

ITS student guide to:

HLS Technology Policies
Personal Computer Security
ITS Resources and Help Services

Fifteenth Edition
August 2008

Harvard Law School Information Technology Services

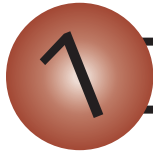
CONTENTS

Policies	3
HLS Computer & Network Resources Usage Agreement	3
E-account Policies	6
FERPA.....	6
Electronic Copyright Violation Policy	7
Computer Security.....	8
Set an Administrator Password.....	8
Configure Automatic Software Updates	9
Personal Firewalls	10
Use Anti-Virus Software	11
Use Spyware Removal Software	11
Phishing: Don't Get Caught!.....	12
Virus Attachments.....	12
Use VPN to Secure Wireless Connections.....	12
Physical Security.....	12
Services Provided By ITS	13
FAStAccess Device Management System - Network Registration	13
HLS E-mail Account	13
Course Management System.....	14
Student Printing Resources.....	15
Law School Site-Licensed Software Offered to Students	15
Additional ITS Resources for Students	17
ITS Student Help Desk	17
Media Services for Students	19
Public Internet Kiosks.....	19
Langdell Library.....	19
Computer Purchases	19
Computer Rentals	19
ITS Student Computer Lab and Help Desk Information	20

Please follow the links within each section throughout this hand book for the most up to date information, as well as further detail regarding the services provided, for each topic.

And remember to watch for News Alerts posted by Information Technology Services here:

<http://www.law.harvard.edu/administration/its/>



POLICIES

<http://www.law.harvard.edu/administration/its/policies/>

HLS Computer & Network Resources Usage Agreement

In support of Harvard Law School's learning, teaching, and research goals, Information Technology Services (ITS) provides current members of the Law School community with access to the School's computer and network resources. To ensure that these resources remain available to all members of the community and to protect the substantial investment the Law School has made in its computer and network systems, your access is conditioned upon your agreeing to and complying with the terms of this Harvard Law School Computer and Network Resources Usage Agreement. This agreement supplements Appendix A in the Catalog, which outlines your Rights and Responsibilities as a member of the Harvard University community.

USE OF COMPUTER AND NETWORK RESOURCES

The Law School community should use the network with respect and care. Unacceptable use of the network should be avoided. Unacceptable use includes: (1) interfere with the work of others, (2) gain unauthorized access to computer or network resources, (3) circumvent or violate local network, electronic accounts, or Web security systems, (4) use Law School electronic accounts of others, (5) damage or inappropriately degrade performance of computer and network resources, (6) willfully misrepresent the identifying attributes of your electronic communications (e.g., date and time of creation or transmission, message identification number, IP address, etc.), (7) unlawfully use, duplicate, or distribute software and files, (8) use computer or network resources for commercial purposes without authorization, (9) use computer or network resources in violation of any applicable law or Law School regulation, (10) Installing any kind of wired networking equipment such as a router or firewall that can hide the identity of machines behind them, or (11) Installing any kind of wireless network equipment including wireless routers or wireless firewalls that can provide wireless services and hide the identity of machines connecting to them.

In addition to possible disciplinary action and/or termination of your network privileges, the violation of any of these restrictions may result in legal penalties. You are responsible for the use of your electronic accounts (e.g., email, course Web sites, and printing) and are not permitted to grant others access to these accounts. Nor should you disclose your password to anyone, including your friends or family. The staff of the Information Technology Services (ITS) department will not ask you for your password when ITS assistance is requested, unless absolutely necessary. ITS does not share your password.

SECURITY AND PRIVACY

Electronic communications, communicative attributes of electronic communications (e.g., date and time of transmission, subject, identification number, with whom you communicate, how often, etc.), and files stored on Law School servers will be kept confidential, in accordance with privacy policies set by Harvard Law School, Harvard University, and the law.

ITS maintains regular backups of network servers, including e-mail messages and files. The purpose of these backups is to restore the system in case of data loss due to a system crash. These backups are

subject to the same privacy protections as any network data.

In the normal course of official duties, ITS system administrators have access to all data on the system, including contents of e-mail messages and communicative attributes. While ITS policy is to avoid coming into contact with or reading any communications, ITS system administrators may if absolutely necessary come into contact with or read communications in order to ensure proper operation of network resources; the most common circumstance in which this contact occurs is during an attempt to deliver a misrouted message. System administrators will produce any available log records, messages, and files at the request of the Dean for Administration, Dean of Students, or the Administrative Board.

When you do request assistance from ITS, you implicitly give the staff permission to view the data in your account or on your computer to the extent necessary to investigate, diagnose, or correct the problem you are having, and ITS staff will make reasonable efforts to alert you to the anticipated and actual scope of any such viewing.

