

TECHNOLOGY RESOURCES

Scope of Rules and Regulations and School District Authority

These Rules and Regulations are promulgated pursuant to the Technology Resources Policy (the "Policy"). These Rules and Regulations govern all use of District computers and other telecommunication devices, the District's local and/or wide area network, and access to the Internet through District computers or the District's local and/or wide area network, which will be collectively referred to in these Rules and Regulations as the District's "network."

The rights of the District include, but are not limited to, those set forth in the Policy and these Rules and Regulations. The Policy and these Rules and Regulations may be supplemented by additional rules, regulations, and other terms and conditions of network use that may be promulgated by District staff pursuant to the Policy or these Rules and Regulations.

Obtaining Authorization to Use the District Network

Authorized Users

Authorized users of the network include students, teachers, administrators, other employees of the District, and Board of Education members whose network privileges are not suspended or revoked.

Students

Students must submit properly signed copies of the Student's Authorization for Telecommunication Network Access (6:235-F1, the "Student Authorization") and the Parental Authorization for Student's Telecommunication Network Access (6:235-F2, the "Parental Authorization") before being permitted to access the network. Copies of these authorizations shall be kept at the school that the student attends.

Unless a student's network privileges have been suspended or revoked, the student and parental authorizations will be valid so long as the student attends the school that the student was attending when the authorizations were first submitted. If a student's network privileges are suspended or revoked, newly-signed copies of the Student and Parental Authorizations must be submitted before the student's access privileges are restored. Newly-signed Student and Parental Authorizations must also be submitted each time the student enters into a new District school.

Any violation of the terms of these authorizations, of the Policy, of these Rules and Regulations, or of additional rules, regulations, or other terms and conditions of network access promulgated by the Superintendent or Building Principals may result in the suspension or revocation of network privileges, disciplinary action, and/or appropriate legal action.

Teachers and Other Non-Students

Teachers and all other non-student users must submit a signed copy of the Teacher and Non-Student Authorization for Telecommunication Network Access (6:235-F3, the "Non-Student Authorization") before being permitted to access the network.

Unless a teacher's or other non-student's network privileges have been suspended or revoked, this authorization will be valid so long as the user remains an employee of the District or a member of the Board of Education. If a teacher's or other non-student's network privileges are suspended or revoked, the user must submit a newly-signed Non-Student Authorization before the user's access privileges are restored.

Any violation of the terms of this authorization, of the Policy, of these Rules and Regulations, or of additional rules, regulations, or other terms or conditions of network access promulgated by the Superintendent or Building Principals will result in the suspension or revocation of network privileges, disciplinary action, and/or appropriate legal action.

Use of Computer Network

Acceptable Use

Access to the District network must be for bona fide educational or research purposes consistent with the District's educational mission and/or for legitimate business reasons. Access also must comply with the Policy, these Rules and Regulations, other rules, regulations or other terms or conditions of network access promulgated by the Superintendent or Building Principals, and all other disciplinary policies and regulations necessary for the safety and pedagogical concerns of the District.

Unacceptable Use

Any use which disrupts the proper and orderly operation and discipline of schools in the District; threatens the integrity or efficient operation of the District network; violates the rights of others; is socially inappropriate or inappropriate for a student's age or maturity level; is primarily intended as an immediate solicitation of funds; is illegal or for illegal purposes of any kind; or constitutes gross disobedience or misconduct is an unacceptable use. Use of the District network for any unacceptable use may result in the suspension or revocation of network privileges, disciplinary action, and/or appropriate legal action. The final decision regarding any inappropriate use will be made by the Superintendent in consultation with the network administrator.

Unacceptable uses of the District's network specifically include, but are not limited to, the following:

1. Taking any steps which threaten, or which may reasonably be interpreted to threaten, any person, group of persons, building, or property with harm, regardless of whether the user intends to carry out such threat;
2. Taking any steps which may be considered bullying or harassment, whether in person or online, of another person or group of persons, regardless of the users intent;
3. Compromising the privacy or safety of other individuals by disclosing personal addresses, telephone numbers, or other personal identifying information;
4. Use of District networks for social media e.g, Facebook, Twitter, LinkedIn, except for educational or business related purposes;
5. Accessing, using or possessing any material in a manner that constitutes or furthers fraud (including academic fraud), libel, slander, plagiarism, forgery, or a violation of copyright or other intellectual property right;
6. Using the network for commercial, private, or personal financial gain, including gambling;
7. Deliberately accessing, creating, displaying, transmitting, or otherwise possessing or disseminating material which contains pornography, obscenity, or sexually explicit, pervasively lewd and vulgar, or indecent or inappropriate language, text, sounds, or visual depictions;

