

## **Andover USD 385 Acceptable Use Agreement**

### Purpose

USD 385 provides computer network and internet access for students and employees. The district has adopted the following Acceptable Use Guidelines to govern the conduct of those who elect to access the computer network or district Internet.

### Acceptable Use Guidelines

All users shall adhere to the following guidelines of acceptable use:

- All use of the computer network and/or Internet will be in support of educational activities.
- Users will report misuse and breaches of network security.
- Users shall not access, delete, copy, modify, nor forge other users' e-mails, files, or data.
- Users shall not use other users' passwords nor disclose their password to others.
- Users shall not pursue unauthorized access, disruptive activities, nor other actions commonly referred to as "hacking," internally or externally to the district.
- Users shall not disclose confidential information about themselves or others.
- User shall not utilize unlicensed software.
- Users shall not access or permit access to pornography, obscene depictions, or other materials harmful to minors.
- Users shall not disable or attempt to disable Internet filtering software.

### Prohibitions

Although the USD 385 reserves the right to determine what use of the district network is appropriate, the following actions are specifically prohibited:

- Transferring copyrighted materials to or from any district network without the express consent of the owner of the copyright.
- Use of the network for creation, dissemination, or viewing of defamatory, factually inaccurate, abusive, obscene, profane, sexually oriented, threatening, harassing, or other material prohibited by law or district policy.
- Dissemination of personnel or student information via the network when such information is protected by law, including the Family and Educational Rights Act or Student Data Privacy Act.
- Utilization of the network to disseminate non-work-related material.
- Utilization of the network as a means for advertising or solicitation.

### Monitoring

The school district reserves the right to monitor, without prior notice, any and all usage of the computer network and district Internet access, including, but not by way of limitation, e-mail transmissions and receptions. Any information gathered during monitoring may be copied, reviewed, and stored. All such information files shall be and remain the property of the school district, and no user shall have any expectation of privacy regarding his/her use of the computer network or the district Internet.

### Internet Safety

In compliance with the Children's Internet Protection Act (CIPA) and the Kansas Children's Internet Protection Act, the school district will implement filtering and or blocking software to restrict access to Internet sites containing child pornography, obscene depictions, or other materials harmful to minors. The school district, however, cannot and does not guarantee the effectiveness of filtering software. Any student who connects to such a site must immediately disconnect from the site and notify a teacher. An employee who accidentally connects to such a site must immediately disconnect from the site and notify a supervisor. If a user sees another user is accessing inappropriate sites, he or she should notify a teacher or supervisor immediately. The school district administration reserves the right to prohibit access to any network or Internet it deems inappropriate or harmful. The school district shall instruct students regarding appropriate online behavior including cyberbullying.

### Penalties for Improper Use

Access to the network and Internet is a privilege, not a right, and inappropriate use will result in the restriction or cancellation of the access. The school district has the right to make the determination of what constitutes inappropriate use and use as an educational tool. Inappropriate use may lead to any disciplinary and/or legal action, up to and including suspension and/or expulsion of district students and suspension and/or termination of employees. Law enforcement shall be notified of inappropriate use which may constitute a violation of Federal or state law, and such use may result in criminal prosecution.