RESPONSIBLE COMPUTER, NETWORK & INTERNET USE

CODE D-3
(Formerly G-11)
(Mandatory)

Purpose

The Leland and Gray Union Middle and High School District recognizes that information technology (IT) is integral to learning and educating today's children for success in the global community and fully supports the access of these electronic resources by students and staff. The purpose of this policy is to:

1. Create an environment that fosters the use of information technology in a manner that supports and enriches the curriculum, provides opportunities for collaboration, and enhances staff professional development.

2. Ensure the district takes appropriate measures to maintain the safety of everyone that accesses the district's information technology devices, network and web resources.

3. Comply with the requirements of applicable federal and state laws that regulate the provision of access to the Internet and other electronic resources by school districts.

Policy

It is the policy of the Leland and Gray Union Middle and High School District to provide students and staff access to a multitude of information technology (IT) resources including the Internet. These resources provide opportunities to enhance learning and improve communication within our community and with the global community beyond. However, with the privilege of access comes the responsibility of students, teachers, staff and the public to exercise responsible use of these resources. The use by students, staff or others of district IT resources is a privilege, not a right.

The same rules and expectations govern student use of IT resources as apply to other student conduct and communications, including but not limited to the district's harassment and bullying policies.

The district's computer and network resources are the property of the district. Users shall have no expectation of privacy in anything they create, store, send, receive, or display on or over the district's computers or network resources, including personal files and electronic communications.

The superintendent is responsible for establishing procedures governing use of IT resources consistent with the provisions of this policy. All Leland and Gray employees will sign the agreement form that lists the stipulations of this policy, **D-3 RESPONSIBLE COMPUTER, NETWORK & INTERNET USE.**

These procedures must include:

1. An annual process for educating students about responsible digital citizenship. As defined in this policy, a responsible digital citizen is one who:

    - **Respects One's Self.** Users will maintain appropriate standards of language and behavior when sharing information and images on social networking websites and elsewhere online. Users refrain from distributing personally identifiable information[1] about themselves and others.
    - **Respects Others.** Users refrain from using technologies to bully, tease or harass other people. Users will report incidents of cyber bullying and harassment in accordance with the district's policies on bullying and harassment. Users will also refrain from using another person's system account or password or from presenting themselves as another person.
    - **Protects One's Self and Others.** Users protect themselves and others by reporting abuse and not forwarding inappropriate materials and communications. They are responsible at all times for the proper use of their account by not sharing their system account password.
    - **Respects Intellectual Property.** Users suitably cite any and all use of websites, books, media, etc.
    - **Protects Intellectual Property.** Users request to use the software and media others produce.

2. Provisions necessary to ensure that Internet service providers and other contractors comply with applicable restrictions on the collection and disclosure of student data and any other confidential information stored in district electronic resources.

3. Technology protection measures that provide for the monitoring and filtering of online activities by all users of district IT, including measures that protect against access to content that is obscene, child pornography, or harmful to minors.[2]

4. Methods to address the following:[3]

    - Control of access by minors to sites on the Internet that include inappropriate content, such as content that is:

[1] For the purposes of this policy, "personally identifiable information" shall not include any information listed as "directory information" in the school district's annual FERPA notice.
[2] Required by Children's Internet Protection Act (CIPA), 47 U.S.C. § 254(1); 47 C.F.R. § 54.520(c)(ii)
[3] Required by Children's Internet Protection Act (CIPA), 47 U.S.C. § 254(1); 47 C.F.R. § 54.520(c)(ii)

- ✓ Lewd, vulgar, or profane
- ✓ Threatening
- ✓ Harassing or discriminatory
- ✓ Bullying
- ✓ Terroristic
- ✓ Obscene or pornographic

- The safety and security of minors when using electronic mail, social media sites, and other forms of direct electronic communications.
- Prevention of unauthorized online access by minors, including "hacking" and other unlawful activities.
- Unauthorized disclosure, use, dissemination of personal information regarding minors.
- Restriction of minors' access to materials harmful to them.

5. A process whereby authorized persons may temporarily disable the district's Internet filtering measures during use by an adult to enable access for bona fide research or other lawful purpose.[4]

Policy Application

This policy applies to anyone who accesses the district's network, collaboration and communication tools, and/or information systems or services.

