

The Latin School of Chicago Computing and Technology Policy

Purpose

This document sets forth the policies for using the computing and technology resources at The Latin School of Chicago. The computing and technology resources are intended to promote the academic advancement of Latin's students, faculty, staff, and administration. Because all users share these resources, each user must be considerate of the rest of the community. Access to these resources is a privilege, not a right, and may be revoked at any time. This policy is subject to change as new technologies and processes emerge. Changes to this document will be posted and available on the Intranet.

Scope

Guidelines and rules contained within this document apply to all members of the Latin community (students, faculty, staff, administrators, Live & Learn, High Jump, and others alike), except where noted. Ignorance of these guidelines and rules is not an acceptable excuse for breaking or failing to follow them. Students are prohibited from using faculty, staff, or administrative office computers without specific written permission from the Information Technology department. With the permission of faculty, students may access computers in the libraries, computer labs, and Lower School classrooms, and in selected Middle and Upper School classrooms.

Privacy

Individuals using Latin's computing and network resources should have a reasonable expectation of privacy in most instances. However, Latin personnel may direct searches for specific violations of policy when there is a reasonable suspicion that computing resources have been misused, policy has been violated, or when routine maintenance and monitoring of computers and the network reveal possible violations of policy.

Server Access

Students in good standing will receive an individual server account for storage of school-related files and data limited to a total of 2 GB. Students are responsible for keeping accounts under the 2 GB limit. Faculty, staff, and administrators will receive an individual server account for storage of school-related files and data limited to 5 GB. Faculty may ask to have a server folder that can be shared by multiple users in a class. Students, faculty, staff, and administrators who can demonstrate a need for greater storage space may make a request to the Information Technology department

and, at the discretion of the systems administrators, their quota may be increased. Some courses may require that students store larger quantities of data in their accounts. Students can, through their teacher, request a temporary increase in their space allotment to accommodate that coursework.

Persons whose accounts exceed the quota typically will be notified via internal e-mail and must reduce the size of their folder as directed. Otherwise, items in the account may be removed by a systems administrator. Users may not store executables, any applications licensed or unlicensed, or any material that violates federal or state laws or Latin policy in a personal server account. Some coursework may require students to store programming code and/or compiled programs in their account. Faculty who have such requirements for their students need to notify a systems administrator as to the nature of the data to be stored, along with a list of the students who require these special privileges.

To ensure that data is not lost, all data should be stored on network servers with the exception of large graphic, audio, or video files. Users can have a reasonable expectation that data stored on the servers will typically be backed up weekly. However, the Information Technology department never creates backups of music files, video files, or any other file greater than 250 MB. Furthermore, Information Technology personnel will restore from backup only in the case of server failure; they will not restore files deleted by individual users. It is the responsibility of the individual to make backup files of documents they create. The Information Technology department recommends that users backup important files to some type of removable media (e.g., CD-R, DVD-R, or USB Flash Memory).

Network and Internet Access

Access to the Internet allows Latin users to explore thousands of libraries, databases, and diverse resources worldwide. The network provides individuals ready access to some of the richest worldwide knowledge bases, including the Web, discussion groups, e-mail lists, and real-time interaction and collaboration with other Internet users. While the Internet is an immense resource for investigation of academic and personal interests, it is also a gateway to less desirable resources. We are aware of the potential dangers and try to protect Latin students through supervision and monitoring while they are at school. Student users are encouraged to explore and investigate topics being studied in school, as well as subjects of personal interest.

No Latin user may participate in any Internet activity or transmit or view materials that violate state or federal law. In addition, viewing pornographic or profane material or viewing sites that advocate violence against a person or a group is strictly forbidden. If a site is accidentally accessed or contacted in error, the individual must leave the site immediately. Any material or user contact with which the individual is uncomfortable must be reported to a faculty member. Furthermore, individuals are prohibited from installing an application or software that shares data or files over Latin's network without the prior written consent of Information Technology personnel.

Wireless Access

Students, faculty, staff, and administrators who wish to take advantage of the wireless network must register their wireless device (i.e. laptop, pda) with the Information Technology department. Wireless access keys are not to be shared among users who have not registered their equipment. Failure to comply with this procedure will result in loss of network access privileges. Furthermore, Latin reserves the right to inspect any personal wireless device, and all files contained on that device.

