The Catamount School Policy 3225

TECHNOLOGY RESPONSIBLE USE

Policy Code: **3225**

A. PURPOSE AND POLICY STATEMENT

The Catamount School (School) provides its students and staff access to a variety of technological resources. These resources provide opportunities to enhance learning, appeal to different learning styles, improve communication within the school community and with the larger global community, and achieve the School's educational goals. Through the School's use of technological resources, users can observe events as they occur around the world, interact with others on a variety of subjects, and acquire access to current and in-depth information.

The School intends that students and employees benefit from these resources while remaining within the bounds of safe, legal, and responsible use. Accordingly, the School establishes this policy to govern student and employee use of School technological resources, which includes any technological resources owned, leased, maintained, or otherwise controlled by the School or Western Carolina University. Use of technological resources must also comply with University Policy 52, Responsible Use of Information Technology Resources, to the extent that it supplements and does not conflict with this Policy. This policy applies regardless of whether such use occurs on or off School property, and it applies to all School technological resources, including but not limited to computer networks and connections, the resources, tools, and learning environments made available by or on the networks, and all devices that connect to those networks.

B. EXPECTATIONS FOR USE OF SCHOOL TECHNOLOGICAL RESOURCES

The use of School technological resources, including access to the Internet, is expected to be exercised in an appropriate and responsible manner. Individual users of the School's technological resources are responsible for their behavior and communications when using those resources. Responsible use of School technological resources is use that is ethical, respectful, academically honest, and supportive of student learning. Each user has the responsibility to respect others in the School community and on the Internet. Users are expected to abide by the generally accepted rules of network etiquette.

General student and employee behavior standards, including those prescribed in applicable University policies, the Code of Student Conduct and Behavior Policy, and other school rules, apply to use of School technological resources, including access to the Internet.

In addition, anyone who uses School computers or electronic devices, accesses the School's electronic storage or network, or connects to the Internet using School-provided access must comply with the additional rules for responsible use listed in Section C, below. These rules are intended to clarify expectations for conduct but should not be construed as all-inclusive.

All students must be trained about appropriate online behavior as provided in policy 3226, Internet Safety.

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

(i.e., by misrepresenting the identity of the sender).

9. Users must respect the privacy of others.

    i. Students must not reveal any personally identifying, private, or confidential information about themselves or fellow students when using email, chat rooms, blogs, or other forms of electronic communication. Such information includes, for example, a person's home address or telephone number, credit or checking account information, or social security number.

    ii. School employees must not disclose on School or University websites or web pages or elsewhere on the Internet any personally identifiable, private, or confidential information concerning students (including names, addresses, or pictures) without the written permission of a parent or guardian or an eligible student, except as otherwise permitted by the Family Educational Rights and Privacy Act (FERPA).

    iii. Users may not forward or post personal communications without the author's prior consent.

    iv. Students may not use School technological resources to capture audio, video, or still pictures of other students and/or employees in which such individuals can be personally identified, nor share such media in any way, without consent of the students and/or employees and the principal or designee. An exception will be made for settings where students and staff cannot be identified beyond the context of a sports performance or other public event or when otherwise approved by the principal.

10. Users may not intentionally or negligently damage computers, computer systems, electronic devices, software, computer networks, or data of any user connected to School technological resources. Users may not knowingly or negligently transmit computer viruses or self-replicating messages or deliberately try to degrade or disrupt system performance, including by streaming audio or video for non-instructional purposes. Users may not disable antivirus programs installed on School-owned or issued devices.

11. Users may not create or introduce games, network communications programs, or any foreign program or software onto any School computer, electronic device, or network without the express permission of the principal or designee.

12. Users are prohibited from engaging in unauthorized or unlawful activities, such as "hacking" or using the computer network to gain or attempt to gain unauthorized or unlawful access to other computers, computer systems, or accounts.

13. Users are prohibited from using another individual's ID or password for any technological resource or account without permission from the individual. Sharing of

an individual's ID or password is strongly discouraged. If an ID or password must be shared for a unique classroom situation, students must have permission from the teacher or other school official.

14. Users may not read, alter, change, block, execute, or delete files or communications belonging to another user without the owner's express prior permission.

15. Employees shall not use passwords or user IDs for any data system (e.g., the state student information and instructional improvement system applications, time-keeping software, etc.) for an unauthorized or improper purpose.

16. If a user identifies or encounters an instance of unauthorized access or another security concern, he or she must immediately notify a teacher or School administrator. Users must not share the problem with other users. Any user identified as a security risk will be denied access.

17. It is the user's responsibility to back up data and other important files.

18. Employees shall make reasonable efforts to supervise students' use of the Internet during instructional time.

19. Views may be expressed on the Internet or other technological resources as representing the view of the School or part of the School only with prior approval by the Dean or designee.

20. Users who are issued School-owned and -maintained devices for home use (such as laptops, Chromebooks, etc.) must adhere to any other reasonable rules or guidelines issued by the principal for the use of such devices.

Exceptions to these rules may be made for employees whose activities are necessary to carry out their job responsibilities and are authorized by law.

D. RESTRICTED MATERIAL ON THE INTERNET

The Internet and electronic communications offer fluid environments in which students may access or be exposed to materials and information from diverse and rapidly changing sources, including some that may be harmful to students. The School recognizes that it is impossible to predict with certainty what information on the Internet students may access or obtain. Nevertheless, School personnel shall take reasonable precautions to prevent students from accessing material and information that is obscene, pornographic, or otherwise harmful to minors, including violence, nudity, or graphic language that does not serve a legitimate pedagogical purpose. The Principal shall ensure that technology protection measures are used as provided in Policy 3226, Internet Safety, and are disabled or minimized only when permitted by law and School or University policy. The School is not responsible for the content accessed by using a cellular network to connect a personal device to the Internet.

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