



Technology Acceptable Use Policy

O.C.G.A. § 20-2-324

Utopian Academy for the Arts (UAFA) recognizes that electronic media, including the Internet and electronic mail, enhance the quality and delivery of instruction in our school by providing access to unique resources and opportunities for collaborative work. Any electronic activity conducted by employees, students, or other persons via the School's network or using Utopian Academy's equipment, computer resources, hardware, or software is subject to inspection and monitoring. There should not be any expectation of privacy while on the school network or using school devices. Use of electronic systems shall be in support of and consistent with the vision, mission, and goals established by Utopian Academy for the Arts and for the purpose of instructional and administrative support. The use of electronic technology is a privilege which may be revoked at any time.

All data accessed, stored, or transmitted via the School's electronic resources shall be used in a responsible, ethical, and lawful manner. Any unauthorized use or any failure to comply with applicable law, policy, and rules relating to the use of electronic resources may result in the loss of electronic devices, network access and/or the imposition of disciplinary actions. Unauthorized use includes, but is not limited to, participation in programming vandalism or "hacking" activities; accessing, viewing transmitting, storing, or displaying of offensive materials or messages including, but not limited to, those that contain the following: sexually explicit images or information; ethnic/racial slurs; defamatory, abusive, obscene, profane, or threatening language; encouragement of the use of controlled substances; or illegal material.

At all times, students, staff, and visitors shall be strictly prohibited from using Utopian Academy's equipment, devices, hardware, software, and/or the school's network with school or personal devices to access, send, receive, view, or download obscene materials, child pornography, or material that is harmful to minors. All persons who willfully violate this prohibition will be subject to disciplinary or other punitive measures regardless of whether the violation occurred while on school property, a school bus or other school vehicle, a school related function, or elsewhere.

In accordance with state law, the School uses technology protection measures to inspect and analyze unencrypted internet traffic for malware and to block or filter electronic access to obscene materials, child pornography, or material that is harmful to minors.

Use of School Devices

Any technology, network, or device owned by the School and utilized by employees and/or students shall only be used for the express purpose for which it was intended and with respect to the school's approved security measures. This may include, but not be limited to, the use of strong passwords (including 2-step authentication), limiting approved applications and system updates, limiting permission levels for users, and the immediate reporting of damage to any device. Employees shall only utilize their own login credentials and students shall utilize only the credentials they are provided by school staff, if applicable.

At no time shall school devices be used to take or disseminate pictures, videos, or other audio or visual recording without the permission of a teacher or school staff and for educational purposes.

At all times, users shall adhere to the information security policies adopted by the School. Any employee, student, parent, or visitor who violates such policies may have their system access privileges revoked and/or may be subject to appropriate disciplinary consequences.

Complaints

An employee, student, or parent who believes this policy has been violated may file a written complaint with the Principal within 10 business days of first becoming aware of an alleged violation. The complaint shall include the name and contact information of the complainant and all pertinent information about the violation that is known, including, but not limited to (1) identity of the alleged violator; (2) the date on which the alleged violation occurred; (3) the specific activity alleged to have violated this policy; (4) the device and/or network on which the violation occurred; (5) any witnesses to the alleged violation; and (6) any other information known to the complainant about the alleged violation.

Upon receipt of a written complaint, the Principal, or his/her designee shall investigate the alleged violation and provide a written response within 15 business days. If additional time is needed to appropriately investigate and respond to the complaint, an estimate of the anticipated timeline for responding should be provided at that time.