The use of encryption to secure the contents of one's communications or files is permitted.

ANONYMOUS AND PSEUDONYMOUS COMMUNICATIONS

The rules governing whether electronic communications may be anonymous or pseudonymous are determined by the particular context within which the communication occurs, and the violation of such rules may result in disciplinary action. Three general rules, however, govern all electronic communications, and may not be locally modified without the expressed curriculum-related permission of the relevant Law School faculty member:

- (1) Electronic communication systems, whether email or discussion groups, produce records that facilitate the ability to trace such communications. These records may not in all cases reveal the identity of the sender, but they do facilitate the identification of a particular communication's origin. You are prohibited from modifying this data in a manner that will interfere with the ability to trace a communication.
- (2) Members of the Law School community are given iCommons and email accounts based on their legal names; you may not take steps to hide your identity in electronic communication when using Law School accounts, computers, networks or servers.
- (3) In no context may you fraudulently misrepresent your identity.

MISUSE OF RESOURCES

In accordance with "Rights and Responsibilities" written in Appendix A of the Harvard Law School Catalog, the Law School neither endorses nor censors any opinion expressed on, or originated on, its computer systems or network. However, because the electronic communications originating from the Law School community automatically carry the Harvard Law School domain name ("law.harvard.edu"), you should be particularly careful not to inaccurately identify yourself as representing or speaking for the institution. More generally, in the use of email or other electronic communication, the same standards of conduct governing the use of telephones and oral and written communication apply. You may not use email to broadcast messages or "spam" the Law School community.

As with any Law School resource, "misuse" includes the theft or deliberate damage of any Law School equipment or resource. With regard to Law School computer and network resources, it also includes other activities that interfere with the efficient and reliable provision of computer and network services. Included are the following specific prohibitions:

- (4) You may not relocate or disassemble any Law School network, computer or peripheral equipment.
- (5) You may not connect your computer to a network port (data jack) unless your computer is assigned to that port or the port is designated as “roaming.”
- (6) You may not attempt to intercept, analyze, record, or tamper with network data packets.

EMERGENCY SITUATIONS AND COMPLIANCE WITH ACCOUNT QUOTAS

In any situation that threatens system security, stability, integrity, or performance, ITS system administrators will take necessary action to defend computer and network resources. These defense measures may include terminating or suspending processes or user accounts without prior notice. ITS will notify affected user(s) as soon as feasible. Emergency situations may or may not involve deliberate misconduct. All users are expected to adhere to the specific usage quotas that govern Harvard Law School accounts. Repeated failure to act upon ITS requests regarding such quotas may result in files or messages being deleted from over-quota accounts.

COPYRIGHT AND SOFTWARE LICENSES

All Harvard users must respect the copyrights in works that are accessible through computers connected to the Harvard network. Federal copyright law prohibits the reproduction, distribution, public display or public performance of copyrighted materials without permission of the copyright owner, unless fair use or another exemption under copyright law applies. In appropriate circumstances, Harvard will terminate the network access of users who are found to have repeatedly infringed the copyrights of others, and may also take disciplinary action.

Users may not install software on Harvard-owned and operated computers without evidence of a valid software license or other right or privilege to install such software.

CASES OF MISCONDUCT

Whenever a case of misconduct is suspected by or reported to ITS, ITS will immediately notify the person or persons accused of such misconduct and the appropriate supervisory authority, such as the Dean of Students or the Dean for Administration. As the situation warrants, the supervisory authority will determine the course of any investigation or disciplinary action. After such notification and while any inquiry is pending, ITS has the right to deny access to Law School equipment and network services to any person or persons believed to be violating the guidelines set forth here.

In addition to possible disciplinary action on the part of the Law School and/or termination of your network privileges, misuse of electronic communications, use of computers for unlawful purposes, and violations of copyright laws carry civil and criminal penalties under Massachusetts and federal law. All users are expected to learn and abide by these laws. Harvard’s policy is to cooperate with law enforcement officials in the detection, investigation, and prosecution of unlawful activity; unless lawfully prohibited by the authorities, you will be notified if information specific to your account or communications is turned over to non-Harvard authorities.

DEPARTURE FROM HARVARD LAW SCHOOL

Before you leave the Law School, you must remove all Law School site-licensed software that you have installed on your personally owned computer(s) (See page 16 for full list of site-licensed software).

