

Technology Acceptable Use Policy (AUP) and Website Guidelines

North St. Francois County R-I School District Bonne Terre, MO



The North St. Francois County R-I School District recognizes the educational and professional value of technology as a communication, educational, and work place tool. The North St. Francois County R-I School District promotes web development as a communication tool between the school district and/or parents, students, and community. The district web site will provide information including but not limited to the following: curriculum, wellness, school related sports and activities information, employee information, school board information, employment information, etc.

Users are defined to include, but are not limited to, all district employees, substitute teachers, full-time and part-time students, UCC students, and/or alternative program students. A user may be designated by the school board, superintendent, and/or building principal(s).

All users signing the “Student Technology Acceptable Use Policy (AUP) Agreement and Website Consent” or the “Employee Technology Acceptable Use Policy (AUP) Agreement and Website Consent” signature form state they have read, in its entirety, this document and agree to comply with the following policy and guidelines.

To meet a lesson objective students may be required to complete the ‘Student Technology Acceptable Use Policy (AUP) Agreement and Website Consent’ form. Failure to sign the form, by either the student or parent, may result in a grade reduction or removal from the course to another course. A \$1.00 technology fee is required before high school students (9-12 grades) receive a computer ID/password. This fee may be paid at the time of registration or to a high school library staff member. The fee is not subject to prorating during the school year.

User Agreement

Use of the district’s technology resources is a privilege, not a right. Users must adhere to district policies, regulations, procedures, and other district guidelines. Therefore, a consistently high level of professional and personal responsibility is expected of all users granted access to the district’s technology resources and/or personal use by personally owned technology. Unless authorized by the superintendent or designee, all users (full time district employees, students, and others as designated by the superintendent) must have an appropriately signed ‘Technology Acceptable Use Policy (AUP) and Website Consent’ on file with the district before they are allowed access to district technology resources. All users must agree to use district technology, on and off district property, in compliance with the district’s policies, regulations and procedures and all local, state, and federal laws.

User Identification and Network Security

All users shall immediately report any security problems or misuse of the district’s technology resources to an administrator, teacher, direct supervisor, librarian, webmaster, or technology department. No student, employee, or other potential user will be given an ID, password or other access to district technology if he/she is considered a security risk by the superintendent or designee.

Attempting to sign, applying for and/or signing an ‘AUP’ for a user ID under false pretenses is prohibited. Using another person’s user ID and/or password is prohibited unless authorized by the school board, superintendent, and/or building principal. Sharing one’s user ID and/or password, for any current or future district program, with any other person, whether a district employee or not, is prohibited unless authorized by the superintendent or direct supervisor. A user will be responsible for stored files and actions taken by any person using the ID or password assigned to the user.

Upon the employee’s resignation, retirement, or termination of employment an employee’s computer ID and/or password will be deleted from the system. Files and/or web page(s) may be assigned to an employee of the North County R-I School District.

Privacy

A user does not have a legal expectation of privacy in the user’s electronic mail (personal or district assigned), Internet use, other activities involving the district’s technology resources and/or the user’s personally owned technology or software. At any time the district may examine stored on district technology resources and/or the user’s personally owned technology for determination of a potential violation of this document. At any time, without prior knowledge or approval from the user, the superintendent, building principal(s), direct supervisor, technology plan coordinator, instructor, webmaster, librarian, and/or technology department may monitor employee and/or student district and personal technology usage or initiate monitoring or examination of usage/files by naming a designee. However, employees or students may not monitor activity or examine information of their chain of command supervisor and/or instructor unless designated by the school board, superintendent, legal counsel, and/or legal warrant. Electronic communications, all data stored on the district’s technology resources and/or the user’s personally owned technology or software, and downloaded material, including files deleted from a user’s account, may be intercepted, accessed or searched by district administrators or designees at any time.

Content Filtering and Monitoring

This form states that the North St. Francois County R-I School District strives to meet state and federal guidelines and the Children’s Internet Protection Act (CIPA). District users and student parents/guardians are advised that district technology can not be guaranteed to be completely

effective. Innocuous Internet search requests may accidentally lead to educationally objectionable sites. Users access the Internet at their own risk. No filtering software is 100 percent effective, and it is possible that the software could fail. Authorized student users access the Internet at their own risk. If the filtering software is unsuccessful, and children and staff gain access to inappropriate and/or harmful material, the school district will not be liable. To minimize student risks, students are to abide by this policy.

