Employee Responsible Use of Technology

Purpose

The purpose of the District's Responsible Use policy is to educate employees about digital citizenship in the Dubuque Community School District.

Employees shall ensure technology is used in a responsible, efficient, ethical, safe, and legal manner, and that such use is in support of the district's education and business objectives. As used in this policy, "employee(s)" include all employees, coaches, directors, managers, officers, supervisors, and volunteers of the District.

The policy is meant to educate employees on how to prevent unauthorized access and other unlawful activities by users online, prevent unauthorized disclosure of or access to sensitive information, and to comply with legislation including, but not limited to, the Children's Internet Protection Act (CIPA), Children's Online Privacy Protection Act (COPPA) and Family Educational Rights and Privacy Act (FERPA). Furthermore, the policy clarifies the educational purpose of District technology.

As used in this policy, "user(s)" includes anyone using computers, Internet, email, and all other forms of electronic communication or equipment provided by the District (the "network") regardless of the physical location of the user. The policy applies even when District-provided equipment (laptops, tablets, etc.) is used off District property. Additionally, the policy applies when non-District devices access the District network or their own private network on District property.

The District uses technology protection measures to block or filter access over the network, as much as reasonably possible, to visual and written depictions that are obscene, pornographic, or harmful to minors. The District can and will monitor users' online activities and access, review, copy, and store or delete any communications or files and disclose them to others as it deems necessary. Users should have no expectation of privacy regarding their use of District equipment, network, and/or Internet access or files, including email in accordance with Freedom of Information Act (FOIA) and Federal Rules of Civil Procedure (FRCP). All information on the District's computer system is considered a public record. Whether there is an exception to keep some narrow, specific content within the information confidential is determined on a case by case basis.

As social media use continues to grow, social media awareness and education is crucial to effectively navigating and productively participating in such online spaces. Participating online with an audience beyond the classroom provides an opportunity to engage with others and experience diverse perspectives. Teaching students to be critical consumers and creators of online material will help them be better positioned for college and career success. Students need guidance on how to responsibly and productively participate online to begin establishing a positive digital footprint. Social media is comprised of online platforms where users engage one another and share information and ideas through text, video, or pictures. To be responsible social media users, students and staff will understand the different types of social media available and ways to engage in safe and productive ways online. Staff are encouraged to use professional and ethical judgement when friending or following students on social media. If staff require the need to communicate with students via social media, it is recommended that they use professional accounts or universal platforms.

Online Learning Platforms - It is important to embrace technology that can foster a creative, interactive learning environment for students, and facilitate employee professional learning and collaboration. The use of online platforms to host remote interaction between students and employees and to facilitate learning is encouraged in the district.

While student and employee instruction and communication using virtual and online platforms provides a wide array of learning opportunities, it is imperative that employees and students recognize that the use of such platforms is a privilege. Training related to the use of online learning platforms will be provided to employees and students.

The district shall carefully safeguard the right of students and employees to learn and teach in a respectful environment, regardless of the method. All instruction and communication through online learning platforms should be appropriate to the age and ability of the participants. Students and employees should be aware that online platforms may be monitored by the district. Verbal and written communication occurring on these platforms may be recorded and stored by the district in accordance with applicable laws.

Any verbal or written communication that is deemed to be inappropriate on these platforms will subject the student and/or employee to the same disciplinary measures that would exist if the interaction took place through traditional in-person learning. Students and employees who have concerns about the proper use of these platforms are encouraged to speak with their teachers or school principal.

The District will take all necessary measures to secure the network against potential cyber security threats. This may include blocking access to District applications, including, but not limited to, email, data management and reporting tools, and other web applications.

Employee Responsibility to Adhere and Promote Positive Digital Citizenship

Employees who are supervising students using technology should be vigilant in order to ensure students are meeting the provisions outlined in the Student Responsible Use policy (5504). All staff are required to report known violations to the site administrator or other authority.

Digital Citizenship

- Employees are responsible for modeling and actively practicing positive digital citizenship.
- Employees using classroom technology are explicitly required to teach students about positive digital citizenship.
- What employees do and post online must not disrupt school activities or compromise school safety and security.
- Accepting invitations to non-school related social networking sites from currently enrolled students is discouraged. Employees should use professional judgement when communicating with students outside of the school environment and should immediately notify a supervisor if communication with a student demonstrates illegal, unethical or unsafe behaviors.

Privacy

- Employees should not share personal information about students and employees including, but not limited to, names, home addresses, birth dates, telephone numbers, student ID numbers, employee numbers, and visuals without consent obtained from the other party.
- Employees should not share protected student information outside of District systems that are secure and password protected.
- Employees should be aware of privacy settings on websites they visit.
- Employees are expected to abide by all laws, this Responsible Use Policy, and all District policies.

Account User Credentials (i.e., Username and Password)

- Under no circumstances should employee account user credentials be shared with others, including other District staff and students.
- Employees should log out of unattended equipment and accounts in order to maintain privacy and security.

