of conduct for the use of technology and the Internet.

The District provides computers and other technological devices, networks, and Internet access to support the educational mission of the schools and to enhance the curriculum and learning opportunities for students and school staff. This policy and the accompanying procedures apply to all District technology, whether in use at school or off school premises, and to any technological devices brought by staff into a school building or to a school activity.

This policy applies to all District employees and to any other person who is provided with e-mail, network, or Internet access by the Pittsburg School District.

II. DEFINITIONS

For purposes of this policy and any accompanying procedures, the following terms apply:

- "Employee" or "staff" refer to all Pittsburg School District and School Administrative Unit ("SAU") #7 employees, contract service providers, substitutes, student teachers, interns, volunteers, and employees of a company under contract with the District or SAU.
- "District technology" or "technology resources" or "technological devices," or the like refers to all District or SAU technological devices, whether maintained in a District facility or issued to a District or SAU employee for their use at school or off-school premises.
- "Incidental personal use" is defined as use by an individual employee for occasional personal communications before or after school hours, during prep time, or during lunch break.
- The District network includes any configuration of hardware and software which connects users, whether at the District level or at the SAU. The "network" includes, but is not limited to, electronic mail (e-mail), local databases, externally accessed databases, recorded media, clip art, digital images, digitized information, communications technologies, and new technologies as they become available. Stand-alone workstations and privately owned technology devices are also governed by this policy.

III. ACCEPTABLE USE OF DISTRICT TECHNOLOGY.

Employees who utilize District technology must do so responsibly and in a professional manner. The level of employee access to school technology is based upon specific job requirements and needs. Unauthorized access to secure areas of the District's technology system is strictly prohibited.

Employee Technology Acceptable Use Policy and Code of Conduct

Employees are expected to use appropriate judgment and caution in communications concerning students and staff to ensure that personally identifiable information remains confidential. Emails containing personally identifiable information about students are subject to the requirements of the Family Education Rights and Privacy Act, 20 USC 1232g.

All employees must sign the District's Acceptable Use Policy Agreement form prior to accessing District technology. All employees assume full legal responsibility and may be held financially responsible for their actions when using District technology resources.

Acceptable use of District technology includes, but is not limited to:

- Use that does not interfere with the normal and proper operation of the District technology devices, network, e-mail system, or Internet access;
- Use that does not impede the ability of others to use District technology; and
- Use that is for an educational purpose.
- Maintaining password security.

Incidental personal use of district technology is permitted as long as such use does not violate any of the above.

Classroom employees shall not use district technology for personal use during class time.

Employees who are aware that the District's Acceptable Use Policies or Procedures have been violated must immediately notify the school principal and/or the Superintendent of Schools. The school principal and/or Superintendent of Schools shall document all violations in writing and shall investigate the violation.

The District reserves the right to:

- Monitor all activity on District technology.
- Investigate the use and misuse of District technology.
- Log network use and storage space utilization by user. Log files shall be maintained for 180 days.
- Make determinations on whether specific uses of District technology are consistent with the Acceptable Use Policy and any accompanying procedures.
- Refuse to allow any individual to access District Technology, including the Internet or to remove a user's access to the network if it is determined by the District that the user engaged in unauthorized activity or violated this policy or any accompanying procedures.
- Cooperate fully with any third-party investigation concerning or relating to the District technology.
- Limit usage in accord with the requirements of third-party providers.

IV. UNACCEPTABLE USE

Unacceptable use activities constitute, but are not limited to, any activity in which any user:

