

- **Rule 18. Technology Offenses (Respect/ Honesty/ Citizenship)**

The school is not responsible for personal electronic devices on school property or at school sponsored events. Electronic devices may be confiscated by the school administrator or designee. See Rule 20, for specific rules relating to use of electronic equipment, including cellular phones, and other items while on the school bus.

- a. Purposely look for security problems, attempt to disrupt school technology resources, or engage in any activity that monopolizes or compromises school technology resources;
- b. Copy computer programs, software or other technology provided by the District for personal use; download unauthorized files; or use school technology resources for personal gain or private business enterprises;
- c. Attempt to, threaten to, or actually damage, destroy, vandalize, or steal private property or school property while using school technology resources on or off school grounds (The local school police officer must be notified of such incidents.);
- d. Use or participate in using personal or school technology resources to distribute or display inappropriate material. Inappropriate material does not serve an instructional or educational purpose and includes but is not limited to the following (See Rule 6b for bullying using technology):
  - Is profane, vulgar, lewd, obscene, offensive, indecent, sexually explicit, pornographic or threatening;
  - Advocates illegal or dangerous acts;
  - Causes disruption to Fulton County School District, its employees or students;
  - Advocates violence;
  - Contains knowingly false, recklessly false, or defamatory information; or
  - Is otherwise harmful to minors as defined by the Children’s Internet Protection Act. (The local school police officer must be notified of such incidents.)

Use of recording devices to record misbehaviors or to violate the privacy of others may also result in a violation of Rule 22.

- e. Refusing to comply with reasonable directions or commands of school staff regarding responsible use of technology, and/or use audio or visual recording devices without permission of a school administrator (including but not limited to Policy and Operating Guideline IFBGA Responsible Use of Enterprise Technology).
- f. Gain or attempt to gain unauthorized access to the District's computer data, network, system, Internet connections, e-mail accounts, or intranet or to any third party's computer system, data, or network, such as:
  - Malicious tampering, phishing, or hacking activities;
  - Intentionally seeking information about passwords belonging to other users;
  - Disclosing a user's password to the District's computer network, system, Internet connections, e-mail accounts, or intranet to other individuals. Students, however, may share their passwords with their parents.
  - Modifying passwords belonging to others;
  - Attempting to log in through another person's account;
  - Attempting to gain access to material that is blocked or filtered by the District;
  - Accessing, copying, or modifying another user's files without authorization;
  - Disguising a user's identity;
  - Using the password or identifier of an account that does not belong to the user; or
  - Engaging in uses that jeopardize access into others' accounts or other computer networks or systems.
- g. Violate the District's Responsible Use Agreement (Operating Guideline IFBGA) in any other way.