To comply with the Children's Internet Protection Act (CIPA), the school district has installed filtering and/or blocking software on the district's servers to restrict access to Internet sites that contain material "harmful to minors". Because the district's server and technology is a shared resource, the filtering/blocking software will apply to all district computers with Internet access. Evasion or disabling of the filtering/blocking software installed by the district, including attempts to evade or disable, is a violation of district policy. Discipline is at the discretion of the building principal or supervisor following district guidelines.

Violation of any provision of the Family Educational Rights and Privacy Act (FERPA) which makes confidential a student's educational records, including, but not limited to, a student's grades and test scores may result in disciplinary action.

The superintendent, building principal direct employee supervisor, district technology coordinator, and/or technology department, may access and monitor, without creator permission, any curriculum related online course, blog, discussion board, etc. content created by district employees and/or students on and off district property and/or using district or personally owned technology.

No Warranty/Availability/No Endorsement

The district makes no warranties of any kind, whether expressed or implied, for the services, products or access it provides. The district's technology resources are available on an "as is, as available" basis. The superintendent, building principal, direct supervisor, technology plan coordinator, webmaster, and/or technology department may suspend access to and/or availability of the district's technology resources to diagnose and investigate network problems or potential violations of any law or district policies, regulations and procedures.

The district is not responsible for loss of data, web pages, delays, non-deliveries, mis-deliveries or service interruptions. The district does not guarantee the accuracy or quality of information obtained from the Internet, or use of its technology resources. Access does not include endorsement of content or the accuracy of the information obtained.

District Technology Resources and Usage

The following is prohibited:

Use of district technology resources in attempting to gain or gaining unauthorized access to any technology equipment, system or the files of another is prohibited.

The deletion, reading, examination, forging, copying or modification of files, web pages, e-mail and/or data belonging to other users without their prior consent.

Accessing and/or disclosing the contents or existence of District computer files, confidential documents, e-mail correspondence, or other information to anyone other than authorized recipients or supervisors. In the case of suspect violation of this policy the information may be disclosed to local, state or federal officials.

Use of district technology to connect to other systems, in evasion of the physical limitations of the remote system.

Mass consumption of technology resources that inhibits use by others.

Non-educational uses of NCS D's network including, but not limited to games, wagering, gambling, junk mail, chain letters, jokes, private business activities, raffles, fundraisers, religious activities, personal or political purposes.

Use of district technology for soliciting, advertising, promoting political or religious beliefs, fund-raising, commercial purposes or for financial gain, unless authorized by the superintendent and/or school board.

To access fee services without permission from an administrator. A user who accesses such services without permission is solely responsible for all charges incurred.

To access, view, disseminate, directly link or within two clicks or less from a district web page link to information while using district resources and/or personally owned technology or software, including, but not limited to e-mail, Internet access, twitters, blogs, sexting, texting, or web pages that are pornographic, obscene, child pornography, harmful to minors, obscene to minors, libelous, racist, pervasively indecent or vulgar, discriminating or harassing any person or persons' rights, technology use that constitutes insulting or fighting words, the very expression of which injures or harasses other people (e.g. threats of violence, defamation of character or of a person's race, religion or ethnic origin); presents a clear and present likelihood that, because of their content or their manner of distribution, will cause a material and substantial disruption of the proper and orderly operation and discipline of the school or school activities; or will cause the commission of unlawful acts or the violation of lawful school regulations; or advertising any product or service not permitted to minors, and/or any technology use that violates any law and/or district board policies or regulations.

To use the school district system and/or personally owned technology or software to access, review, upload, download, store, share, fileshare, print, post, or distribute materials that graphically depict or advocate violence, that advocate dangerous or illegal acts, that advocate discrimination (hate literature), or that constitute harassment, bullying, intimidation, or discrimination.

Accessing, viewing or disseminating information on any product or service not permitted to minors is prohibited unless under the direction and supervision of district staff for curriculum-related purposes.

Any unauthorized, deliberate, negligent action and/or attempt to, which damages or disrupts technology, alters its normal performance, or causes it to malfunction is prohibited, regardless of the location or the duration of the disruption.

Remove any district technology or software from the district premises, unless authorized by the superintendent, district administrators, and/or direct supervisor.

To create student district and/or personal email addresses.

Students may not access the Internet without a teacher or other district staff member present in a computer lab or classroom nor secure or attempt to secure a higher level of privilege on the technology resources.

