

Search

Find Policy by Category

Academic Affairs

Academic Disability Accommodations

Academic Freedom Policy

Academic Transcripts

Adequate Full Time Faculty

Administrative Procedures for Research Involving Liberty University-Affiliated
Participants

Advisors

Assessments

Break in Undergraduate Enrollment

Certificate Completion Plan Audit

Certificate Completion Requirements

Certificate Enrolled Students

Certificate to Another Certificate or Degree Seeking Program

Change of Certificate

Change of Major

CITI Requirement

Class Attendance Graduate

Class Cancellation

Community Public Outreach or Service Policy

Computer Competency

Copyright Policy

Communication and Public Relations

Enrollment and Admissions

Admission on Academic Caution or Probation

Admission Requirements - Test Scores

Application for Admission - Online

Application Requirements - Homeschool Transcripts

Application Requirements - Other

Application Requirements - Transcripts

Assessment of Prospective Students

Break in Undergraduate Enrollment

Certificate to Another Certificate or Degree Seeking Program

Change of Certificate

Change of Major

Class Cancellation

Coursework At Other Institutions While Enrolled At Liberty

Credit by Examination Policy

Dropping and Adding Online Classes

Enrollment Verification

Equal Opportunity Admissions Policy

Graduate Semester Load

Health Form

International Admissions

Facilities and Auxiliary Services

LaHaye Recreation and Fitness Center Policies

Printing Services Policy

Temperature Setpoint Policy

Finance and Risk Management

Financial Aid

10.0.0.0 Financial Aid Disbursement Policy

11.1.0.0 2019-20 Financial Aid Satisfactory Academic Progress Policy

11.1.0.0 2020-21 Financial Aid Satisfactory Academic Progress Policy

12.1.0.0 2019-20 Financial Aid Withdrawal Policy

12.1.0.0 2020-21 Financial Aid Withdrawal Policy

3.2.1.0 Enrollment Levels and Types Policy

3.2.3.0 2019-20 Financial Aid Repeat Coursework Policy

3.2.3.0 2020-21 Financial Aid Repeat Coursework Policy

3.3.3.0 Federal Work Study Program Policy

3.3.4.0 Federal TEACH Grant Policy

3.5.4.0 2019-20 Financial Aid General Scholarship Rule Policy

3.5.4.0 2020-21 General Scholarship Rule Policy

3.5.5.0 Liberty Christian Academy (LCA) and Affiliate High School Scholarship Policies

4.0.0.0 Liberty University Financial Aid Consumer Information

4.1.7.1 Financial Aid General Appeal for Assistance

4.1.7.2 Institutional Scholarship Appeal Process

4.1.7.4 Virginia State Grant Appeal Policy

4.1.7.5 Federal Student Loan Appeal Process

4.1.7.7 Continuing Education Appeal

4.1.7.8 Athletic Scholarship Appeal

Governance

Board Dismissal

Board/Administration Distinction

CEO Appointment & Evaluation

Governing Board Control

Human Resources

Emeritus Emerita Status Policy

Faculty Load and Compensation for Full Time Benefited Faculty

Faculty Termination Policy

University Responsibility to Assist Faculty Professional Development

Information Services and Technology

4.1.8.0 Peer to Peer File Sharing Policy

Acceptable Use Policy

Branded and Connected IT Services

Data Storage Policy

Domain Chargebacks And Approvals

External Sharing Policy

GDPR Privacy Notice

IT Personnel Entering Residence Halls

Liberty Username

Multifactor Policy

myLU Application Privacy Policy

Password Policy

PCI Data Retention and Disposal Policy

Physical Security - Media Policy

Privacy of IT Collected Data

Program and Project Budgets

Qualtrics Usage

Remote Access Policy

Software Compliance

Software Purchases And Renewals

Libraries

[Access and Privileges Policy](#)

[Archives Policy](#)

[Borrowing Services Policy](#)

[Cataloging and Metadata Services Policy](#)

[Curriculum Library](#)

[Digital Collections Policy](#)

[Ehrhorn Law Library Use Policy](#)

[Interlibrary Loan Policy](#)

[Jerry Falwell Library Assessment Policy](#)

[Jerry Falwell Library Copyright Policy](#)

[Jerry Falwell Library Lockers Policy](#)

[Library Room Request Reservation Policy](#)

[Research Assistance Policy](#)

[Scholars Crossing Policy](#)

[Special Collections Development Policy](#)

[Technology Commons Policy](#)

Marketing and Branding

Branding Policy

Marketing Approval of Qualtrics Surveys

Marketing Policy

Photo Policy

Public Safety and Security

Liberty University Weapons Policy

Lost & Recovered Property

Mandatory Withdrawal Policy

Policy for Unmanned Aerial Systems Operations On or Over Liberty University Property

Traffic & Parking Regulations

Records

FERPA/Privacy of Information

Student Affairs

[4.1.7.10 Student Complaint Resolution Process](#)

[4.1.7.11 Online Student Complaint Reporting Policy](#)

[4.1.7.3 State Consumer Complaint Contact Information](#)

[4.1.7.6 Submitting Complaints of Fraud, Waste, and Abuse to the Office of Inspector General](#)

[4.1.7.9 Resident Complaint Reporting](#)

[4.1.8.0 Peer to Peer File Sharing Policy](#)

[Club Sports Concussion Policy](#)

[Community Boards](#)

[Complaint Policy](#)

[CSER Supervisor Policy](#)

[FERPA/Privacy of Information](#)

[HSOG Dress Code](#)

