Syosset Central School District
ACCEPTABLE USE POLICY SUMMARY

Introduction

The Syosset Central School District ("District") has adopted an Acceptable Use Policy (Policy No. 4526). This summary is not meant to replace the full Acceptable Use Policy. If you have any questions, please see the full District policy. If there is something that seems different in this summary from the full policy on Acceptable Use, follow the statements in the full policy.

Purpose

The School District's computer equipment including all telephones and data lines is provided for educational reasons and should only be used for those purposes. All of us at the District are required to follow the same basic rules in this policy if we use the District's network or equipment whether the devices we use are owned by the District or are personally owned, including wireless devices. Examples of such devices include computers, tablets, laptops, printers, software, internet access, cell phones, watches, and fax machines or any device using the District's computer network.

Use of the District's computer equipment is a privilege, not a right, and may be taken away if anyone uses it for a reason that is not academic, professional, or does not follow the District's policies on honesty, and respect for others and property included in the Code of Conduct.

The District's general Acceptable Use Policy rules are:

1. Use technology only for academic or professional purposes.
2. Be responsible and respectful (Do not use technology in any form, including but not limited to, words, sound, or pictures to say or show anything bad about another).
   Also, using technology for academic purposes that includes another should not be done without the other's permission.

These rules apply to all students, employees, parents/guardians, and visitors in the District.

Definitions
FERPA - Family Educational Rights and Privacy Act
HIPAA - Health Insurance Portability and Accountability Act
Education Law Section 2-d – The unauthorized release of personally identifiable information
Social media sites - for the purposes of this document include: websites, blogs, wikis, online forums and any other social media available to the Syosset District community

which do not fall within the District's electronic technology network (e.g., Facebook, MySpace, Twitter, LinkedIn, Instagram, SnapChat, etc.).
"Personal electronic devices" or "School District issued devices" – for the purposes of this document include, but are not limited to: personal laptops, smart phones, portable storage media, all recording devices, all Internet connected devices, and handheld devices such as Chromebooks, iPods, iPads, and include student owned and school district issued devices.

Use of the District's Computer Equipment and Network

The following groups have permission to use the District's equipment including the network: Employees, students, parents/guardians, and any other person who has been given access by the District. Those without permission to access the network or equipment may NOT do so. By using the District's equipment and network, the user agrees to the District's rights stated in the full Policy with respect to the District's computer resources, as well as the information stored in or sent by the District's computer equipment and software.

Privacy Expectations

Users of the District equipment should not think that any information they access, send, or receive is private. For example, e-mails, information in Google Drive, and even information sent and received over social media websites using the District network may be viewed by District employees who have permission to do so.

The District may at any time view or monitor any information or communication stored in or sent by its equipment. This information may be used to investigate complaints of acceptable use and may be used for disciplinary and legal purposes. This information may also be seen by others unintentionally who monitor and maintain the systems.

I. STUDENT RESPONSIBILITIES

1. Users may not invade the privacy of others, use another's work or images and claim it as their own (plagiarize). "Another" may include a student, teacher, or any electronic or any non-electronic source. Information used from the internet must be properly cited to give proper credit to its author.

2. Revealing information or gossiping (including but not only) by using e-mail, voice mail, internet instant messaging, social media sites, chat rooms (or on other types of Web pages) about confidential information belonging to the District is not permitted.

3. Users may not waste the use District's computer equipment services or prevent others from using them. Users may not access, modify or delete others' files or system settings without express permission from a staff member or other. Deliberate attempts to tamper with, circumvent filters or access, change, corrupt, or compromise the performance of the District's computer system or equipment

or to deprive users of access to or use of such is not permitted.

4. Users may not store material such as music, video games, or personal pictures on the District's computer system and/or network.

5. Students may not send broadcast e-mail or broadcast voice mail.

6. Users are responsible for both the information and possible effects of their messages on the network. For example, users may not create or send: viruses, information that reflects poorly on the School District, "chain letters", and inappropriate messages (such as those that have information that would violate the Dignity for All Students Act for bullying, harassment or discrimination).

7. Users may not change electronic communications to hide the identity of the sender or pretend to be someone else, which is illegal.

8. Users may not install, copy or use software on School District equipment unless it is legally purchased and has been approved by the District's Technology Manager or his/her designee.

9. Students are not permitted to record classroom instruction unless provided with the express permission of the teacher.