To create, attempt to create, download, use, and/or introduce computer “viruses,” “hacking” tools, tunneling, or other disruptive/destructive programs into a school computer, the school network, or any external networks.

To add, remove or alter computer passwords, security measures, configuration settings or monitoring devices without school board, superintendent, librarian, technology department, and/or the building principal’s authorization.

Any file that can interfere with the normal operation of the computer and/or compromise the network security, including but not limited to: unauthorized file sharing, downloading unauthorized games, programs, files, posting, emailing, transmitting, or otherwise making available any content that is unlawful or dangerous.

Streaming any online content not curriculum related or necessary to complete a school assigned work task.

Other files as new technologies are developed and in violation of this document. See the technology web page for files that can and cannot be downloaded. This page will be periodically updated as new technology emerges.

Linking to purchase school related or non school related products, unless approved by the superintendent and/or school board.

Students using teacher computers and/or computers not designated for student use, even if the teacher and/or substitute teacher gives permission for computer usage.

Teachers will supervise students using computers or approved technology to meet a lesson objective. No games are allowed during instructional or student free time, with the exception that the game is curriculum related, written in the curriculum guide, and approved by the building principal.

No substitute teacher or substitute employee, in any district capacity, may use district technology, without superintendent and/or building principal approval.

Roughly handle, hit, mark on, color on, deface in any way, alter or abuse, play around, scuffle, eat, drink or have liquids of any kind around computer and/or media equipment or in any way deface, alter or abuse, move, unplug or adjust computer equipment without permission from the technology department.

Student attempting or using credit cards through any district technology source.

Intentional or negligent attempts, whether successful or unsuccessful, to interfere with the ability of others to utilize any district technology.

All district-wide emails require the approval of one of the following: superintendent, principal and/or technology plan coordinator. The sender is required to state in the body, preferably in the email introduction, the name of the administrator/coordinator approving the district-wide email. All district-wide emails must abide by this policy.

Using Internet tools such as, but not limited to, discussion boards, Blogs, Twitter, texting, chat rooms, and instant messaging for personal rather than educational purposes. Such use for curriculum must be approved by the District Technology Committee.

Any user using school technology to access and/or update social networking programs such as but not limited to Facebook, MySpace, etc. in school or on personal time, that violates this policy, will result in disciplinary action as determined by the employee’s supervisor, teacher, administrator or school board.

Forwarding out of district emails with non-employee emails within the forwarding email.

Any use or attempted use not stated elsewhere in this policy that may compromise the district network security, operations, and/or privacy violations is prohibited and subjected to disciplinary action.

Allowable technology uses:

Comply with all federal or state copyright laws by containing unauthorized or plagiarized content (including written materials, pictures, graphics, audio, video, and/or yet developed technology). State copyright guidelines, "Copyright Applies to Everyone", may be viewed at the following web address: <http://www.dese.state.mo.us/divimjprovc/curriculum/copyright/index.htm> or search DESE's web site for the full document.

Install and use properly licensed software, audio or video media purchased by the district or approved for use by the district. All users will adhere to the limitations of the district's technology licenses. Copying for home use is prohibited unless permitted by the district's license, and approved by the district.

Users should only access computer programs that have been placed on their menus and/or district web site. See the technology web page for approved downloadable files. It is the responsibility of the user to periodically check the technology web page for updates.

Only district approved online course management systems, for example, NCS D Moodle (hosted on district server), Blogs, Texting, Message Boards, READ, etc. or web editing web sites, for example; Teacher Web or School Notes for the purpose of curriculum, extra curriculum activity and/or sports development. An updated list, as an addendum to this document, is accessible on the technology department web page. Students are required to have parent/guardian permission, except where the student is of legal age (18 yrs.) or court emancipated to participate, create, or manage any online course/program listed above but not limited to yet developed web based and/or NCS D server hosted software communication or curriculum related programs. It is the responsibility of the creator and user to stay informed by checking for program updates on the technology department's web page.

Employees may subscribe to curriculum related newsletters, online notices, online marketers/advertisements, listservs, etc. necessary to complete a school related work task.