E-account Policies

ELECTRONIC ACCOUNT ELIGIBILITY

The following HLS affiliates are eligible for HLS e-mail accounts: faculty (including visiting); exempt and non-exempt staff; students (including students on leave); casual workers and contractors upon request and approval by ITS; and visiting researchers and fellows. Cross-registered and auditing students are eligible for HLS e-mail accounts only to the degree that such accounts enable access to course-related web sites and MyHLS content: such accounts are typically locked and forwarded to the student's existing Harvard or other-university account. Incoming 1L, LLM, and SJD student accounts are created automatically during the summer based on information provided by the Registrar's Office. Other students should request e-mail accounts from the Student Help Desk located in the basement of Hauser Hall. Faculty and staff e-mail accounts are created upon request by the Faculty-Staff Help Desk, located in the basement of Hauser Hall.

ITS will only extend your expiration date for one of three reasons:

1. Your student status at the Law School has been extended--if you have been extended, please provide a photocopy of your new Harvard Law ID card showing the new expiration date.
2. You do not possess a Harvard Law ID card with new expiration date, but will be working with an HLS faculty member or department--please provide an original letter from the faculty member or department head stating your role and the end date for this employment.
3. You have been accepted at HLS as staff and can provide a copy of your new ID card, or your new end date can be verified in the University employee database.

If you are eligible for an extension for any of these reasons, bring the required documentation to Hauser 020 to request the extension at the student help desk.

LEAVE OF ABSENCE

If you are planning to take a leave of absence from the Law School, the Registrar's office will inform ITS of your change in status and by default your email account will be set to expire one month after your anticipated return date. Upon your return, the Registrar's office will inform ITS of your new graduation date and your account expiration date will be updated accordingly.

FIND MORE INFORMATION REGARDING E-ACCOUNT POLICIES ON THE WEB:

<http://www.law.harvard.edu/administration/its/policies/email.php>

FERPA

If, as is your right under FERPA (Family Educational Rights and Privacy Act) regulations, you want to have your email address kept private, you must request this through the Registrar's Office. If you have requested email address privacy and want it to be removed, again, you must make this request through the Registrar's Office.

Electronic Copyright Violation Policy

Under the terms of the Digital Millennium Copyright Act, Harvard must respond to notifications of infringing content on its network, and implement a policy that provides for the restriction or termination of network services for repeat offenders. In accordance with the HLS Network Usage Agreement, which states:

“In appropriate circumstances, Harvard will terminate the network access of users who are found to have repeatedly infringed the copyrights of others, and may also take disciplinary action.” violators are subject to the following consequences:

First violation: warning. User must remove infringing content and assert in writing their commitment to upholding copyright and acceptable use policy (see Electronic Copyright First Violation Student Agreement). Failure to respond to the warning within 7 days will result in the suspension of network privileges until the matter is resolved.

Second violation: immediate temporary suspension of HLS network privileges. User will not be able to register their computer system(s) for use on the HLS network for a period of 90 days.

Third violation: indicates a serious disregard for HLS policy, appropriate use of HLS network resources, and for federal copyright law. Your network privileges will be immediately suspended indefinitely. A permanent loss of HLS network privileges may be incurred and matter is referred to the Dean of Students for possible disciplinary action.

Violators may also be criminally liable for their actions and be subject to other fines, civil damages and prosecution as applicable by law.

APPEALS PROCESS

If you think your second violation may be the result of a security compromise that allows a third party to share copyrighted material via your personal computer without your knowledge, you may appeal the standard 90-day suspension. Your network privileges will be suspended while the matter is investigated. If it is determined that the violation was in fact the result of a security compromise and the content was being shared without your knowledge, your network privileges will be reinstated after 30 days from the date of the notice. If no evidence of a security compromise is found, your network privileges will be suspended for the full 90 days.

ACCESS TO ELECTRONIC ACADEMIC MATERIALS DURING NETWORK SUSPENSION

You will still be able to access your HLS email account and all HLS electronic resources necessary to meet course and degree requirements on-campus via public computers located in the ITS Student Computer Lab and Langdell Library.

FIND MORE INFORMATION REGARDING THE ELECTRONIC COPYRIGHT VIOLATION POLICY ON THE WEB:

http://www.law.harvard.edu/administration/its/policies/copyright_violation.php

2

COMPUTER SECURITY

<http://www.law.harvard.edu/administration/its/students/security/index.php>

Introduction

Your computer is under the constant threat of electronic attack. There are several precautions you can take to minimize your computer's vulnerability to these threats, and protect your data and personal information.

Many people think Macintosh computers are impervious to the viruses and security holes that plague Windows users. However, the new generation of viruses that exploit specific applications or affect a network in general. In some cases, as with the Nimbda virus, a Macintosh acts as a "carrier computer" or agent that spreads the infection over the network. Also, if you use a Windows emulator or have a dual boot system, your computer faces the same security vulnerabilities a Windows machine does. Macintosh users need to be just as diligent and conscientious about practicing good security as Windows users do.