Laptops

Users of personal laptop computers in school must abide by the computing policy. Use of personal laptop computers in class, for note taking, etc., is allowed at the discretion of the instructor. Please be aware that Latin reserves the right to inspect any personal laptop computer, and all files contained on that system. Anyone who would like to connect a computer to the Latin computer network (or phone lines) needs to first contact the Information Technology department and obtain the required permission. Users must have current virus software protection.

E-mail and Intranet

Latin students, faculty, staff, and administrators may be provided with e-mail and Intranet account privileges. These accounts are utilized regularly as a normal channel of communication within the Latin community. It is therefore the account holder's responsibility to check his or her Latin e-mail and Intranet accounts periodically. Internal e-mail groups are maintained by the Information Technology department to more easily target e-mail to specific departments or groups at Latin. If you wish to have a list added, please e-mail your request to postmaster@latinschool.org. Use of Latin's internal e-mail groups will be monitored and any abuse will be met with the appropriate disciplinary action.

E-mail and the Intranet are resource-intensive services, requiring strict monitoring and enforcement of rules and standards of behavior. Users must follow these rules:

- Any type of harassment, including harassing e-mail, will not be tolerated.
- No one, under any circumstances, may send anonymous e-mail to any person within or outside the Latin School community. If you have received anonymous e-mail, please contact the mail administrator at security@latinschool.org.
- No one, under any circumstances, may send e-mail as someone other than themselves to any other person within or outside the Latin School community. If you have received e-mail from someone who has falsely identified themselves, please contact the mail administrator at security@latinschool.org.

- Do not send any commercial e-mail, solicitations, chain/pyramid letters, or virus alerts from your Latin account. If you receive such e-mail please alert the Information Technology department by sending e-mail to security@latinschool.org.
- Sending large volumes of unsolicited e-mail to a user or users (spamming) is not permitted.
- Every user must accept personal responsibility to monitor and control all materials sent or received under his or her account.
- When sending e-mail to multiple people please limit the number of recipients to 25. If you need to send to more than 25 people please contact the Information Technology department to have your list added to the server.

Websites

The Latin School offers the world a unique view of our community through our website. The Web is one of the most valuable and far-reaching methods of communication and interaction, and we are confident that by sharing a view of our values and mission we will further illuminate our high standards and achievements. Latin may on occasion seek to reproduce the image or likeness of a student, along with his/her name, on web pages designed or published by the School. Before placing student work on a website (classroom projects, artwork, etc.), Latin will typically ask the student for permission.

Currently, students can post a web page only under the direct supervision of a faculty or staff member. Individual student web pages are not allowed. Student-authored web pages that are part of a project must adhere to the following guidelines:

- Commercial activity, solicitations, or advertisements of any kind may not be attached to a web page.
- Content must reflect the spirit and substance of Latin's educational mission and must adhere to the guidelines provided in the Honor Code. Any content that disrupts the educational environment or process is prohibited.
- No copyrighted material may be posted without written authorization from the copyright holder, except where provided by fair use standards.
- Do not reproduce a person's image or likeness, or post any personal information about another person without his or her written consent.
- Under no circumstances may a web page threaten bodily harm, mental anguish, or property damage to individuals or groups.

Before any web page is posted or modified and made available to the public, it must be approved.

Software

Acquisition

To have a reliable software inventory all software purchases must be forwarded to the Information Technology department. Academic software must be approved by the Information Technology department and the Vice President of Academic Affairs who will consider several factors, including compatibility with existing systems and costs.

Installation

Students are not permitted to install any software on Latin School computer systems. Faculty, staff, and administrators are prohibited from installing any unlicensed or personally licensed software. Only members of the Information Technology department may install server software or software which allows remote access or control of a machine. Users are further prohibited from installing any software or hardware to record keystrokes or participate in peer-to-peer networks. If in doubt contact the Information Technology department.

Licensing

All licensing information and master software copies must be given to the Information Technology department, who will create backup copies of the software. The creation of said backups must comply with applicable license agreements. Master copies will be used for installation only if backup copies cannot be made. Any software found on school computing resources that is not licensed for use at The Latin School will be deleted upon discovery.

Support

There are three categories of software support. All operating systems and applications purchased by Latin fall into one of the three support categories. In some cases the Information Technology department may provide support for software that was not purchased by Latin. A complete list of supported software can be found on the Intranet. If it becomes apparent that a particular piece of non-supported software demonstrates a need for additional support then a request may be made to have the software reclassified to either the full or limited support category.