8. Creating or forwarding chain letters, "spam," or other similar unsolicited types of communication;
9. Creating or sending e-mail or other communications which purport to come from another individual (commonly known as "spoofing"), or otherwise assuming an anonymous or false identity in communicating with other individuals, businesses, or organizations;
10. Modifying, disabling, compromising, or otherwise circumventing any anti-virus, user authentication, or other security feature maintained on the District network or on any external telecommunication device, telecommunication system, or telecommunication account;
11. Using or accessing another user's network account or password, with or without consent from that user;
12. Disclosing any network password (including your own) to any other individual;
13. Downloading or installing non-work related text files, images, or other files or software to the District's devices without prior permission from the Superintendent, Building Principal, or their designees;
14. Creating or deliberately downloading, uploading, or forwarding any computer virus, or otherwise attempting to modify, destroy, or corrupt computer files maintained by any individual on any computer;
15. Participating in, or subscribing to, any mailing list, newsgroup, chat service, electronic bulletin board, or other association or service that is not work-related and that would cause a large number of emails or other electronic messages to be sent to the District's network or digital devices;
16. Using encryption software or otherwise encoding or password-protecting any file which is created with, sent to, received by, or stored on the District's network;
17. Wastefully using resources, such as file space;
18. Hacking or gaining unauthorized access to files, resources, or entities;
19. Posting anonymous messages;
20. Attempting to commit any action that would constitute an unacceptable use if accomplished successfully.

Student Use of the Internet and Internet Safety

The District's primary concern in maintaining Internet access is that student safety and security not be compromised at any time. Some of the most effective safety measures can only be implemented by students themselves. The District encourages parents and guardians to discuss the following safety concerns with their students:

1. Students should not give out such personal information as their name, age, home address, telephone number(s), photograph, their parents' or guardians' work address or telephone number, or the name or location of the school over the Internet or through email. Students should not give out such personal information about other individuals over the Internet or

through email.

2. Students should immediately inform their parents, guardians, or a member of District staff if they come across any information on the Internet or in an email that makes them feel uncomfortable. Students should not respond to any e-mail or other message that makes them feel uncomfortable.
3. Students should never agree to meet someone in person whom they have “met” online without parental knowledge, permission, and supervision.
4. Students should never agree to send or accept any item to or from a person whom they have “met” online without parental knowledge, permission, and supervision.

Publication of Student Name, Photograph, and Work on a District Website

Pictures of CCSD89 students and exemplary work, accompanied by a student’s first name and last initial, may be published on District and school websites, unless a parent withholds consent by signing form 6:235-F4.

Downloads

Users may only download non-work related text files, images, or other files or software obtained through the Internet, e-mail, file transfer protocol (ftp), or other means of file-sharing with the permission of the Superintendent, Building Principal, or their designees. Users must scan all such files with virus detection software before installing, executing, or copying such files onto a District computer.

Privacy

Any electronic communications or files created on, stored on, or sent to, from, or via the network are the property of the District. Consequently, users do not have any expectation of privacy with respect to such messages and files. Users should remember that such messages and files can be recovered from the network’s back-up system even after they have been deleted from a user’s individual account.

The Superintendent, Building Principals, and/or their designees may access and review such messages and files when necessary to maintain the integrity and efficient operation of the network; to monitor compliance with the Policy, these Rules and Regulations, and all other rules, regulations, or other terms or conditions of network access promulgated by the Superintendent or Building Principals, and to further all other educational, safety and pedagogical concerns of the District. The District also reserves the right to intercept, access, and disclose to appropriate authorities all information created with, sent to, received by, or stored on the network at any time, with or without user notice. Use of the District’s network to create, store, send, receive, view, or access any electronic communication or other file constitutes consent by the user for the District to access and review such files consistent with this paragraph.

Technology Protection Measures

Consistent with the District’s legitimate educational and pedagogical concerns, the District shall implement technology protection measures, which include filtering and/or blocking software, on every District telecommunication device that has access to the Internet. Such technology protection measures shall be implemented in the best manner practicable to prevent access to any material, including visual depictions, which is obscene; which constitutes pornography, including child pornography; or which, with respect to use of computers or other telecommunication devices by minors, would be harmful to or inappropriate for minors. The Superintendent, Building Principals, or their designees may disable the technology protection measure on an individual telecommunication

device during use by non-student adults to enable access to material needed for bona fide research or other lawful purposes.

