Computer Resource Policy for USD #286 Staff

The use of District **Computer Resources**: All networks (including connections to external networks i.e. Internet), processors, peripherals and supplies under the administration of the USD 286 Technology Director, Library Media Center, and/or other District distributors, is a privilege not a right.

Computer Resources are made available to staff members under the following conditions.

Staff:

All staff whether part time, full time, teaching staff or non teaching staff are allowed access to computer resources in accordance with the following provisions.

Staff Equipment Use:

- All certified teaching staff will be provided a laptop computer, if they choose to accept the offer.
- Staff will be solely responsible for the replacement of the laptop provided to them in the event it is lost or stolen.
- USD 286 will provide productivity related software. If a staff member chooses to purchase personal software they may install said software on their laptop computer.
- Staff members must provide proof that all installed software is legal and not installed illegally on their laptop. USD 286 will not be responsible for illegally installed software on a staff members laptop, the staff member will be responsible for all fines, legal fees, etc. associated with the prosecution of illegal and/or pirated software.
- Laptops are for staff use only, unless the staff member has given others permission to use the laptop for school related work.
- All laptop computers should be given to the Technology Director for repair – Only the Technology Director may submit laptops for repair, DO NOT ENLIST THE SERVICES OF ANY ONE OUTSIDE THE DISTRICT.
- Each classroom will be provided with a minimum of one desktop computer with productivity software for student use. Students will be allowed access to these computers to complete class work, teachers will use their laptops if they need to complete work at the same time students are completing assignments.
- Teachers will not install purchased software on the desktop computers. ONLY the Technology Director or an appointed staff member may install software. Special permission may be obtained from the Technology Director once software licensing has been verified.
- All other technology equipment: digital cameras, projectors, LCD panels, scanners, PDAs, mobile laptop labs, etc. are to be checked out through the Technology Director only. Students are allowed to use the equipment, however the staff member is responsible for teaching the proper usage of the equipment, and must ensure that the equipment will be used properly without damage.

All Staff Internet use shall be for the purpose of:

- Providing information for students or for the teachers of students such that they may have a better understanding of subject matter.
- For the up-skilling of staff through research, professional development and procurement of information via the internet.
- The use of E mail for contact with other teaching staff on school business or to request information to the benefit of the school –NO chain letters should be forwarded. (Email is not considered private and is monitored, District Administration retains the right to review all school e-mails.)
- Use of the Internet for personal use during the contracted business day is not permitted.
- Internet use using the WWW shall be for school purposes only, no home based business related work shall be done using the District network or equipment.
- Internet Chat shall be for classroom purposes only

USD 286 Liability

- USD 286 is not, and cannot be held responsible for the loss of material, accidental corruption or any other action that might affect transmission or loss of data.

- USD 286 has taken all possible precautions to maintain safety of all users and these guidelines are written and enforced in the interest of all users safety and effective use of the Internet.

- If requested, USD 286 must comply with providing access to data that is considered public knowledge, e-mail content and web sites accessed are logged and do fall into this category.

Computer Resource Usage:

Definitions:

Computer Resources:
All networks (including connections to external networks i.e. Internet), processors, peripherals and supplies under the administration of the USD 286 Technology Director, Library Media Center, and/or other District distributers.

Computer Account:
A computer resource user's unique ID, which allows them access to specific computer resources.

Rights:
Use of the USD 286 computer resources is a privilege and not a right. As with all privileges, abuses will not be tolerated.

Inappropriate Usage:
Examples of inappropriate usage include, but are not limited to, the activities in the following list:
* Use a computer account that you are not authorized to use.
* Allow use, of your computer account to another individual.
* Attempt to read, copy, change, or delete another user's files without the explicit agreement of the owner.
* Use the school's network to gain unauthorized access to any computer system or network.
* Knowingly run or install a program on any computer system or network, or give to another user, that intends to damage or to place excessive load on a computer system or network.
* Attempt to circumvent data protection schemes or uncover security loopholes on any computer resource within the school or connected to the school.
* Violate, terms of applicable software licensing agreements or copyright laws.
* Deliberately waste computer resources.
* Use electronic mail or messaging services to send , threatening, harassing or abusive messages.
* Employ personal use during scheduled work time.
* Use, computer resources for personal reasons that result in an expense to the school, or attend to other matters of a vocational nature not related to school business.
* Transmit or possess materials which explicitly or implicitly refer to sexual conduct.

Privacy:
The computer resource administrators, in order to preserve the integrity or operational state of all computer resources, may find it necessary to manipulate, without prior consent, any data or files of any users that exist on any resource.

You should be aware that no computer security system, no matter how elaborate, can absolutely prevent a determined person from accessing stored information that they are not authorized to access. Thus, while the network tries to provide a reasonable level of confidentiality for information stored on the network, we cannot guarantee the privacy and/or confidentiality of any information stored on it. Therefore, if there is any information that must remain confidential, you should not store it on the network.

The USD 286 Network Administrator, Principals, and Superintendent reserve the right to read and/or remove any files on the system without prior notification to system users.

Internet Information Content:
The USD 286 Network Administrator, Principals, and Superintendent have no control of the information on the Internet. USD 286 Network Administrator, Principals, and Superintendent do provide the following technological barriers: Shelterbelt proxy server and PIX firewall, to account holders accessing the full range of information available. Sites accessible via the Internet may contain material that is illegal, defamatory, inaccurate, or potentially offensive to some people. Access to any information on the Internet is ultimately the responsibility of the user.

Vandalism Policy:
Due to the complexity and cost of technology within USD 286, when any user's actions

results in damage to any computer resource, all costs incurred for repair will be the responsibility of the user. Due to the possible damages caused by diskette usage, a virus-scanning program must examine all diskettes not originating and being used strictly within the school before being placed into any computer.

Software Installation:
Only individuals assigned by the Technology Director may install software (demo or full version) onto any computer resource within the school.

Staff:
Shall include, but not be limited to, part time, full time, teaching staff and non teaching staff, office administrators, technology directors, principals, superintendents, etc.

Computer Usage Policy Enforcement Guidelines:
An individual's computer resource use privilege may be suspended immediately upon the discovery of a possible violation of the policies.
Depending on the nature and severity of the policy violation, the school may take one or more of the following disciplinary actions:
* Verbal, written, or electronic mail warning.
* Probational usage and monitoring.
* Temporary access denial (account lockout).
* Permanent access revocation.
* Disciplinary school suspension.
* Alternative, disciplinary action not involving access or usage restrictions.
* If warranted, the principals and/or superintendent will refer the case to an appropriate local, national, or federal authority for further disposition.

Demonstrated intent to violate policy will be considered the same as an actual policy violation.
Demonstrated intent means evidence of actions, that if successful or if carried out as intended, would result in a policy violation.

(Employee Copy)

Authorization For Use Of Computer Resources Within USD 286.

Staff signatures are required below prior to use of computer resources within the school.

As a Staff member of USD 286, I agree to abide to the school's policies regarding use of computer resources.

Staff name: _____

Staff signature: _____

Date: _____

District Copy

Authorization For Use Of Computer Resources Within USD 286.

Staff signatures are required below prior to use of computer resources within the school.

As a Staff member of USD 286, I agree to abide to the school's policies regarding use of computer resources.

Staff name: _____

Staff signature: _____

Date: _____