ITS recommends that you take the following steps to protect your computer before you attempt to connect to the HLS Network. Failure to do so may delay your network registration process and will leave your computer and data vulnerable to attack.

Set an Administrator Password

Computers without Administrator passwords are extremely vulnerable to hackers, viruses and worms. Choose a strong password made up of a combination of at least eight letters, numbers and other characters. Simple passwords composed of words, or words with numbers added to the beginning or end are easily deciphered. A strong password is your first line of defense.

To set an Administrator Password in Windows XP:

1. Turn your computer off, wait 15 seconds, then restart it. When your computer manufacturer's logo appears on the screen, start pressing the **F8 key** on your keyboard. A text menu should appear. Use the arrow keys on your keyboard to select **Safe Mode** and hit the **Enter** key.
2. The next menu will prompt you to select your operating system, highlight **Microsoft Windows XP** and hit **Enter**.
3. When safe mode has loaded, you will be brought to the Welcome screen. Select the **Administrator** account to log in.
4. Once the Administrator account has logged in, you will be presented with a message warning you that you are in safe mode. Click **Yes** to proceed to work in safe mode.
5. From the **Start** menu, choose **Control Panel**.
6. In the **Control Panel**, double-click on **User Accounts**.
7. In the **User Accounts** window, select **Administrator** account.
8. In the **Administrator** account settings screen, click on the link for **Create a password**.
9. In the **password creation window**, fill out the requested blanks. When you're finished, hit the **Create Password** button.

10. If asked if you wish to make this account's files private, click either **Yes** or **No** (depending on your preference), then click **Finish**.
11. Close the User Accounts window and **restart** your computer normally.

To set an Administrator Password in Windows Vista:

- Microsoft has disabled the Administrator account in Windows Vista in an attempt to create a more secure operating system*.

**You should also make sure all other user accounts on your computer are protected by a secure password.*

To set Account Passwords in Mac OS X:

1. Click the **Apple Menu**, then **System Preferences**.
2. Under **System**, click **Accounts**.
3. For each account on your computer, select the account from the left and click **Password**.
4. Enter a strong password comprised of letters and numbers for each account.

FIND MORE INFORMATION REGARDING CHANGING YOUR ADMINISTRATIVE PASSWORD ON THE WEB:

WINDOWS: <http://www.law.harvard.edu/administration/its/students/security/passwordxp.php>

MAC: <http://www.law.harvard.edu/administration/its/students/security/macpassword.php>

Configure Automatic Software Updates

Microsoft and Apple are continually releasing patches and updates to their operating systems (OS) to fix security holes that allow hackers and viruses to exploit your computer. To stay current with these security patches, you can configure your OS to automatically download updates.

To Enable Auto-Updates in Windows XP:

1. Click on **Start**.
2. Right click on **My Computer**, and choose **Properties**.
3. Click on the **Automatic Updates** tab.
4. Choose **Download updates for me, but let me choose when to install them**.
5. Click **OK**.

To Enable Auto-Updates in Windows Vista:

1. Click on **Start**.
2. Click on **Control Panel**.
3. Click on the **Security** icon.
4. Under **Security Center** click **Turn Auto Updates On/Off** to **On**.
5. Close the **Control Panel**.

Once Windows notifies you that your updates have been downloaded, all you need to do is install them!

For more information on Windows Update, please visit

<http://www.windowsupdate.com>. More information regarding Windows security can be found at: <http://www.microsoft.com/athome/security/default.mspx>.

To Enable Automatic Software Updates in Mac OS X:

1. Click the **Apple Menu**, then click **System Preferences**.
2. Under **System**, click **Software Update**.
3. Click on **Check for Updates**. (For some versions of OS X, this is called **Update Software**.)
4. Under **Check for Updates**, select **Daily**.
5. To update your computer immediately, click **Check Now** and install all available updates.

FIND MORE INFORMATION REGARDING ENABLING AUTOMATIC UPDATES ON THE WEB:

WINDOWS: <http://www.law.harvard.edu/administration/its/students/security/windowsupdate.php>

MAC: <http://www.law.harvard.edu/administration/its/students/security/macsoftwareupdate.php>

Personal Firewalls

Personal firewall software adds another protective barrier between your computer and potentially harmful Internet traffic by blocking certain ports that are commonly exploited by viruses and hackers. Blocking these ports can also prevent desired tasks, such as transferring files via Instant Messaging, hosting multi-player games and file sharing.

ITS recommends enabling the built-in firewall in Windows XP, Vista and Mac OS X. There are a number of other firewall products on the market; make sure that you do not have 2 or more firewalls running on the same PC as this will cause programs to malfunction.

