

## **Rules Pertaining to Electronic Device Usage**

Prohibitions. Students, employees and visitors of the School District shall not:

- 1.** use any DIGITAL TECHNOLOGY<sup>1</sup> for any purpose other than for the legitimate educational purposes of our students or for purposes of advancing the legitimate business of the School District;
  - 2.** use any DIGITAL TECHNOLOGY for personal business or affairs, except as expressly provided in this policy or in administrative guidelines promulgated and adopted by the SUPERINTENDENT;
  - 3.** use any of our COMPUTERS unless and until a confidential USER ID and password has been assigned to the student or employee;
  - 4.** use any of our COMPUTERS without using his/her USER ID and password;
  - 5.** terminate use of any COMPUTERS without logging off the COMPUTER;
  - 6.** disclose his/her USER ID or password to any other individual;
  - 7.** use or utilize the USER ID and/or password belonging to or assigned to any other individual, or impersonate, in any manner, any other person;
  - 8.** open or logon to any COMPUTER, software, program or application using, utilizing or inputting the USER ID and/or PASSWORD of any other individual or entity, or use any default or preset USER ID and/or PASSWORD without express authority;
  - 9.** misrepresent his/her identity when using the School District's COMPUTERS;
  - 10.** bypass any blocking software that may be used or installed by the School District;
  - 11.** intentionally, willfully, maliciously or through reckless indifference damage or corrupt the functioning of any DIGITAL TECHNOLOGY or any data stored, either temporarily or permanently on any DIGITAL TECHNOLOGY;
  - 12.** visit or access pornographic websites;
  - 13.** violate the School District's Code of Student Conduct or any other applicable policy of the School District;
  - 14.** use any COMPUTERS unless and until the individual has signed an acknowledgment in the form prescribed by the School District attesting to the individual's understanding of the rules governing the use of DIGITAL TECHNOLOGY.
  - 15.** intentionally enter any secure or confidential area of the School District's systems, network(s) or COMPUTERS without proper authority;
  - 16.** violate any copyright laws or the ownership or license rights of any person or entity;
  - 17.** violate the legal rights of others;
  - 18.** knowingly infect any COMPUTER with any virus;
  - 19.** use any software or Internet site in violation of any applicable licensing agreement or applicable terms of use;
  - 20.** use any DIGITAL TECHNOLOGY to hack into anyone else's COMPUTERS or networks in any way or manner that is not authorized;
  - 21.** use any data mining, robots, or similar data gathering and extraction methods in violation of any person's or entity's rights;
  - 22.** use DIGITAL TECHNOLOGY to violate any applicable law, INCLUDING the Wiretap and Electronic Surveillance Control Act;
  - 23.** install any software program on or in or download any software program onto or in any COMPUTERS without the express written approval of the SUPERINTENDENT, except for the following:
    - a. Printer drivers;
-

b. Adobe® Acrobat® Reader®

24. fail to report to the School District's technology administrator any time when he/she inadvertently visits or accesses a pornographic site;
25. violate any applicable work rule when using the School District's DIGITAL TECHNOLOGY;
26. alter or change the DESTKTOP or the look or operation of any DESKTOP of any COMPUTER;
27. alter or change the screen saver, or the look or operation of any screen saver, installed by the School District;
28. delete or remove any program, application, security feature, or virus protection from any School District COMPUTER;
29. incur any charges or costs of any nature or type to the School District in connection with DIGITAL TECHNOLOGY or your use of DIGITAL TECHNOLOGY; except as specifically and expressly authorized in accordance with applicable procurement requirements established by the School District or by law, or telephone charges by an employee incurred for School District purposes and consistent with the employee's authority;
30. hack into any hardware and/or software owned or licensed by the School District for any purpose;
31. violate any applicable criminal statute pertaining to computers, property or electronic devices, INCLUDING Chapter 76 of the Crimes Code, relating to computer offenses. 18 Pa.C.S.A. §7601 *et seq.*;
32. plant any virus, pornography or other prohibited content or software on anyone's COMPUTER;
33. disconnect any COMPUTER from the network without prior explicit direction to do so;
34. disconnect any hardware from any COMPUTER (other than a printer) without prior explicit direction to do so;
35. delete any files, documents, data, material, or folders from any COMPUTER belonging to or supplied by the SCHOOL DISTRICT, in any of the following situations:
  - a. in violation of litigation hold instructions provided to the employee or student;
  - b. that the employee or student knows to be relevant to any LITIGATION in which the SCHOOL DISTRICT, any employee or official of the SCHOOL DISTRICT, or any student is involved or may be involved; and/or
  - c. when the employee or student has notice that he or she is involved in any investigation of any complaint or disciplinary matter.
36. insert any removable media into the COMPUTER for any purpose without permission; and/or
37. with respect to employees only, use a COMPUTER not belonging to the School District for School District matters. For example, notes of School District meetings, emails pertaining to work for the School District, and other documentation or data pertaining to the work of the School District must not be on a COMPUTER owned by the employee.