- Full Support

Software that is used by a large segment of the Latin community is assigned to the full support category. This would include, but is not limited to, Microsoft Office, FileMaker Pro, and Internet Explorer. Support is provided on an as-needed basis for fully supported software. Training may be provided for individuals or groups who wish to broaden their knowledge. The Information Technology department will provide internal and vendor documentation. The Information Technology department is responsible for providing, when appropriate, updated versions of full support software. Upgrades are performed on a regular basis. The Information Technology department will provide a reasonable level of communication and make every effort to minimize user disruption when upgrades of this software are performed.

- Limited Support

Software that does not require standardization on a school wide basis is given limited support. Vendor documentation will be made available and the Information Technology department may provide internal documentation.

- No Support

A user or department may request that a particular piece of software be installed, even if they are the only ones who will use that software. The responsibility of non-supported software lies with the individual or department who initially requested the software.

Security

Every member of the Latin School community is entitled to a secure and supportive learning environment, and the opportunity to make the greatest possible academic use of our computing and network resources. To ensure the integrity and reliability of the technological resources, users must respect the rights of other users and observe all relevant computing guidelines and School regulations. Compromising the integrity of computing and network resources in any way will affect all members of the Latin School community. Security guidelines are as follows:

- You are ultimately responsible for your own account:
 - Users must change all default passwords immediately upon receiving a new account.
 - Do not give another person your password or allow him or her to access your account in any way.
 - Make sure to logout when you have finished using a particular resource. (e.g.,

e-mail, OS X, PowerSchool, and the Intranet)

- Do not attempt to log into another person's account.
- Change your password periodically.
- Choose passwords that are "obscure," containing letters, numbers, and mixed case.
- Do not leave passwords in easily accessible places on your desk or near your computer.
- Vandalism, attempting to damage, harm, or obtain another user's data, or interrupting, delaying, or otherwise impeding another user's access to resources will not be tolerated.
- Theft of data, damaging, destroying, altering, or copying of another user's data will be treated as property theft and may result in disciplinary action, including immediate suspension of access privileges, suspension or expulsion from school, termination of employment, and/or civil and criminal charges.
- Vandalism or theft (either physical or electronic) of any Latin technology will result in disciplinary action.
- No one may gain access to network or computing resources anonymously. No one may attempt to gain access to network or computing resources using another user's login or password.
- Do not transmit viruses. Exercise extreme caution when downloading files from the Web and when accepting attachments to e-mail.
- Do not adversely modify settings or data on Latin School technology systems.
- Do not attempt to bypass security measures. Attempting to circumvent security will be treated the same as an actual security breach.

In short, there can be no inappropriate use of network or computing resources. Notify the Information Technology department of any potential security risk or violation immediately.

Copyrighted Material and Peer-to-Peer Software

Receipt of, possession of, or distribution of copyrighted material without the permission of the copyright holder is prohibited. Students, faculty, staff, and administrators should note that such acts may be a violation of the laws of the United States (title 17, U.S. Code). Violators of copyright law could be subject to

felony charges in state or federal court, and may be sued by the copyright holder in civil court. Such civil suits could subject the violator to liability for infringement, with significant monetary damages. Thus, peer-to-peer software such as LimeWire and Kazaa are not allowed on the Latin School's computer systems or network; this includes any personal electronic device. Furthermore, any software that can be used for file sharing (peer-to-peer or otherwise) is also prohibited from being installed, stored, or executed on the Latin School's computer systems or network without the specific written permission of the Information Technology department.

Discipline

Minor infractions of any policy will result in an e-mail and/or verbal warning that may become part of one's permanent record. Infractions such as, but not limited to, the sharing of passwords, harassment, or repeated or flagrant minor infractions may result in the loss of some or all computing privileges. Serious violations will be referred to the administration for appropriate action, and may result in suspension of privileges, expulsion, termination of employment, and/or civil and criminal charges.

Requesting Assistance

- To report security violations or the abuse of network or computing resources or to raise any concerns or questions, please contact the Information Technology department at security@latinschool.org or call (312) 582-6130.
- Questions and concerns regarding e-mail and e-mail accounts should be directed to it@latinschool.org.
- For further information, an on-line version of this policy, and answers to frequently asked questions, please see the Intranet.

This document last revised 7/11/05.