To Enable the Built-in Firewall in Windows XP:

1. Click on **Start**.
2. Go to **Settings, Control Panel**.
3. Double click **Windows Firewall**.
4. In the **General** tab, select the radio button next to the green shield that says **on**.
5. If a program is going to access the internet you must give it permission via the firewall software. Select the **Exceptions** tab and check any programs that you want to access the Internet. If you need programs that are not on the list, click the **Add program** button.

To Enable the Built-in Firewall in Windows Vista:

1. Click on **Start**.
2. Go to **Control Panel**.
3. Go to **Security**.
4. Click on **Windows Firewall On/Off** and choose **On**.
5. Close the **Control Panel**.

🔑 To Enable the Built-in Firewall in Mac OS X:

1. Click on the **Apple Menu** and select **System Preferences**.
2. Under **Internet and Network**, double-click on **Sharing**.
3. In the **Sharing** window, click on the **Firewall** tab and click the **Start** button.
4. By default the Mac OS X firewall does not allow most file sharing options. If you would like to enable them click the **On** check box. If you need programs/ports/functions that are not on the list click the **New** button.

Please refer your personal firewall software support questions to the software manufacturer. Information regarding Mac OS X's built-in firewall can be found at: <http://www.apple.com/macosx/features/security>.

Use Anti-Virus Software

ITS provides all currently enrolled HLS students a free copy of Symantec Anti-Virus (SAV). SAV is a full-featured anti-virus program designed to scan all internal and external drives, as well as all incoming and outgoing emails and attachments. You may install and use SAV on your personal computer during your HLS affiliation. Licensing restrictions prohibit the distribution to non-HLS affiliates. SAV is available for both Mac and PC.

It is important to note that your computer should only have ONE anti-virus program installed. If you wish to download the HLS SAV client, please uninstall any anti-virus software you may already have on your machine.

Download your copy of SAV at: <http://www.law.harvard.edu/administration/its/students/antivirus.php>. For complete instructions on installing SAV and configuring auto-updates, please refer to the above link.

KEEP YOUR ANTI-VIRUS SOFTWARE UP TO DATE

New viruses are developed every day. To keep your computer adequately protected you must regularly update your virus definition (DAT) files. If your DAT files are out of date, your virus scan software will not detect new viruses.

Use Spyware Removal Software

Spyware is often bundled with freeware and shareware downloads and is used to covertly track your usage and gather personal information. Users of peer-to-peer file sharing programs are particularly susceptible to spyware. It can be as harmless as installing a cookie used by advertisers, or as insidious as capturing your keystrokes and snooping around your hard drive.

Spyware can consume major system resources, resulting in a degradation of your computers performance. It can also make changes to your system, such as resetting your Internet browser's home page.

To protect your computer and personal information, you should use a malware removal program provided by Windows XP SP2 or Windows Vista on a regular basis. SAV also provides a spyware removal tool.

Phishing: Don't Get Caught!

SPAM and virus related emails are becoming more sophisticated. A technique called phishing is used to fraudulently gather confidential personal information such as SSN, credit card numbers and passwords. They often purport to be from trusted companies, and ask you to follow a link provided in their email to update or verify your account information. They often threaten dire consequence for failing to comply. If you receive an email asking you to provide confidential information, do not follow the link provided in the email. Instead, go directly to the company web site by typing their web address into your browser. Do not use the address provided in the email. More information about phishing can be found at: <http://en.wikipedia.org/wiki/Phishing>.

Virus Attachments

Similarly, virus emails may purport to come from a trusted source, such as HLS ITS, and may instruct you to open an attachment containing important account information. Note that any emails sent to the HLS student community will come from help@law.harvard.edu, and will not contain any attachments.

All email that passes through the MyMail server is scanned with anti-virus software. However, this does not mean that you do not need to use anti-virus software on your personal computer. Viruses can be spread directly over a network, or through infected media such as CD's and floppy disks. Always use virus detection software on your personal computer and keep it up to date with the latest virus definition files.

Use VPN to Secure Wireless Connections

Data travels through the wireless network over open radio waves, making it very easy for malicious users to intercept any data you are transmitting, including passwords, bank account numbers, and other sensitive information. VPN encrypts data being sent between your computer and the wireless access point, making it nearly impossible for a malicious user to decrypt your data. ITS provides Virtual Private Networking (VPN) software to the HLS community to secure wireless and remote connections to the HLS Network. See <https://www.law.harvard.edu/administration/its/software/> for information on how to download VPN.

Physical Security

Unattended laptops pose several security issues. A good rule of thumb is to never leave your laptop unattended in a public space.

THEFT

There are several types of security locks to protect your laptop from theft. The Harvard Police Department offers two laptop registration programs. More information on these programs can be found here: www.hupd.harvard.edu/laptop.php

ACCESS TO YOUR COMPUTER AND ACCOUNTS

To prevent unauthorized access to your system or accounts (such as email), you should lock your computer when you are away from it.

