## Employee Responsible Use of Technology

**Purpose**

The purpose of the District's Responsible Use Policy (RUP) is to educate employees about digital citizenship.

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 RUP 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 RUP 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 RUP applies even when District-provided equipment (laptops, tablets, etc.) is used off District property. Additionally, the RUP 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, as much as reasonably possible, to visual and written depictions that are obscene, pornographic, or harmful to minors over the network. 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 used 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.

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**

*If you are supervising students using technology, 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 District systems that are secure and password protected.
- Employees should be aware of privacy settings on websites they visit.
- Employees agree to abide by all laws, this Responsible Use Policy, and all District policies.

**Passwords**

- Under no circumstances are District passwords to 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.

**Professional Conduct**

- 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).
- Are responsible for the information they post, share, or respond to online.
- If an employee identifies him or herself as a school employee, 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.

- Employees should 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 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**

- Do 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.
- The use of the District network for illegal, political, or commercial purposes is strictly forbidden.
- Transmitting electronic content that is unrelated to District business and disruptive to the District network is prohibited.

**Security**

- All users are responsible for respecting and maintaining the security of District electronic resources and networks.
- Do not use the District network or equipment to obtain unauthorized information, attempt to access information protected by privacy laws, or impersonate other users.
- Do not try to bypass security settings and filters, including through the use of proxy servers.
- Do not install or use illegal software or files, including unauthorized software or apps, on any District computers, tablets, smartphones, or new technologies
- Do 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**

- Take all reasonable precautions when handling District equipment.
- Use caution when downloading files or opening emails as attachments could contain viruses or malware.
- Vandalism in any form is prohibited and must be reported to the appropriate administrator and/or technical personnel.

**Copyright**

- While there are fair use exemptions (http://www.copyright.gov/fls/fl102.html), all users must respect intellectual property.
- Follow all copyright guidelines (http://copyright.gov/title17/) when using the work of others.
- Employees should not download illegally obtained music, software, apps, and other works.

**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 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 under employment with 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: March 10, 2014
Revised: August 14, 2017