Limitation/Disclaimer of Liability

The District is not liable for unacceptable use or violations of copyright restrictions or other laws, user mistakes or negligence, and costs incurred by users. The District is not responsible for ensuring the accuracy, age appropriateness, or usability of any information found on the District's electronic resources network including the Internet. The District is not responsible for any damage experienced, including, but not limited to, loss of data or interruptions of service. The District is not responsible for the accuracy or quality of information obtained through or stored on the electronic resources system including the Internet, or for financial obligations arising through their unauthorized use.

Enforcement

The district reserves the right to revoke access privileges and/or administer appropriate disciplinary action for misuse of its IT resources. In the event there is an allegation that a user has violated this policy, a student will be provided with notice and opportunity to be heard in the manner set forth in the student disciplinary policy.

Allegations of staff member violations of this policy will be processed in accord with contractual agreements and legal requirements.

[4] Required by 20 U.S.C. § 6777(c)

Date Warned:
12-8-2015
Date Adopted:
1-26-2016
Legal Reference(s):

17 U.S.C. §§101-120 (Federal Copyright Act of 1976 as amended)
20 U.S.C. § 6777 et seq. (Enhancing Education Through Technology Act)
18 U.S.C. §2251 (Federal Child Pornography Law—Sexual Exploitation and Other Abuse of Children)
47 U.S.C. §254 (Children's Internet Protection Act)
47 CFR §54.520 (CIPA Certifications)
13 V.S.A. §§2802 et seq. (Obscenity, minors)
13 V.S.A. § 1027 (Disturbing Peace by Use of…Electronic Means)
13 V.S.A. §2605(Voyeurism)

Cross Reference:

Student Conduct and Discipline (F1)
Copyrights (G2)
Selection of Instructional Materials (G5)
Complaints About Instructional Materials (G6)

D3-P: Procedure: RESPONSIBLE COMPUTER, NETWORK & INTERNET USE

All employees are given the responsibility for using technology owned by the school districts in the form of access to electronic resources, computer hardware and software, technology, and the Internet. Employees must agree to the terms of the Acceptable Use Procedures Agreement below.

Acceptable Use Agreement

I understand that:

1. The districts extend no rights of privacy or ownership to work completed by me on district-owned technology.

2. I understand that I am responsible for appropriate use of my school-provided email account and Internet use.

3. I may not exhibit or divulge the contents of any record, file, or information to any person unless it is necessary for the completion of my job responsibilities. I will not distribute any information about any student's records or files to persons outside the school system, unless such distribution is authorized by law or there is written permission from the parent/guardian or student to do so.

4. I will not enter, change, delete or add any data to any information system or files outside of the scope of my job responsibilities. This includes recording or reporting false, inaccurate, or misleading information

5. I will report immediately to my supervisor any violation of confidentiality of data, records, or files.

6. I will not use the district's software, services, applications or technology for my personal gain or profit or for any commercial use not sanctioned by the school district.

7. I will adhere to the district's licensing agreements.

8. My username and password are to be kept confidential and must not be shared with anyone without approval from the principal or superintendent. It is my responsibility to change passwords if I suspect that someone may have obtained access to it.

9. I understand that I may bring my own personal computing device provided that the device imposes no tangible cost to the district; the device does not unduly burden the district's computer or network resources; the device has no adverse effect on an employee's job performance; the district is not responsible for damage to or loss of the device.

10. I understand that, when using digital communication platforms other than those

provided by the district, platforms such as Facebook, Twitter, Snapchat, etc., all the above rules apply. I understand that I am always expected to follow the expectations of online communication as outlined in the district's faculty/staff handbook.

11. I understand the examples outlined below of inappropriate uses of electronic records and network access:

- Accessing or reviewing a student's record for a reason other than specifically related to a work task.
- Releasing confidential student information to any person or organization that does not have a legitimate educational purpose, without the parent's written authorization, or if over 18 years old, the student's written authorization.
- Leaving reports or computer screens containing confidential student information unattended or in view of others who do not have a legitimate educational interest in the data.
- Failing to shred or destroy documents with protected information when no longer needed.
- Using student information for personal business.
- Failing to lock the computer when unattended while logged in.

12. I understand that the consequences of a violation of the above requirements may result in disciplinary action up to and including loss of privileges and termination of employment.

My signature on this document indicates that I have received and understand the school district's policy and regulations and that I agree to abide by their terms.

Name (Print): _____ Position: _____

Signature: _____ Date: _____