Always use the log out button to log out of applications and close the browser to prevent unauthorized access to your accounts, especially when working on public lab or kiosk computers.

3

SERVICES PROVIDED BY ITS

<http://www.law.harvard.edu/administration/its/students/>

FASStAccess Device Management System - Network Registration

Before you can connect your computer to the HLS network, you must first secure it (see pages 9-13) and then register it via the FASStAccess Device Management System: <http://autoreg.fas.harvard.edu>.

Please note that you will need to register each device you wish to use separately. This means if you intend to connect to the HLS network via both a wired and a wireless card, you need to register both cards. Please also note that you are responsible for adhering to the HLS Network Usage Agreement (pages 3-6) and the Electronic Copyright Violation Policy (pages 7-8). Violations of these policies may result in the loss of network privileges.

FIND MORE INFORMATION REGARDING NETWORK ACCESS ON THE WEB:

<http://www.law.harvard.edu/administration/its/students/network.php>

HLS E-mail Account

Harvard Law School provides every HLS affiliate with an HLS email address and access to the HLS MyMail email system. You can access MyMail through a desktop email client such as Outlook or through the MyMail web client.

MYMAIL WEB CLIENT

The MyMail web client, located at: <https://mymail.law.harvard.edu>, allows you to access your mail through a web browser from any computer connected to the Internet; no special software is required. When using the web client, you are interacting directly with the mail server. Messages (incoming and outgoing) are not saved to the computer's hard drive. Complete instructions for using the web client can be accessed by clicking on the **Help** link in MyMail.

DESKTOP EMAIL CLIENTS

A desktop email client is a software program you install on your personal computer to manage your mail. These programs are generally configured to "pop" (download) your mail to store copies of your messages on your local hard drive. If you wish to read mail both via a desktop pop client and via the MyMail web client, you will need to configure your pop client to leave a copy of your mail on the server.

Find instructions on recommended desktop client programs, configuration settings, and best practices on the web, linked below.

FIND MORE INFORMATION REGARDING YOUR HLS E-MAIL ACCOUNT ON THE WEB:

<http://www.law.harvard.edu/administration/its/students/email.php>

Email Quota Policy

All HLS students are allocated 250 MB of storage space on the email server. If you exceed 90% of your quota (225 MB), you will receive a warning email and you will see an on-screen warning when you log into the web client. You will receive another warning message when your account reaches 95% of your

quota allocation (237.5 MB). You will receive a third message notification when your account reaches your quota maximum, informing you that your account is over quota and incoming messages will be rejected until you free up space by deleting messages. Heed these warnings! If your account goes over quota, or if the system tries to deliver a message that would put it over the quota, mail is not delivered to your account. You will still be able to log into your account and view old mail. New mail that exceeds the quota will be returned to the sender with a notice that the message was not delivered because the account was over quota. These messages will not be re-delivered.

To avoid undelivered messages, you should effectively manage your email quota. As soon as you receive a quota warning, you should clean out mail stored on the server to make room for new mail. You will receive a verification email from the system when you have brought your account back under quota. You can view your quota at anytime by logging into the MyMail web client at <https://mymail.law.harvard.edu>. Your quota usage is displayed in the upper left corner of the page.

NetLocker

NetLocker is an on-line file management system available to all students at HLS. This means that your files can be uploaded, organized, viewed, and obtained from any computer with an Internet connection. The benefits of NetLocker include:

- The ability to access your files globally from any computer with an Internet connection.
- The ability to collaborate and share information with others.
- The ability to share these files with both NetLocker and non-NetLocker users.
- The ability to have a back-up copy of files that are currently stored on your hard drive.
- The ability to securely store your files. Only you can access your files and only you can grant permission for others to access and share your files. (Exceptions relating to ITS access to systems for maintenance and security are outlined in the HLS electronic Usage Agreement.)

Find more information regarding NetLocker on the web:

<http://www.law.harvard.edu/administration/its/students/netlocker.php>

Course Management System

The majority of course web sites at HLS are found in the MyHLS course management system at: <http://myhls.law.harvard.edu>.

MyHLS requires you to log in with the first eight digits of your Harvard ID number and your PIN. If you do not already have a pin, you can request one at: <http://www.pin.harvard.edu>.

Most faculty utilize the MyHLS course management system to maintain their course web sites. The system provides a single view into your MyHLS course web sites, links to tools such as Netlocker, MyPlan, and MyMail, and lists of links to HLS internal resources and useful, external resources as well. You can also customize the Home page of MyHLS by adding resources, links, and RSS feeds.