Technology Security and Unauthorized Access

It shall be the responsibility of all users to appropriately supervise and monitor usage of district technology including but not limited to: Internet usage, online course management system, Blogs, Message Boards, etc. to ensure compliance with this document and the Children's Internet Protection Act. If a user inadvertently accesses inappropriate information, he or she should immediately disclose the inadvertent access to a teacher, administrator, or direct supervisor. All users are to promptly report any breaches or attempted breach of district security to their teacher, administrator, direct supervisor, librarian, or technology department. A Technology Violation Form may be used to report a violation and is available at: <http://www.ncsd.k12.mo.us/tech/techforms/techviolation.pdf> Failure to promptly report any incident may subject the user to corrective action consistent with the District's board policies, procedures, and regulations.

Technology Safety - Disclosure, Use, and Dissemination of Personal Information

As outlined in the district technology plan, students will be instructed on the dangers of sharing personal information about themselves or others over the Internet.

Student users are prohibited from sharing personal information about themselves or others using the Internet, district technology resources, and/or personally owned technology or software, unless with parent and/or guardian approval and authorized by the district. Student users shall not agree to meet with someone they have met on-line without parental approval. A student user shall promptly disclose to his/her teacher or another school employee any message the user receives that is inappropriate, bullying in nature, or makes the user feel uncomfortable.

District technology and/or personally owned technology or software used for online chatting, IM messaging, Twitter, texting, sexting, or other yet developed online communications that violates any law and/or board policies, procedures, and regulations is prohibited. Any communication form, equipment and/or software using district or personally owned technology and/or software that possibly merits educational use can be evaluated by the technology committee for curriculum use. A list of approved online communications may be found on the technology web page. It is the user's responsibility to periodically check the technology web page for updates.

All district employees will abide by all laws, including FERPA, and board policies and regulations when communicating student information. All student information is confidential, therefore employees transmitting student information using district or personal technology and/or email will not post the student's name in the 'subject line'. Employees will take precautions to prevent negligent disclosure of student information or student records while using district or personally owned technology on or off district property.

No curriculum or non-curriculum related publication distributed using district technology will include the address, phone number or e-mail address of any student without permission.

Students participating in any online curriculum activity including, but not limited to; class projects, typing assignments, texting, an online course, blog, discussion group, etc. will be required to sign a “FERPA Consent Form for Online Curriculum Activity Participation” form in addition to the ‘Student Technology Acceptable Use Policy (AUP) Agreement and Website Consent’ form. Parent/guardians will also be required to sign the permission form before the student can participate in the online activity. This form may be a requirement for some coursework. Students will follow all rules, regulations, and expectations as outlined by the online activity moderator. Failure to sign, student or parent, the required form(s) may result in a grade reduction, course failure and/or removal from the course to another course.

In the case of a research project in a non-related online curriculum activity that requires a “FERPA Consent Form for Online Curriculum Activity Participation” form for the class, that does require online resources teachers will make available print copies to students without Internet accessibility.

Students are prohibited from subscribing to newsletters, list serves, blogs, and/or discussion groups unless a part of an online curriculum approved activity. Students will adhere to the instructor’s guidelines for online curriculum related activities.

With teachers, counselors, librarians, and/or administrators permission a student user may access a personal email account for college, homework, scholarship, and/or career information. The student must obtain permission before accessing a personal email account. Failure to do so may result in disciplinary action. Students are to use a student computer for approved access not an employee’s computer.

No district web page may contain a direct link or two links (‘clicks’) away, from a district web page that violates any portion of this policy.

Employee Users

Authorized employees may use the district’s technology resources for reasonable, incidental personal purposes as long as the user does not violate any provision of this document, board policies or regulations or any law. All employees must model the behavior expected of students, exhibit the same judgment as expected of students, and serve as role models for students.

Web page guidelines

When creating and maintaining web pages the web page creator and/or responsible party is to comply with, in it’s entirety, this document, ‘Technology Acceptable Use policy (AP) and Website Guidelines’ in addition to the guidelines listed below:

All web pages are the ownership of the North St. Francois R-I School District and stored on the district server, except if an approved web editor program is used and stored on a remote server. A list of approvable web editors with remote storage access is available on the technology department’s web page.

Web pages stored on remote servers are to comply with this document. All web pages stored on remote servers are to be approved by the superintendent and/or building principal and webmaster. The creator of a remotely stored web page is to supply the web address to the webmaster.

All web pages, district or remotely stored, are subject to review from the root of the district server, at any time by North County’s district webmaster, technology department, and/or district administrators.

Any employee, student, and/or community patron of the North County R-I School District is free to notify the district webmaster of any content, link, or page design that may violate any portion of this document. Notification may be in the form of completing a district “Technology Violation” form or directly reporting to the superintendent, building principal, direct supervisor, technology plan coordinator, or technology department.

