Based on the nature and severity of the offense and the circumstances surrounding the incident, violations of this policy will result in appropriate remedial actions or discipline up to and including long-term suspension for students and dismissal for employees, and may result in revocation of user privileges. Willful misuse may result in criminal prosecution under applicable state and federal law.

C. RULES FOR USE OF SCHOOL TECHNOLOGICAL RESOURCES

1. School technological resources are provided for School-related purposes only. Acceptable uses of such technological resources are limited to responsible, efficient, and legal activities that support learning and teaching. Use of School technological resources for commercial gain or profit is prohibited. Student personal use of School technological resources for amusement or entertainment is also prohibited unless approved for special situations by the teacher or other school administrator. Because some incidental and occasional personal use by employees is inevitable, the School permits infrequent and brief personal use by employees so long as it occurs on personal time, does not interfere with School business, and is not otherwise prohibited by University or School policy or procedure.

2. Unless authorized by law to do so, users may not make copies of software purchased by the School. Under no circumstance may software purchased by the School be copied for personal use.

3. Users must comply with all applicable laws, School and University policies, administrative regulations, and school standards and rules, including those relating to copyrights and trademarks, confidential information, and public records. Plagiarism of Internet resources will be treated in the same manner as any other incidents of plagiarism, as stated in the Code of Student Conduct and Behavior Policy.

4. Users must follow any software, application, or subscription services terms and conditions of use.

5. No user of technological resources, including a person sending or receiving electronic communications, may engage in creating, intentionally viewing, accessing, downloading, storing, printing, or transmitting images, graphics (including still or moving pictures), sound files, text files, documents, messages, or other material that is obscene, defamatory, profane, pornographic, harassing, abusive, or considered to be harmful to minors.

6. Users must not circumvent firewalls. The use of anonymous proxies to circumvent content filtering is prohibited.

7. Users may not install or use any Internet-based file sharing program designed to facilitate sharing of copyrighted material.

8. Users of technological resources may not send electronic communications fraudulently

an individual's ID or password is strongly discouraged. If an ID or password must be

E. PRIVACY

Students, employees, visitors, and other users have no expectation of privacy in anything they create, store, send, delete, receive, or display when using the School's network, devices, Internet access, email system, or other technological resources owned or issued by the School, whether the resources are used at school or elsewhere, and even if the use is for personal purposes. Users should not assume that files or communications created, transmitted, or displayed using School technological resources or stored on servers, the storage mediums of individual devices, or on School-managed cloud services will be private. Under certain circumstances, School officials may be required to disclose such electronic information to law enforcement or other third parties, for example, as a response to a document production request in a lawsuit against the School or University, in response to a public records request, or as evidence of illegal activity in a criminal investigation.

The School may, without notice, (1) monitor, track, and/or log network access, communications, and use; (2) monitor and allocate fileserver space; and (3) access, review, copy, store, delete, or disclose the content of all user files, regardless of medium, the content of electronic mailboxes issued by the School, and system outputs, such as printouts, at any time for any lawful purpose. Such purposes may include, but are not limited to, maintaining system integrity, security, or functionality, ensuring compliance with School and University policy and applicable laws and regulations, protecting the School from liability, and complying with public records requests. School personnel shall monitor online activities of individuals who access the Internet via a school-owned device.

By using the School's network, Internet access, electronic devices, email system, devices, or other technological resources, individuals consent to have that use monitored by authorized School personnel as described in this policy.

F. USE OF PERSONAL TECHNOLOGY ON SCHOOL PROPERTY

Users may not use private WiFi hotspots or other personal technology on campus to access the Internet outside the School's wireless network. Students' use of personal technology devices, including cell phones, e-readers, and tablets, is prohibited during the school day, unless an exception is made. Violations of this section will result in disciplinary action in accordance with the Student Code of Conduct. The School assumes no responsibility for personal technology devices brought to school.

Legal References: U.S. Const. amend. I; Children's Internet Protection Act, 47 U.S.C. 254(h)(5); Electronic Communications Privacy Act, 18 U.S.C. 2510-2522; Family Educational Rights and Privacy Act, 20 U.S.C. 1232g; 17 U.S.C. 101 *et seq.*; 20 U.S.C. 7131; G.S. 143-805, implemented by Section 7 of Session Law 2024-26.

Cross References: Internet Safety (policy 3226), University Policy 52

Issued: October 15, 2024