SAYDEL COMMUNITY SCHOOL DISTRICT

ACCEPTABLE USE OF TECHNOLOGY

Scope

This policy applies to all Users of technology-based resources, including but not limited to Saydel Community School District students, employees and volunteers. It applies to the use of all technology.

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 Saydel Community School District, is governed by this policy.

Policy Statement

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

- To promote the use of technology-based resources in instruction that further 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 ensure that technology-based resources are used for their intended purposes; and
- To establish policy for addressing misuse.

Policy 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.

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

Approved: May 2008

Reviewed: March 2017

Revised: March 2017

ACCEPTABLE USE OF TECHNOLOGY CONTINUED

C. Business Use. District technology is to be used primarily to carry out the mission of the District. Any personal use is not private and is subject to this policy. Personal use must be incidental, occasional and kept to a minimum. Electronic communications reflect the District's image. They should be courteous and professional. Because the District is a public institution, Users should have no expectation of privacy.

D. Specific Proscriptions on Use. 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.

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 damages the integrity of District or other technology-based resources. This category includes, but is not limited to, the following six activities:

a) Attempts to defeat system security
b) Unauthorized access or use
c) Disguised use
e) Modification or removal of data or equipment
f) Use of unauthorized devices

6. Use in violation of law. Use in violation of civil or criminal law at the federal, state or local level.

7. 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.

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

Approved: May 2008

Reviewed: March 2017

Revised: March 2017

ACCEPTABLE USE OF TECHNOLOGY CONTINUED

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

10. 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.

H. Warranty. The District makes no warranties of any kind, expressed or implied, for technology-based resources provided to students and employees. 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.

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. In addition to accessing technology-based resources the District, through the appropriate Systems Administrator, may deactivate a User's privileges when necessary, whether or not the User is suspected of any violation of this policy, to preserve the integrity of facilities, User services or data, or upon termination of employment.

Approved: May 2008

Reviewed: March 2017

Revised: March 2017

ACCEPTABLE USE OF TECHNOLOGY CONTINUED

C. Reporting Observed Violations. If an individual has observed or otherwise is aware of a violation of this policy 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 policy 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 shall 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 charges may also be imposed as a result of misuse or damage to these technology resources by the User.

Definitions
Disguised use: The act or practice of deceiving - any attempt to appear as a different User or to hide the use of any technology.
Security scanning systems: Software, hardware or both that intercept and/or interpret network traffic.

Approved: May 2008

Reviewed: March 2017

Revised: March 2017