There are several Tabs across the top of the MyHLS page. Clicking on the COURSES tab will bring you to a page that contains links to course sites in which you are enrolled. You may not see course sites for all of your classes, however as use of the MyHLS system is optional for faculty. If you have questions about your course registration you should first check MyPLAN which is the system of record for your official HLS registration. Follow-up registration questions should be directed to the HLS Registrar.

MyHLS course sites have an array of tools that may be present in one or more of your course sites. These include a discussion board tool, class email tool, profiles tool, blog tool, file upload tool and a podcast tool.

FIND MORE INFORMATION REGARDING OUR COURSE MANAGEMENT SYSTEM ON THE WEB:

<http://www.law.harvard.edu/administration/its/students/icommons.php>

Student Printing Resources

Each incoming student is issued a printing account at registration. You must have a printing account to print from any of the public printers on campus. LLM and JD students are allocated a \$50 print credit each year.

Once your \$50 dollar allocation is exhausted, printing costs will be charged to your term bill each month during the academic year. The system tracks your print usage and charges the accumulated dollar amount to your term bill. The charge will appear on your term bill as "Printing- HLS". You will not receive any notification from the system when you have exhausted your allocation credit; it is the responsibility of the individual to monitor personal print usage. You can track your balances at: http://printing.law.harvard.edu/acct_info.

You can download and install the public printing software (LPT:One) via the Software Library, linked below. The public printers are located (and named) in the Student lab in Hauser 020 (Daisy), the Harkness Common (Hark), Austin Hall (Austin), and the Langdell Library (Areeda).

FIND MORE INFORMATION REGARDING STUDENT PRINTING ON THE WEB:

<http://www.law.harvard.edu/administration/its/students/printing.php>

Law School Site-Licensed Software Offered to Students

Information Technology Services provides its students with with the following software packages:

Microsoft Windows

- Microsoft Office Suite
- Symantec Anti-Virus
- LPT:One - Print Cost Management
- HLS/FAS VPN Client
- SSH Secure Shell

FIND MORE INFORMATION REGARDING MICROSOFT WINDOWS SOFTWARE OFFERINGS AND DOWNLOADS ON THE WEB:

<http://www.law.harvard.edu/administration/its/software/windows/>

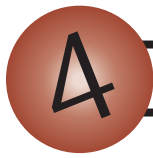
Macintosh

- Microsoft Office Suite
- Symantec Anti-Virus
- LPT:One - Print Cost Management

- HLS/FAS VPN Client
- Fetch - SSH Secure Shell

FIND MORE INFORMATION REGARDING MACINTOSH SOFTWARE OFFERINGS AND DOWNLOADS ON THE WEB:

<http://www.law.harvard.edu/administration/its/software/mac/>



ADDITIONAL ITS RESOURCES FOR STUDENTS

ITS Student Help Desk

The Student Help Desk, located in Hauser 030, provides the following services to HLS students, visiting researchers, fellows and scholars:

- Trouble shooting assistance for problems accessing the HLS Network from your personal computer (computer must meet the HLS minimum hardware requirements)
- General assistance with problems using supported software on your personal computer
- Assistance with using the Student Computer Lab hardware and software
- Assistance with the HLS Student Print System (LPTOne)
- Assistance recovering data files necessary to meet degree requirements

Support for research applications (Westlaw, Lexis/Nexis and HOLLIS) is handled by the Library. Please contact the Library for training and other assistance with these research applications.

All requests for help are taken on a first-come, first-served basis. If your problem cannot be resolved during the initial contact, you may need to bring your computer equipment and related software to the Help Desk for further assistance; the ITS Student Help Desk is unable to do on-site visits for students. Due to licensing and copyright laws, ITS can only install/ re-install software from your original media and product key. We are unable to provide you copies of software, so please remember to bring all necessary software to school with you.

NETWORK ASSISTANCE

If you live on campus and are experiencing trouble with the data jack in your room, please make sure you have registered your wired Ethernet card as instructed on page 17. If your card is properly registered and you think the data jack may be broken, contact the Student Help Desk or fill out the Dorm Jack Repair Request form located at: http://www.law.harvard.edu/administration/its/forms/jack_repair.php. The Help Desk will then schedule an appointment to check the jack in your room.

If you are experiencing problems using the wireless network on campus, please contact the Student Help Desk or fill out the form located at: http://www.law.harvard.edu/administration/its/forms/wireless_repair.php with the following information:

- Your name and contact information
- The exact location of the problem (building and room number)
- Exact time and date of the problem

Wireless problems can result from many factors, so it is critical that you provide us with as much timely information as possible to help us pinpoint the cause.