Class and/or department web pages are required to be linked from a building faculty page, from the responsible faculty person’s name. Web pages are to target appropriate curriculum and/or lesson objectives. Activity, club, organizational, sports, and other extra-curricular web pages are to be linked from the appropriate district web page, not a faculty page. These pages also are to be approved by the building principal and webmaster.

Web pages are required to have written parental permission to display a student’s name, individual photo, or personal information. The web page creator is to keep a copy of the ‘Student Technology Acceptable Use Policy (AUP) Agreement and Website Consent’ form on file. Student information not to be displayed includes attaching his/her name to a specific picture, phone number or address to a photo. Class photos can be posted as long as the picture doesn’t explain which individuals are standing where in the picture.

A student’s name may appear as a responsible party at the bottom of an individual web page with the supervising school employee’s name and contact information. DO NOT provide contact information for the student. Students are only allowed to create web pages as part of a curriculum objective with parental/guardian approval.

Web pages are required to have written permission to display the name or picture of administrators, faculty, staff, or school board members.

Links to individual news articles containing information about district employees or students is prohibited. A web page may link to the homepage of a news source.

Web sites that can be reached in two clicks or less from any district web page should not contain or point to pornographic, violent, obscene, objectionable, offensive material, and/or a violation of board regulations and policies.

Using copyrighted materials, graphics, including commercial software, without permission of the copyright holder, and in violation of state, federal or international copyright laws is prohibited. If web page creators are unsure whether or not they are using materials in violation of copyright

provisions, they should ask the librarian, teacher, or administrator for assistance. School-based personnel are encouraged to contact the Department of Elementary and Secondary Education (DESE) if they have questions regarding the use of copyright materials.

Web pages should never contain information or material that the district would not be willing to publish in other media forms (e.g., newspaper, television, brochures, etc.).

Must have the responsible school employee's name and contact information, contact information (school email address or phone number) at the bottom of individual web pages.

Never promote specific political, metaphysical or religious viewpoints or agendas. Links to such pages may be placed on a web page for research purposes if the links are balanced.

The superintendent, webmaster and/or technology department have the right to limit use of graphics and current and new technologies on district web pages to ensure server space for all district personnel web pages.

District approved web design elements are accessible on the technology departments web page. It is the web page creator's responsibility to follow the design elements and periodically check the technology department's web page for updates.

Violation of Technology Acceptable Use Policy (AUP) and Website Guidelines

Use of technology resources in a disruptive, inappropriate or illegal manner impairs the district's mission, squanders resources and shall not be tolerated. Therefore, a consistently high level of personal responsibility is expected of all users granted access to the district's technology resources. It shall be a violation of district policy for any employee or student to engage in any activity that does not conform to the established purpose and general rules and policies of the district's technology resources as set out in this document and district board policies and regulations. Any attempted violation of this document and/or district policy, regulations or procedures, regardless of the success or failure of the attempt, may result in the same discipline or suspension of privileges as that of an actual violation.

Users are required to comply with this technology acceptable use policy and website guidelines, all local, state, and federal laws, including criminal, copyright, privacy, defamation and obscenity laws and NCSD's district board policies and regulations. All damages incurred by the district due to the misuse of the district's technology resources by any user, including the loss of property and employee time, will be charged to the user. Monetary restitution for equipment or software will not exceed the replacement cost of the damage or destroyed technology/software. Disciplinary action is at the discretion of the school board, district administrators, direct supervisors, technology department, webmaster, and/or librarians. Disciplinary action may include, but not limited to, suspension of user technology usage expulsion from school or employment. Students and their parents/guardians accept that if a student is enrolled in a course that requires the use of technology and the student violates any portion of this document disciplinary action is a result of a violation(s) of any portion of this document grades may suffer or loss of course credit even if the course requires

The school district will render all reasonable assistance to local, state or federal officials for the investigation and prosecution of persons using district technology in violation of any law. District administrators have the authority to sign any criminal complaint regarding district technology.

Addendum

The North St. Francois County R-I School District recognizes that technology rapidly changes; therefore, updates to this document may be found on the technology department's web page. It is the user's responsibility to periodically check this website for updates.

The Technology Acceptable Use Policy (AUP) and Website Guidelines is available online at: http://www.ncsd.k12.mo.us/techplan/NCSD_AUP_2009.pdf

Board Approved: July 30, 2009