- Any use that is illegal or that violates another School District policy, procedure, or school rule, including but not limited to, harassing, bullying, discriminatory, or threatening communications or any other antisocial behaviors; violating copyright laws; profanity, etc. towards other employees, students or third parties. The school assumes no responsibility for illegal activities of employees who use District technology.
- Accessing, creating, viewing, storing, or transferring, or otherwise using materials (including but not limited to, text, images, movies, sound recordings, or electronic or digital files) that are obscene, pornographic, sexually explicit, or sexually suggestive.
- Accessing, creating, viewing, storing, or transferring or otherwise using materials (including, but not limited to, text, images, movies, sound recordings, or electronic or digital files) that are harmful to minors.
- Any use to execute a scheme to defraud, or to obtain for private financial gain, property, services, or other things of value by false pretenses, promises, or representations, or any other use for commercial, advertising, political lobbying, or solicitation purposes.
- Any communication that represents an employee's personal views as those of the school's or that could be misinterpreted as such.
- Downloading or installing software or applications without permission from technology staff. Unauthorized copying of software is illegal and may subject the copier to substantial civil and criminal penalties. The school assumes no responsibility for illegal software copying by employees.
- Seeking to gain, or gaining unauthorized access to information. Any malicious use or disruption of the school's computers or other technological devices, networks, or Internet services; breach of security features; or misuse of computer passwords or accounts (the employee's or those of other users); misrepresenting oneself as another user; and/or accessing another's folders, work, files, or emails.
- Any deliberate misuse or neglect that results in damage to the school's technology equipment.
- Any attempt to access unauthorized sites, or any attempt to disable or circumvent the school's filtering/blocking technology (unless a filter override has been issued by the technology office for purposes that support the educational mission of the district). Creating non-educational hyperlinks between the school's website and other Internet sites is not acceptable.
- Using District technology after such access has been denied or revoked.
- Any attempt to delete, erase, or otherwise conceal any information stored on a school computer or other technological device that violates these rules or other School District policy or school rule, or refusing to return technology equipment issued to the employee upon request.

- Accessing student records without a “legitimate educational interest,” as that phrase is defined in the District’s FERPA policy.
- Unauthorized disclosure of personally identifiable student information contrary to FERPA or District policy.
- Any electronic communication with students or minors, including social networking websites.
- Using District technology for any other use that is inconsistent with the District’s educational mission and/or is not for educational purposes.
- Unauthorized access, including so-called ‘hacking’ and other unlawful activities.

The Pittsburg School District reserves the right to add and include additional inappropriate behaviors and activities that may result in appropriate disciplinary action.

Employees who are uncertain as to whether particular activities are acceptable should seek further guidance from the building principal or other appropriate administrator.

V. INTENTIONAL VIOLATIONS

Any employee who intentionally violates this Acceptable Use Policy and any accompanying procedures shall be subject to disciplinary action in accord with Section VI of this policy. Any employee who intentionally damages District technology shall be subject to disciplinary action in accord with Section VI of this policy. An employee who intentionally damages District technology shall also assume legal and financial responsibility for such damage.

VI. DISCIPLINE

Compliance with the District’s policies, procedures and rules concerning technology use is mandatory. An employee who violates this policy, procedures, and/or any rules governing the use of District technology shall be subject to disciplinary action, including but not limited to one or more of the following: written warning, removal of computer and networking privileges, removal from the classroom, suspension from employment, with or without pay, or termination from employment. Illegal use of the school’s technology may also result in referral to law enforcement.

VII. NO EXPECTATION OF PRIVACY

The District’s technology system remains under the control, custody, and supervision of the District at all times. The District reserves the right to monitor all technology activity by employees and other system users. Employees have no expectation of privacy in their use of any District technology or any technology used on school grounds, including email, stored files, and Internet access logs. Employees have no right to privacy in District technology resources, including but not limited to, District computers, computer network, e-mail, website, and Internet access.

VIII. DUTY TO SUPERVISE STUDENT USE OF DISTRICT TECHNOLOGY

Employees who use District technology with students must supervise such use. Employees are expected to be familiar with the school's policies and rules concerning student technology and Internet use and are required to enforce those policies and rules. When, in the course of their duties, employees become aware of any violation, they are expected to stop the activity and inform the building principal.

IX. NOTICE AND IMPLEMENTATION

Employees shall be informed of this policy and the accompanying rules through handbooks, the district web site, and/or other means selected by the Superintendent.

The Superintendent is responsible for implementing this policy and any accompanying procedures and rules. The Superintendent is authorized to develop additional administrative procedures or school rules to govern the day-to-day management and operations of the District's technology system. Any such procedures or rules shall be consistent with School District policies and rules. The Superintendent may delegate specific responsibilities to building administrators, technology staff, and/or others as he/she deems appropriate.

X. COMPENSATION FOR LOSSES, COSTS, AND/OR DAMAGES

Employees who violate this policy and any accompanying procedures, are responsible for compensating the District for any losses, costs, or damages incurred by the District as a result of the violation.

The District is not responsible for any unauthorized charges or costs incurred by Employees who use District technology.

Cross Reference:
GCSA-R—Employee Technology and Internet Use Rules
IJNDB—Student Technology and Internet Use

Legal Reference
N.H. RSA 194:3-d, School District Computer Networks
N.H. RSA 189:13, Dismissal of Teacher

First Reading & Adoption: March 24, 2014