North Andrew School District – Technology Policy

Access to computers, computer system, information networks, and to the information technology environment within the North Andrew School District system is a privilege, not a right, and must be treated as such by all students and staff. The North Andrew School District seeks to protect, encourage and enhance the legitimate uses of technology by placing fair limitations on such use and sanctions for those who abuse the privilege. All users are required to be good technology citizens by refraining from activities that annoy others, disrupt the educational experiences of their peers, or can be considered as illegal, immoral and/or unprofessional conduct. The student is ultimately responsible for his/her actions in accessing technology. Failure to comply with the guidelines of technology use may result in the loss of access privileges and/or appropriate disciplinary action.

The North Andrew School District has the right to take disciplinary action, remove computer and networking privileges, or take legal action or report to proper authorities, any activity characterized as unethical, unacceptable, or unlawful. Unacceptable use activities constitute, but are not limited to, any activity through which any user:

1. Violates such matters as institutional or third-party copyright, license agreements or other contracts. The unauthorized use of and/or copying of software is illegal.

2. Interferes with or disrupts other network users, services, or equipment. Disruptions include, but are not limited to, distribution of unsolicited advertising, propagation of computer viruses or worms, distributing quantities of information that overwhelm the system (chain letters, network games, etc.) and/or using the network to make unauthorized entry into any other resource accessible via the network.

3. Attempts to disable, bypass or otherwise circumvent the content filter that has been installed in accordance with the federal Children's Internet Protection Act. This includes but is not limited to the use of proxy servers.

4. Seeks to gain or gains unauthorized access to information resources, obtains copies of, or modifies files or other data, or gains and communicates passwords belonging to other users.

5. Uses or knowingly allows another to use any computer, computer network, computer system, program, or software to devise or execute a scheme to defraud or to obtain money, property, services, or other things of value by false pretenses, promises, or representations.

6. Destroys, alters, dismantles, disfigures, prevents rightful access to, or otherwise interferes with the integrity of computer-based information resources, whether on stand-alone or networked computers.

7. Invades the privacy of individuals or entities.

8. Uses the network for commercial or political activity or personal or private gain.

9. Installs unauthorized software or material for use on District computers. This includes, but is not limited to, downloading music, pictures, images, games, and videos from either the Internet or via portable drives.

10. Uses the network to access inappropriate materials.

11. Uses the District system to compromise its integrity (hacking software) or accesses, modifies, obtains copies of or alters restricted or confidential records or files.

12. Submits, publishes, or displays any defamatory, inaccurate, racially offensive, abusive, obscene, profane, sexually oriented, or threatening materials or messages either public or private.

13. Uses the District systems for illegal, harassing, vandalizing, inappropriate, or obscene purposes, or in support of such activities is prohibited. Illegal activities are defined as a violation of local, state, and/or federal laws. Cyber-bullying and harassment are slurs, comments, jokes, innuendos, unwelcome comments, cartoons, pranks, and/or other verbal conduct relating to an individual which: (a) has the purpose or effect of unreasonably interfering with an individual's work or school performance; (b) interferes with school operations; (c) has the purpose or effect to cause undue emotional stress or fear in an individual.

14. Vandalism is defined as any attempt to harm or destroy the operating system, application software, or data. Inappropriate use shall be defined as a violation of the purpose and goal of the network. Obscene activities shall be defined as a violation of generally accepted social standards in the community for use of a publicly owned and operated communication device.

VIOLATIONS/CONSEQUENCES

Students who violate this Policy will be subject to revocation of access up to and including permanent loss of privileges and discipline up to and including expulsion.

Violations of law will be reported to law enforcement officials.

Disciplinary action may be appealed by parents and/or students in accordance with existing procedures for suspension or revocation of student privileges.