

SAYDEL COMMUNITY SCHOOL DISTRICT

STAFF ACCEPTABLE USE OF TECHNOLOGY

Staff Acceptable Use Statement

This statement applies to all Users of technology-based resources, including but not limited to, Saydel Community School District employees and volunteers.

Use of technology-based resources within the school district, even when carried out on a privately owned computer or device that is not managed or maintained by the Saydel Community School District, is governed by this statement. It also applies to technology-based resources, owned by the district, being used off of school property.

Purpose

The purpose of this statement is to ensure a technology-based infrastructure that promotes the mission of the Saydel Community School District. In particular, this Statement aims:

- To promote the use of technology-based resources in instruction that furthers the mission of the District;
- To ensure the integrity, reliability, availability, and superior performance of all technology-based resources;
- To ensure that use of technology-based resources is consistent with the mission, goals and policies that govern use of Saydel Community School District facilities and services;
- To interpret the Saydel Board of Education's Acceptable Use Policy;
- To ensure that technology-based resources are used for their intended purposes; and
- To establish policy for addressing misuse.

Statement Sections

Appropriate Use of Technology-based Resources

A. Appropriate Use. Technology-based resources may be used only for their authorized purposes which support the mission of the Saydel Community School District. The particular purposes of any technology-based resource as well as the nature and scope of authorized, incidental personal use may vary according to the duties and responsibilities of the User.

1. Personal devices, including but not limited to, cell phones, smart phones, mp3 players, notebooks, personal electronic devices, and games may be used to enhance educational goals. The use of these devices is not appropriate when it interferes with the educational environment.

Reviewed: March 2017

Revised: March 2017

STAFF ACCEPTABLE USE OF TECHNOLOGY CONTINUED

2. District devices. The staff will seek ways to enhance educational goals and the educational environment by infusing innovative uses of technology into the curriculum.

B. Proper Authorization. Users are entitled to access only those elements of the technology-based resources that are consistent with their authorization. Internet and email access is a privilege granted to Users to carry out the mission of the District.

C. Business Use. Any personal use is not private and is subject to this statement. Personal use must be incidental, occasional and kept to a minimum. Electronic communications reflect the District's image. They should be courteous, ethical and professional. Users are expected to understand and follow proper etiquette when using technology, including email. Because the District is a public institution, Users should have no expectation of privacy.

D. Specific Prohibited Uses. The following categories of use are inappropriate and prohibited:

1. Use that impedes, interferes with, impairs, or otherwise causes harm to the activities of others.
2. Use that is inconsistent with the Saydel Community School District non-profit status. This includes the use of any district technology for commercial use, such as advertising or promoting any product or service that is not an approved district function or fundraising activity.
3. Use that suggests Saydel Community School District's endorsement of any political candidate or ballot initiative.
4. Use that harasses, threatens or bullies.
5. Use that indicates or suggests pornography.
6. Use of inappropriate language.
7. Use that damages the integrity of district or other technology-based resources. This category includes, but is not limited to, the following activities:
 - a) Attempts to defeat system security.
 - b) Unauthorized access or use.
 - c) Disguised use, using or attempting to use User names, passwords, folders, or work that belongs to others.
 - d) Modification or removal of data or equipment without specific authorization

Reviewed: March 2017

Revised: March 2017

STAFF ACCEPTABLE USE OF TECHNOLOGY CONTINUED

e) Use of unauthorized devices without specific authorization. The use of private equipment on the District's internal network must be approved in advance. The equipment will be inspected for appropriate protection from virus, spyware, malware or other programs that may damage or compromise the security of the network.

f) Use of technology that consistently uses or excessively uses network resources for non-academic uses. Examples include network feeds, weather programs and real-time conference features.

g) Use in violation of civil or criminal law at the federal, state or local level. Transmitting or receiving any material, information or software in violation of federal, state or local laws and regulations, including material protected by trade secret or copyright guidelines.

8. Personal use of internet, social networking and communication tools that conflict and/or interfere with academic time.

9. Use in violation of district contracts. All use of technology-based resources must be consistent with the District's contractual obligations, including limitations defined in software and other licensing agreements.

10. Use in violation of district policy. Use in violation of other district policies also violates this statement. Relevant district policies include, but are not limited to, those regarding sexual harassment and racial and ethnic harassment, as well as district and building policies and guidelines.

11. Use that transmits pornography, anarchy, racism, treason, or discrimination.

12. Use in violation of external data network policies. Users must observe all applicable policies of external data networks when using such networks.

E. Personal Account Responsibility. Users are responsible for maintaining the security of their own accounts and passwords. Accounts and passwords are normally assigned to single Users and are not to be shared with any other person without authorization by the applicable systems administrator.

F. Data Access. Users will only access data appropriate to their position. Confidential data will only be shared or disseminated in appropriate circumstances.

G. Use of Security Scanning Systems. By attaching privately owned personal computers or other technology-based resources to the District's network, Users consent to district use of scanning programs for security purposes on those resources while attached to the network.

Reviewed: March 2017

Revised: March 2017

STAFF ACCEPTABLE USE OF TECHNOLOGY CONTINUED

H. Warranty. The District makes no warranties of any kind, expressed or implied, for technology-based resources provided to staff. Resources such as files stored on the network may not be backed up. Any storage is provided as a convenience to the User and no assurance is made as to the integrity or reliability of that storage.

I. Network Etiquette. Users will be expected to abide by the following network etiquette:

1. The use of the school network is a privilege and may be taken away for violation of Board policy or regulations. As a User of the Internet, students may be allowed access to other networks.
2. Users will respect all copyright and license agreements.
3. Users will cite all quotes, references and sources.

Monitoring and Sanctions

A. Systems Monitoring. The District unconditionally reserves the right to monitor and examine any and all files on district computers and servers and all network and systems activity. This includes any non-district owned technology-based resources brought into the District.

B. User Access Deactivations. A district administrator may deactivate a User's privileges when necessary, whether or not the User is suspected of any violation of this statement, to preserve the integrity of facilities, User services or data, or upon termination of employment.

C. Reporting Observed Violations. If an individual has observed or otherwise is aware of a violation of this statement, but has not been harmed by the alleged violation, he or she may report any evidence to the appropriate administrator

D. Legal Liability for Unlawful Use. In addition to district disciplinary action, Users may be subject to criminal prosecution, civil liability, or both, for unlawful use of any technology-based resource.

E. Penalties. Individuals found to have violated this statement may be subject to penalties provided for in other district policies or guidelines dealing with the underlying conduct. Violators may also face specific penalties, including temporary or permanent reduction or elimination of some or all technology-based resource privileges. The appropriate penalties will be determined by the applicable administrative authority.

F. Damages. The District reserves the right to charge a User for physical damages or electronic damages incurred from purposeful introduction of viruses or other programs that have the intent of damaging or altering computer programs or files. Fees, fines or other

Reviewed: March 2017

Revised: March 2017

STAFF ACCEPTABLE USE OF TECHNOLOGY CONTINUED

charges may also be imposed as a result of misuse or damage to these technology resources by the User.

Reviewed: March 2017

Revised: March 2017