

TECHNOLOGY AND INTERNET ACCEPTANCE USE POLICY (AUP)

Notre Dame Academy grants students the privilege of access to computers, peripherals, a local area network, the Internet, and other technology tools, all of which are owned, maintained, and controlled by NDA. The Academy expects that students will use these technology resources only in accordance with NDA's mission and only for academic purposes. The purpose of this document is to inform parents, guardians and students of the rules governing the use of personally owned computing/network devices while on and at school-sponsored functions, as well as the Academy's technology resources and remote access. Please read the following information carefully before signing the attached permission form.

Definition

Computer Resources: All networks (including any connections to external networks i.e. Internet), processors, peripherals and supplies under the administration of the Notre Dame Academy Computer Account.

Privileges

Use of Notre Dame Academy computer resources is a privilege and not a right. As with all privileges, abuses will not be tolerated. Students should not expect any privacy in their use of the Academy's technology resources. All data created, stored, received, sent, and viewed on or through such resources are subject to monitoring and access by the Academy at any time. Furthermore, NDA technology staff, in order to preserve the integrity or operational state of all computers, may find it necessary to manipulate, without prior consent, any data or files of any users that exist on any resource. Notre Dame Academy reserves the right to read and/or remove any student files on the system without prior notification to system users.

Internet Information Content

Notre Dame Academy has no control of the information on the Internet, and provides only limited technical barriers to account holders accessing the full range of information available. Sites accessible via the Internet may contain material that is illegal, defamatory, inaccurate, or potentially offensive. Access to any information on the Internet is ultimately the responsibility of the user. Deliberate access of inappropriate material will result in disciplinary action.

Respect for Others and Ethical Conduct for Users

Users should respect the rights of others using the NDA network by:

- Understanding that cyber bullying will not be tolerated.
- Always logging off workstations after finishing work.
- Not deliberately attempting to disrupt system performance or interfere with the work of other users.
- Leaving equipment and room in good condition for the next user or class.

It is the Responsibility of the User to:

- Use only her account or password. It is a violation of the NDA AUP to give access to an account to any other user, or to read, modify, or remove files owned by other users.
- Recognize and honor the intellectual property of others; comply with legal restrictions regarding plagiarism and the use and citation of information resources.
- Not to download and/or use material in violation of copyright laws or violate terms of applicable software licensing agreements or copyright laws.

- Not to knowingly run or install a program on any computer system or network that intends to damage or to place excessive load on a computer system or network, or attempt to circumvent data protection or uncover security loopholes on any computer resource within or connected to NDA.
- Not to deliberately waste computer resources, including paper or use computer resources for personal reasons that result in an expense to NDA.
- Not use computer systems for personal use during class time.
- Not transmit or view materials which explicitly or implicitly refer to sexual conduct.

Vandalism Policy

Due to the complexity and cost of technology, when a user's actions result in damage to any computer resource, all costs incurred for repair will be the responsibility of the user. This includes the transmission of malware through CDs and USB drives.

Software Installation

Only individuals assigned by NDA Information Technology staff may download or install software (demo or full versions) onto any computer resource within the Academy.

Student Social Networking Policy

When using social networking sites, virtual reality sites, email or text/picture/instant messaging systems of any kind, students must consider the impact on themselves and on other members of the community and be mindful of the Academy rules, mission and values. In particular:

- Any posting that creates, directly or indirectly, an uninviting / threatening atmosphere for any member of the NDA community, or creates an environment that is contrary to the values of NDA, will be investigated and considered a serious violation of the Academy's harassment and bullying policies no matter when or on what system it was created or transmitted.
- Anonymous postings on sites such as "formspring," Honesty Box, etc. that violate Academy norms and rules will be investigated. Such postings weaken the atmosphere of trust that is one of the Academy's beliefs and will be addressed accordingly.
- Students need to be mindful that they are always representing NDA. Students should not post anything compromising that could then be linked to the Academy.
- Students should be aware that many college admissions offices and future employers will look at applicants' social networking sites. Be aware of the consequences of your postings.
- Students may not use the name or logos of NDA for any posting without written permission from NDA and may not use the logos of copyrighted material of any other person or organization without appropriate permission.
- Current students should not send "friend" or "link" requests to faculty or staff at Notre Dame Academy. In addition, any such requests made by faculty or staff to students must be reported to the principal. Communication between faculty, staff and students should be limited to Academy sanctioned online tools.

Basic Guidelines for Safety on Social Networking Sites

- Be cautious with the personal contact information you post on social networking sites.
- "Personal contact information" includes your full name, home address, location, home phone number, cell phone number, and any other information that would allow an individual to find you.
- Sharing personal information on social networking sites can lead to unwanted and unsafe attention from individuals you do not know.
- Facebook and other sites provide numerous privacy settings for information contained in their pages. Use these settings to protect personal contact information and private information.
- Be mindful that once posted, the information becomes property of the website.

Violations of the Acceptable Use Policy

Violations of this Acceptable Use Policy will be handled in the same manner as all other disciplinary issues. All violations will be referred to the Principal. Student sanctions may include the revocation of student access to all technology resources, suspension, or expulsion.