PERSONAL COMPUTER EQUIPMENT SUPPORT

ITS will troubleshoot and suggest repair options for software and hardware on personally owned computers. Insurance policies prevent us from repairing student-owned hardware and equipment. However, if hardware repairs are necessary, the Student Help Desk will provide the student with an assessment and referral form to facilitate hardware repairs by preferred vendors.

If you would like to know more about purchases of personal computer equipment, please see "Computer Purchases" on page 19.

ITS Student Computer Lab

HARDWARE AND SOFTWARE

The Lab, located in Hauser 030, offers a full range of hardware and software resources to HLS students. There are 20 Windows and 5 Apple workstations equipped with the following software packages:

- Microsoft Office 2003 Suite
- Corel Word Perfect
- SFTP client
- STATA*
- Adobe Studio 8 (includes Dreamweaver, Flash, Contribute, Fireworks and FlashPaper)
- Instant Messaging software
- Internet browsing software (IE, and Netscape)
- Lexis/Nexis
- Westlaw
- HOLLIS
- Photoshop is installed at the scanner stations

**The complete set of STATA manuals are available for reference at the Student Help Desk (located in the Lab). Due to the complex nature of STATA, Help Desk staff are unable to provide application specific support for this particular program.*

PRINTING

There are two high-speed black and white printers and one high speed color printer in the Lab. All three printers are enabled for double-sided printing. These printers are listed as Daisy, Zeke and Color within the lab systems.

SCANNERS

There are several scanners available for student use in the Lab (both Mac and PC). Instructions for scanning in Photoshop and creating PDFs are located at the scanner stations.

VIDEO EDITING

Two video editing stations are available for student video projects. Please refer to <http://www.law.harvard.edu/administration/its/students/lab.php> for more information.

FAXING

A fax machine is available for student use. Incoming faxes are free (the number is posted on the fax machine). Domestic and international rates are posted on the fax machine. A fax machine is also available outside of the student lab in Austin Hall.

Media Services for Students

Services such as videotaping, video playback, audio and video duplication, data projectors, public address systems, web streaming, and post-event file encoding are provided by the ITS Media Services group for classes, student organization events and conferences. There is no charge for curriculum-based requests. Fees may apply to all other requests. Advance reservations are always necessary. For more information, including pricing and reservations, please visit: <http://www.law.harvard.edu/administration/its/forms/#av>.

Public Internet Kiosks

There are two public Internet kiosks located on campus for quick stop email and network access. One is located on the ground floor of the Harkness Commons and the other is located in the basement of Austin Hall. Each kiosk cluster is enabled for printing through the LPTOne student printing system, allowing you to print via your student print account.

Langdell Library

The Library has nearly 100 workstations, 30 laser printers, and 500 high-speed Ethernet jacks for patron use. All terminals are configured for Library searching, general law research through online databases Lexis and Westlaw, and Internet browsing. The Library also provides photocopiers for student use. Please note that the Library IT support staff maintains the Library equipment and any support issues should be directed to the Library Tech RAs.

Computer Purchases

Harvard has partnered with Apple and Lenovo to offer the HLS community substantial discounts on computer equipment. Harvard also has substantial educational discounts on software. For more information go online, linked below, however, you may also visit the Harvard University Technology Product Service Center showroom located in Science Center B11 on the FAS campus where you can view current computer models. <http://www.law.harvard.edu/administration/its/students/admit.php>

Through this website you will be able to purchase a laptop pre-configured with the Law School's image. Loaded onto this image the Lenovo ThinkPads will include:

- Microsoft Office 2003
- Symantec Anti-Virus
- Will be configured to access the HLS wireless network
- Contain pre-configured links to HLS resources
- Will be fully supported by the HLS Student Help Desk.

Due to limitations with the imaging technology, we will not be able to offer the custom HLS image with any hardware changes to the models listed online.

Computer Rentals

Harvard Student Agencies provides convenient computer rentals through Corris Computers and Rush Computers. Visit <http://www.hsa.net> for more information.

ITS Student Computer Lab and Help Desk Information

CONTACT INFORMATION:

Telephone: 617-495-9576

Email: help@law.harvard.edu

Location: Hauser 030

Web site: <http://www.law.harvard.edu/administration/its/students>

HOURS OF OPERATION:

Student Help Desk staff is on duty during regular Lab hours.

Academic year hours of operation:

Monday- Thursday: 8:30 a.m. to 12 midnight
Friday: 8:30 a.m. to 9:00 p.m.
Saturday: 10:00 a.m. to 9:00 p.m.
Sunday: 10:00 a.m. to 12 midnight

Summer hours begin Memorial Day weekend and are:

Monday -Friday: 9:00 a.m. to 5:00 p.m.

Hours are subject to change; please check MyHLS' Administrative Updates for changes to the schedule.