  IMPORTANT: Account user credentials are personal to each employee. The District has no need for employee credentials, and the District will NEVER ask employees to provide credentials or other personal information through any electronic message, notice or solicitation; therefore, any such request will almost certainly be fraudulent.

  Equally, employees should NEVER provide account user credentials in response to any internal or external communication, such as electronic messaging (email) with included attachments or hyperlinks (URLs) redirecting you to websites or unsolicited phone calls and/or text messages.

  Credentials give employees access as part of employment to various DCSD systems and to data stored within those systems. If employees divulge credentials to others, they will have the same access that employees have, and personal information, including personal identity and payroll and bank account information, will be at risk. District systems and information will be at risk. The person or persons to whom employees have given credentials will probably use them very quickly. The potential for serious damage to employee personal interests and the interests of the District is great, and employees may be responsible for resulting damage.

  If employees share or divulge credentials, the District and the School Board will not be responsible for any resulting loss or expense (financial or non-financial) employees may suffer, and the District may seek to recover from the employee any loss or expense it sustains.

Professional Conduct

Employees must:

- Use professional language in all work-related communications including email, social media posts, audio recordings, conferencing, and artistic works.
- Keep personal social network accounts separate from work-related accounts.
- Never share confidential or privileged information about students or personnel (e.g., grades, attendance records, or other pupil/personnel record information).
- Be responsible for the information they post, share, or respond to online.
- Identify themselves as school employees; steps should be taken to ensure that the user's profile and related content are consistent with how professionals should present themselves to colleagues, parents, and students.
- Not use the District's logo or make representations that their personal social media sites speak in an official District capacity.

Cyberbullying

- Bullying in any form, including cyberbullying, is unacceptable both on and off the District's premises. Posting inappropriate threatening, harassing, racist, biased, derogatory, disparaging and/or bullying comments toward or about any student, employee, or associated person on any website is prohibited and may be subject to discipline.
- Employees must report all cases of bullying to the site administrator or other authority.

Inappropriate Material

Employees must:

- Not seek out, display, or circulate material that is hate speech, sexually explicit, or violent while at school or while identified as a District employee. Exceptions may be made in an appropriate educational context.
- Not use the District network for illegal, political, or commercial purposes.
- Not transmit electronic content that is unrelated to District business and disruptive to the District network.

Security

Employees must:

- Be responsible for respecting and maintaining the security of District electronic resources and networks.
- Not use the District network or equipment to obtain unauthorized information, attempt to access information protected by privacy laws, or impersonate other users.
- Not try to bypass security settings and filters, including through the use of proxy servers.
- Not install or use illegal software or files, including unauthorized software or apps, on any District computers, tablets, smartphones, or new technologies
- Not engage in acts of vandalism, mischief, tampering, theft and other criminal acts through the use of Network/Internet or other electronic communication services and/or the data infrastructure hardware and wiring used to access these services.

Equipment and Network Safety

Employees must:

- Take all reasonable precautions when handling District equipment.
- Use caution when downloading files or opening emails as attachments. Doing so could contain viruses or malware.
- Report vandalism in any form to the appropriate administrator and/or technical personnel.

Copyright

Employees must:

- Respect intellectual property. (http://www.copyright.gov/fls/fl102.html)
- Follow all copyright guidelines (http://copyright.gov/title17/) when using the work of others.
- Not download illegally obtained music, software, apps, and other works.

Employees must abide by all laws, this Responsible Use policy and all other District policies.

Consequences for Irresponsible Use

Misuse of District devices and networks may result in restricted access or account cancellation. Failure to uphold the responsibilities listed above is misuse. Such misuse may also lead to disciplinary and/or legal action against employees, including personnel action (suspension or termination) and/or criminal prosecution by government authorities. The District will attempt to tailor any disciplinary action to the specific issues related to each violation.

Disclaimer

The District makes no guarantees about the quality of the services provided and is not liable for any claims, losses, damages, costs, or other obligations arising from use of the network or District accounts. Users are responsible for any charges incurred while using District devices and/or the network. The District also denies any liability for the accuracy or quality of the information obtained through user access. Any statement accessible online is understood to be the author's individual point of view and not that of the District, its affiliates, or employees.

Summary

All users are responsible for practicing positive digital citizenship. Positive digital citizenship includes appropriate behavior and contributions on websites, social media, discussion boards, media sharing sites and all other electronic communications, including new technology. It is important to be honest in all digital communications without disclosing sensitive personal information. What District community members do and post online, both in school and out of school time, must not disrupt school activities or otherwise compromise individual and school community safety and security.

This Responsible Use policy applies to all employees in the employment of the Dubuque Community School District. Additionally, all existing policies and behavior guidelines that cover employee conduct on the school premises and at school-related activities similarly apply to an online environment.

Adopted: April 19, 1999
Revised: August 14, 2017/September 18, 2017
Revised: January 13, 2020
Revised: October 12, 2020