10. Digital resources downloaded or installed from the internet could damage or interfere with the District's equipment or network; therefore, users may not do so unless express permission has been received from the Technology Manager or his/her designee.

11. **Inappropriate Information –** Users may not create, have, or send pornography in any form at school, including but not only in the form of magazines, posters, videos, electronic files or other electronic materials.

12. Users may not use the District's network or equipment to create, access, download, edit, view, store, send or print information that is illegal, harassing, offensive, discriminatory, sexually explicit or graphic, pornographic, or obscene. Also, users may not use the District's network or equipment to engage in sexting or cyberbullying.

Devices

13. Personally owned or District provided devices may be used for educational purposes with the classroom teacher's approval. The School District has the right to monitor, inspect, and/or take from a student, a personal device when administration has a reasonable suspicion that someone has not followed the Acceptable Use policy.

For example, complaints about cyberbullying may give an administrator reason to take and examine a student's cell phone to investigate the complaint.

14. Personally-owned devices that are lost, stolen, or damaged are NOT covered by the District's insurance; therefore, loss or damage to such devices is NOT the District's responsibility. If lost or stolen, the loss should be reported immediately to the Information Technology Manager or his/her designee so that appropriate action can be taken to minimize any possible risk to the District and the District's computer system.

15. The District is not responsible for and will not provide technical support, troubleshooting, or repairing of electric devices owned by anyone except for the District.

16. Users may only connect to the "public" wireless network when using personal electronic devices.

17. Students who are loaned a device to use for educational purposes are responsible for the device. For example, a student provided a Chrome Book to use will be responsible for the full replacement cost of the device if it is lost, stolen, damaged, or misused.

18. Students should log-off of devices at the end of class to prevent confidential information from being viewed by others.

Security

19. Users are responsible for keeping the information on their devices secure. Computer accounts, passwords, and security codes must not be shared with others. Further, to protect personal safety, personal information should not be given out on websites, chat rooms, etc.

20. Users may not attach a server or provide server services without the express permission of the Technology Manager. Further, users may not tamper with the security controls on any system.

21. Unless approved by the Information Technology Manager or his/her designee, modem use is not allowed on computers that are directly connected to the District's network.

22. Any information online that causes discomfort should be reported to the classroom teacher.

23. If any user receives a threatening message, they should record/save the message and report the incident to the Principal.

All members of the school community are expected to follow the rules of this policy. Anyone found to have violated these rules may receive a range of consequences including loss of access privileges, disciplinary action, or legal.

II. STAFF RESPONSIBILITIES

Staff are accountable for all Student Responsibilities (in Section I) in addition to the following (in Section II).

1. When a staff member is no longer employed by the District or changes positions for which District computer property is no longer required, the property will be returned.

2. School District business conducted electronically must be done on a District account and may be subject to FOIL with no expectation of privacy.

3. Users must maintain the confidentiality of student information in compliance with all applicable federal and state laws (including FERPA, HIPAA, and Education Law, section 2-d). Devices should be locked when away to prevent unauthorized access to student information.

4. Communications must at all times be professional, ethical and meet the standards of one representing the School District.

5. Software licenses must be adhered to. No software may be installed, copied or used on District equipment without the permission of the Technology Manager or his/her designee.

6. Personal electronic devices must conform to District standards and are subject to review if there is reason to believe the device has compromised the District's computer resources. The use of such devices are subject to FOIL if used in the course of professional responsibilities.

7. The cost to purchase all personal electronic devices is the responsibility of the staff member, including services such as phone options or other "apps."

8. Staff members are responsible for the maintenance of personal electronic devices, including maintenance to conform to District standards.

9. Removing or relocating District computer resources from its location is prohibited without express permission from the Technology Manager.

10. Suspected violations of this policy should be reported to the Technology Manager.

11. Users may not include personal links and addresses, such as blogs, YouTube videos, etc., in District email unless used for District business or as part of the District's curriculum.

12. The signature portion of a user's email may not include external links or images unrelated to the content of the email.

13. Voice mailboxes may not be used for advertising or commercial purposes.

District-Issued Cell Phones

14. Cell phones issued by the District should be used for school business only.
15. There should be no expectation of privacy in the use of District-issued phones.
16. Employees will be required to reimburse the District for repair or replacement of device if stolen, lost, or damaged due to negligence.