



Chesterfield County Schools Acceptable Use Guidelines Employee Agreement

The Chesterfield County School District views the use of technology as a tool for productivity and learning. As such, technology operates as an extension of the classroom and library media center, and is an integral part of the curriculum. These guidelines extend to both school and home use of all District network and District-owned technology, including computers, laptops, printers, handheld devices, digital cameras, digital media players, televisions, and digital white boards.

The District expects responsible behavior from all technology users, including faculty and staff. Violation of the following guidelines may result in legal or disciplinary action, including termination, repair or replacement charges, and referral to law enforcement as appropriate. Faculty and staff have greater access than students to technological resources, including equipment, passwords, and Internet sites, and should act responsibly to protect against theft and abuse.

The District uses filtering software designed to prevent access to certain sites and monitors the network activity of all users as they access e-mail, websites, instant messages, chat rooms, and bulletin boards. Administrators reserve the right to examine, use, and disclose any data found on the school's information networks to further the health, safety, discipline, or security of any person, or to protect property.

Technological resources include, but are not limited to CPUs, monitors, keyboards, mice, printers, modems, disk drives, cables, connections, switches, handheld devices, cellular phones, digital cameras, digital media players, televisions, digital white boards, and electrical supplies.

Appropriate Uses and Care of Technological Resources

Employees agree to:

- Use technological resources for educational purposes only, including reference and inquiry, as well as production of educational documents.
- Review and familiarize yourself with the District's Acceptable Use Guidelines for students and any applicable disciplinary consequences that may result from violating those guidelines.
- Ask for assistance if you do not know how to operate any equipment.
- Use appropriate procedures for start-up, shut-down, and log-in functions.
- Keep food, drinks, gum, and magnets away from all equipment.
- Remember that students are not to play games or use technological resources for any non-academic activities during instructional time.
- Follow all copyright laws when using information from electronic resources (e.g. online databases, electronic encyclopedias, news services), including using appropriate reference citations.
- Never download, use, or copy illegal music, games, software, or other copyright-protected files.
- Never delete, alter, or modify software on school equipment. This includes modifying system setups, such as Windows desktop controls, menu settings, or network security settings.
- Never knowingly use portable data storage devices which contain viruses or in any other way knowingly spread computer viruses.
- Never damage or deface technological resources in any manner.

Communications and E-mail

Employees agree to:

- Never create or transmit material in violation of District guidelines or policies or any local, state, or federal law. This material includes, but is not limited to, material that is copyrighted or protected by trade secret, threatening, bullying, gang-related, obscene or pornographic, and information transmitted via sexting.
- Never post your own or anyone else's personal data (e.g. full name, address, phone number, social security number, personal photograph) or engage in any activity that results in the loss of another person's privacy.
- Remember that student communication is limited to use of District-provided accounts unless approved by a District administrator. Social networking sites are strictly prohibited for students.
- Never run an executable file attached to an e-mail message without receiving prior authorization.
- Never send confidential information using District technological resources.
- Limit e-mail to school-related communication only. All electronic communications are the property of the District and must be conducted in a professional, polite, and considerate manner. Employees are prohibited from using District technological resources, including e-mail, for personal businesses, sales, or commercial purposes.
- Remember that any information, such as e-mail, text messages, instant messages, or messages on social networking sites transmitted through District- or privately-owned technological equipment, either during or outside of school hours, is the concern of the District if it prevents the employee from effectively performing assigned functions during duty hours, disrupts the educational environment, or violates state or federal law, board policy, or contractual agreements.
- Never fraternize with students through electronic means, including through social networking sites, except on matters that pertain to school-related issues.
- Remember that any behavior of a sexual nature which may constitute professional misconduct and/or is a violation of criminal or civil statutes, professional codes of ethics or board policy, is strictly prohibited. This includes any action or conduct communicated or performed in person, in writing and/or electronically through such means as telephone, email, text messages, instant messages or social networking sites.

Software, Internet, and System Security

Employees agree to:

- Only use District-approved software and never install, copy, or execute software not approved by the District.
- Only use computers connected to the network with security software installed. Any computer brought from home must first be checked by District personnel to ensure it has appropriate software, licensing, security, and updates.
- Never circumvent any filtering software provided by the District.
- Never attempt to access inappropriate sites such as those that contain obscenity, pornography, advertisements for products or services not permitted to minors by law, bullying, hate or gang sites, or other sites which may be harmful to minors or may cause a substantial disruption to the academic environment.
- Never engage in any activity that might be harmful to the computer or network, such as sending mass forward e-mails or e-mail blasts, creating viruses, damaging files, disrupting service intentionally, or accessing hacking programs.
- Never alter files, change BIOS settings, or hide directories or files.
- Never obtain unauthorized remote access or hack into school resources.

Classroom Use of Online Resources

Employees are responsible for reviewing the acceptable use guidelines with students prior to using technological resources and should always closely supervise students as they access technology. All online resources and searches should be previewed before presenting to students. Guided Internet use involves employees modeling or directing student use of specific online resources to small groups or an entire class, whereas independent Internet use involves employees directing student use of appropriate online resources to students working independently or in small groups. While only guided Internet use should be used for elementary students, both guided and independent Internet use are appropriate for middle and high school students.

Ownership of Property

Upon the employee's separation from the District, all hardware, software, e-mail, and electronic files created by the employee are considered the property of the District. Employee access of District-owned technological resources terminates upon leaving employment, and all District-owned equipment must be returned to the employee's administrator.

Summary

These Acceptable Use Guidelines are designed to describe how the District expects technological resources to be used. Employees violating these guidelines may suffer disciplinary action up to and including termination. The District's goal is to provide employees and students with access to technology in a safe environment that encourages and supports instruction. As users of these technologies, employees are expected to read, understand, and acknowledge these employee guidelines, student guidelines, Board Policies IJNDB and GBEB, and Administrative Rule IJNDB-R before using technological resources.

Enforcement

The District considers any violation of the Acceptable Use Guidelines to be a serious offense and reserves the right to copy and examine any files or information present on District systems allegedly related to unacceptable use. Violators are subject to disciplinary action. Offenders also may be prosecuted under laws including, but not limited to, the Privacy Protection Act of 1974, The Computer Fraud and Abuse Act of 1986, The Computer Virus Eradication Act of 1989, Interstate Transportation of Stolen Property Act, the Electronic Communications Privacy Act, and the Children's Internet Protection Act. If an employee incurs unauthorized costs, he or she will be responsible for all such costs.

The District monitors all computer usage through a security system. Federal law mandates that all computer activity within schools be closely watched in order to ensure the safety of our students. It is the policy of the District to: (a) prevent access over its computer network to, or transmission of, inappropriate material via Internet, e-mail, or other forms of direct electronic communications; (b) prevent unauthorized access, including so-called "hacking," and other unlawful online activity; (c) prevent unauthorized online disclosure, use, or dissemination of personal identification information of minors; and (d) comply with all applicable laws and regulations.

Employee Name (Print): _____

Sign and return this section to your school/supervisor. Please keep pages 1-3 for your records.

Signatures

I understand and agree to abide by the Chesterfield County School District's Acceptable Use Guidelines. I understand that there are consequences if I do not follow these guidelines.

Employee Signature

Date