San Juan School District's Responsible Use Policy for Technology Resources: **Employees**

Introduction

San Juan School District prides itself on providing a high quality network for internet connection and other digital resources for employees in order to provide them the tools and resources that are an essential part of teaching in the 21st century. Access to online resources and other educational technologies is an invaluable asset to the teaching and learning process and the district continues to invest in making technology an integral part of the district's core mission of educating every child in addition to making these resources available to all staff in the business and administrative functions of the school district.

With access to the internet and other available technology comes the need for responsible use from the end-user in the district. It is the purpose of this Responsible Use Policy to inform all employees of the general guidelines for internet and other technology use and the potential consequences for not following these guidelines outlined in this document.

Responsible Use: Internet

While part of the school district's responsibility is to provide access to the internet and its vast array of educational resources, it is also the responsibility of the district to take available precautions to restrict access to materials that may be considered inappropriate, illegal, or of no professional value in the context of the operations of a school district.

As a result, the district has in place a filtering service that is provided by the Utah Education Network (UEN) and which is monitored closely by the district's Educational Technology Department. The filtering service works to block inappropriate materials while still giving staff access to materials that are appropriate to their positions that may not otherwise be available to the general student population. The filtering service does track each site accessed (*and* attempts at access) and records that information. It needs to be clearly understood that there is no expectation of privacy for employees on the network even if the activity is deemed "personal" by the user; accounts are monitored and when inappropriate or illegal sites are accessed or attempted to access, staff will be reported to appropriate school and/or district personnel. Such persons may be subject to immediate discipline up to and including loss of employment and benefits; licensed staff may also be subject to loss of license and endorsement(s). All users of the system also need to understand that due the size of the internet and its ever changing content that filtering will never be perfect. Users will from time to time unintentionally access inappropriate or illegal material; they will also occasionally be blocked from material which is not inappropriate. It is the responsibility of the user to report either of these items occurring to the Educational Technology Department, to protect their own standing and to improve the system for all users.

General Guidelines: Internet

The district's network and the internet and other data access it provides are intended only for educational purposes as it relates to the teaching, learning, business, and administrative functions of the school district.

Employees are responsible for all use associated with their network accounts--this means they are not to share their password with anyone else for any reason including family members, students, etc.; if an employee suspects their network password has been used by someone else, they need to change their password immediately **and** report their concerns immediately to their assigned technician and/or to the Educational Technology Department. (*If help is needed to change a password, the user should contact the Educational Technology Department.*) In addition, please safeguard personal, school, department, and district information in all online communications/activities.

Employees are expected to conduct themselves appropriately at all times while on the internet or on other places on the network. For example (the following *is not* a comprehensive list):

- Employees will use the district's network and internet and other data resources to further their respective roles in the district.
- Employees will interact with staff and students in a responsible, appropriate, and polite manner in all online communications and content creation.
- Employees will only use district email and other district-sponsored communication tools as it relates to their position or to their professional goals, roles, responsibilities, and objectives of San Juan School District. District email and other district-sponsored communication tools are not to be used for political lobbying, sales, solicitations, etc. and other purposes that do not meet the objectives of San Juan School District.
- As explained above, email and other forms of district-sponsored communication tools are not private--private communications need to occur on a private account on the employee's own time.
- As more Web 2.0 tools become available for employees to use in the context of their district positions, the same responsible use as explained in this document and other updated communication will be required.
- Employees are not to communicate in such a way with anyone that would be inappropriate and deemed as harassment or cyberbullying. Cyberbullying is against the law in the state of Utah and against district policy.
- Employees are not to use the district's network and internet access for any illegal, obscene, or inappropriate activities.
- Employees are not to attempt to bypass the filter to access sites that are deemed inappropriate by the school district.
- Employees will not search for, create, duplicate, store, or transmit pornographic materials or items that are sexist, racist, etc.
- Employees will not duplicate, store, or transmit copyrighted materials that are not theirs to use.
- Employees will not share their password(s) with anyone else--employees are responsible for any and all use associated with their account (see above for information about potentially "stolen" passwords)
- Employees will represent themselves, their schools/department, and the district in a professional manner.
- Employees will not attempt to access network files, programs, and other information that they are not allowed nor will they in any way attempt to malicious cause damage to the network.
- Employees are not to abuse data storage on file servers and district email accounts. The district's servers are not designed to house personal music, photos, video, and other digital files (see *Responsible Use: Technology Tools* below for more information).

- Employees will follow all other policies and procedures as it relates to internet use and hardware and software best practices established by the district.

General Guidelines: Mobile Devices and Network Access

As mobile devices such as the iPad become more integrated in the teaching and business process, employees may be able to--if it is deemed appropriate and if it is approved by the Educational Technology Department--have their personal mobile devices joined to the network for those purposes which fit within the scope of their duties within district; mobile devices purchased by the district will be joined to the network. Please note that the same rules and guidelines apply to mobile devices as with all district-owned internet-enabled devices. In most cases personal and mobile devices will be joined to a separate network which provides access to the internet but restricts access to district network resources. Individuals with legitimate professional need for access to inside resources from personal or mobile devices will need to have this access approved by the Educational Technology Department.

Any violation of the above guidelines will result in immediate consequences as outlined by school and district policy--which may include the loss of all internet and network privileges and/or even the loss of employment and benefits; licensed staff may also be subject to loss of license and endorsement(s).

Responsible Use: Technology Tools

As stated above, the district has invested heavily in educational technology and making sure employees have access to network and internet resources--the devices that help each employee fulfill their role in the district also need to be included as part of this Responsible Use Agreement. Computers, printers, cameras, mobile devices, SMART Boards, and a variety of other classroom and business technology are essential to the operation of a 21st century school district and must be treated with care and responsibility. For example, teachers are to have in place rules and procedures for students that guide student use and safeguards such equipment against damage and should also monitor students' use of such equipment at all times; other business and administrative employees should also have and follow rules and procedures which safeguards the technology they work with. Failure to do so will result in a loss of privileges and other consequences as outlined by the schools and/or district.

Employees are given storage space on district servers where they can store their personal work and they are encouraged to use this space for that purpose. District servers are not intended as a place to store personal files, pictures, videos, or music libraries except in cases where these files are part of a work project. In cases where employees take up large amounts of space with personal files the Educational Technology Department reserves the right to delete those files or place space restrictions on the user forcing them to delete them, without notifying the user.

Responsible Use: Private Information

Many district employees have access to private information regarding students, staff, or district business. Much of this information already regulated under law as by the Family Educational Rights and Privacy Act (FERPA) and/or the Health Insurance Portability and Accountability Act (HIPPA). Employees shall be responsible to know which information which they have access to is regulated and to follow those regulations. Even information which is not regulated under law can cause serious damage to individuals or to the district; for this reason employees are responsible to keep private information, such as information which can be used to uniquely identify or impersonate another person, private. This means that they do not transmit private information via standard unencrypted email nor carry such information off of district property on removable media or portable computing devices without first encrypting it and password protecting it.

Disclaimer

While the district and its Educational Technology Department does all in its power to maintain the network and all the data therein, there is the chance for loss of data and/or service due to a number of potential problems. The district will not be responsible for any loss of data and/or service that may occur and recommends to all employees and students that they keep a separate personal backup of those items which are critical to them.

I have read and agree to the district's Responsible Use Agreement and understand that I will be required to read and agree to follow this policy on an annual basis (in print and/or digital format):

Employee Name (print)	
Employee Signature	
Work Location (print)	
Date	