The District shall monitor the use of the computer network by students and any other minor users in order to ensure compliance with the Policy, these Rules and Regulations, other rules, regulations or other terms or conditions of network access promulgated the Superintendent or Building Principals, and other disciplinary policies and regulations necessary to further the educational, safety, and pedagogical concerns of the District.

Security

The security and integrity of the District's network is a high priority. Users are to keep their account and password secure and confidential at all times. If a user believes at any time that he or she has identified a security gap, weakness, or breach, on the District's network or on the Internet, the user must notify a District staff member immediately. The user may not exploit the gap, weakness, or breach, and the user may not inform any other individuals of it, unless the user is informing a District staff member for the purpose of curing the security gap, weakness, or breach. Any user who violates this security policy may be subject to a suspension or revocation of network privileges, disciplinary action, and/or appropriate legal action.

No Warranties

- A. The District makes no warranties of any kind, whether express or implied, for the service of providing network access to its users, and bears no responsibility for the accuracy or quality of information or services obtained from the network or any loss of data suffered in connection with use of the network. The District will not be responsible for any damages any user suffers, including loss of data resulting from delays, non-deliveries, missed deliveries, or service interruptions caused by users' errors, omissions, or negligence. Use of any information obtained from the network is at the user's own risk. The District specifically denies any responsibility for the accuracy or quality of information obtained through the network.
- B. The District assumes no responsibility for any unauthorized charges or fees, including telephone charges, long-distance charges, per-minute surcharges, and/or equipment or line costs, relating to, or arising out of, an individual user's use of the network.
- C. The District has acted in good faith and in a reasonable manner in selecting and implementing filtering software, blocking software, and other technology protection measures to prevent access to material which is obscene, pornographic, or, with respect to use of computers or other telecommunication devices by minors, harmful to, or inappropriate for minors. Nevertheless, by using the District's network, users acknowledge that such technology measures do not prevent access to all prohibited material, and may prevent access to non-prohibited material. The District assumes no responsibility for access gained or denied by the technology protection measures that have been implemented.

Indemnification

The user agrees to indemnify the District for any losses, costs, damages, charges or fees, including, but not limited to, telephone charges, long-distance charges, per-minute surcharges, equipment or line costs, or attorney fees, incurred by the District and relating to, or arising out of the user's use of the District's network or any violation by the user of the Policy, these Rules and Regulations, or other rules, regulations or other terms or conditions of network access promulgated by the Superintendent or Building Principals.

Cooperation with Investigations

The District reserves the right to participate and cooperate fully in any investigation requested or undertaken by either law enforcement authorities or a party alleging to have been harmed by the use of the District network. Evidence of illegal activity may be reported or turned over to appropriate authorities.

Enforcement

The failure of any user to abide by the Policy, these Rules and Regulations, or other rules, regulations or other terms or conditions of network access promulgated by the Superintendent or Building Principals, may result in the suspension or revocation of the user's network privileges, disciplinary action, and/or appropriate legal action. Network privileges may be suspended or revoked by the Superintendent or Building Principal. Disciplinary measures, if any, will be considered and imposed consistent with District discipline policies.

Policy Modifications

The Board of Education may modify the terms and conditions of use and/or the provisions of the Policy and these implementing Rules and Regulations at any time. The Superintendent or Building Principals may also promulgate additional rules, regulations, or other terms or conditions of network access as may be necessary to ensure the safe, proper, and efficient operation of the network and the individual District schools. Notice of any such modifications or additional rules, regulations, or other terms of conditions of access shall be promptly communicated to all authorized users, including by posting such modifications on the network or in a conspicuous place at access locations. Use of the network constitutes acceptance of the terms of the Policy, these Rules and Regulations, and any additional rules, regulations, or other terms or conditions of network access that may have been promulgated by the Superintendent, Building Principals, or their designees.

CROSS REF: Policy 6:235 and Forms 6:235-F1 to F4

LEGAL REF: Children's Internet Protection Act, 47 U.S.C. §254(h) and (l).
Enhances Education Through Technology, 20 U.S.C. §6751 et seq.
720 ILCS 5/11 et seq.

REGULATION

Adopted: 8/17/98
Revised: 12/17/01, 3/20/06, 6/18/07, 5/18/09, 7/21/14, 6/15/15, 12/14/2020
Reviewed: 11/14/11, 11/17/14, 12/18/17, 5/14/18, 5/20/19, 6/21/2021



Board of Education, Glen Ellyn, Illinois