[Liberty University Discrimination, Harassment, and Sexual Misconduct Policy](#)

[Mandatory Withdrawal Policy](#)

[Off Campus Living Guide Policy](#)

[On Campus Living Guide Policy](#)

[Service and Emotional Support Assistance Animal Policy](#)

[Student Honor Code/Liberty Way Policy](#)

[Click here to view faculty-only policies](#)

Acceptable Use Policy

ISSUING OFFICE

Information Services

POLICY

Liberty University will document and communicate its standards of acceptable use of University computing resources.¹ The information systems of Liberty University are intended for the use of authorized members of the community in the conduct of their academic and administrative work. Liberty's information systems consist of all networking, computing and telecommunications wiring, equipment, networks, security devices, passwords, servers, computer systems, computers, computer laboratory equipment, workstations, Internet connection(s), electronic mail services, television and radio technologies, University-owned mobile communication devices and all other intermediary equipment, services and facilities (hereafter referred to as "information systems"). These assets are the property of the University.

Users of Liberty University computing resources are expected to review and understand the contents of this policy and its associated standards.

STANDARDS

User Rights and Responsibilities

Assent to Terms of the Acceptable Use Policy

By accessing and/or using University information systems, and/or by "clicking through" a usage agreement during sign-on to any university system, registration onto Liberty University's Network or other equipment registration procedure, users assent to the Terms and Conditions of the Acceptable Use Policy.²

Access To and Use of Systems/Normal Duration of Service

Access to and use of Liberty information systems are privileges granted by the University to faculty, staff, students and authorized third parties. Additional electronic experiences that may be offered to parents and extended populations are included under the provisions of this paragraph. The University retains sole discretion over the extent to which access privileges are granted, extended and/or revoked.

Use of Computer Accounts and Facilities

Members of the Liberty community may use only the computer accounts and facilities authorized by the University for their individual use. Use of another person's account, identity, security devices/tokens, or presentation of false or misleading information or credentials, or unauthorized use of information systems/services is prohibited.

Behavior of all users on the network will be consistent with the mission of the University, and in accordance with The Liberty Way (for resident students), The Liberty Way Online Honor Code (for Online students), Faculty Handbook (for Residential faculty), The LU Online Faculty Handbook (for Online faculty, currently under review), and The Employee Handbook (for staff).

Management of University Assigned Computers

Faculty & Staff will allow their systems to be managed via the IT Desktop Management department, to ensure their systems are kept up to date, and collect appropriate asset management data. Software discovered on managed Faculty/Staff machines that is not in compliance with this policy (such as violation of valid licensing) may be removed remotely or automatically as part of routine maintenance without notice to the user.

All 3rd party software must be properly licensed. Each user accepts personal responsibility for the legality of all software not installed by Desktop Management or approved by the IS Accounts Management & Compliance office.

Users Responsible for Actions Conducted Under their User ID(s)

Users are responsible for all use of information systems conducted under their user ID(s), and are expected to take all precautions including password security and file protection measures to prevent use of their accounts and files by unauthorized persons/entities. Sharing of passwords or other access tokens with others is prohibited. Users who disclose their passwords to third parties are solely responsible for all consequences arising from such disclosure.

Duties When Speaking in Electronic Communications

Use of University email for non-university communication is discouraged.

Posting of Personal Information/Web Pages/Other Electronic Writings

Users are responsible for the timeliness, accuracy and content/consequences of their personal information, web pages and other electronic writings. Personal information of members of the Liberty community, including, but not limited to students, faculty and staff, may not be posted or maintained on public networks or sites, unless the user fully complies with applicable laws and regulations governing handling of personal information.

Use of University-Recognized Messaging Systems

Electronic messages pertaining to the official business of the University, including all academic and administrative matters should be sent from University-owned or University-recognized messaging systems. For example, inquiries about students must be sent from an account associated with a University-recognized e-mail system. Replies from faculty or staff must be sent using the same University-recognized accounts. In cases where unrecognized third-party messaging systems are used to originate a message, and/or where a party chooses to forward messages from a University-owned or University-recognized system to a third-party unrecognized system, individuals using these systems will be solely responsible for all consequences arising from such use.

Commercial Use

University information systems may not be used for commercial purposes except only as permitted with the explicit prior written approval of the Offices of the Provost and General Counsel.

Offering, Providing, Lending or Renting Access to University Systems

Users may not offer, provide, lend, rent or sell access to University information systems. Users may not provide access to individuals outside the University community. Expansion or redistribution of Liberty's cable television services is not permitted. Personal, private or departmental switches, routers, wireless access points or DHCP-serving devices may not be connected to centrally-managed administrative network segments, except only as may be agreed to in writing between the device owner and Information Technology Services.

Compliance with Internet Service Provider Terms of Use

Internet use must comply with the Terms of Service stipulated by our Internet service provider(s). In addition, the Acceptable Use, Terms of Service and/or other policies of systems and/or electronic resources accessed through University Internet connection(s) also bind users of University Internet connections. Failure of users to comply with these Terms of Service may result in sanctions, up to and including separation from the University.

Use of Remote Resources

Users may not connect to remote resources such as a printer, file systems, or any other remote resource, regardless of location on or off the Liberty network, unless the administrator of the remote resource has first granted permission to do so.

All access to University electronic resources will occur through reasonable and customary means. For example, all electronic resources offered through a web-based experience should be accessed using a web browser only.

Electronic resources are available to faculty and staff using remote access, also known as the Virtual Private Network (VPN). The University reserves and intends to exercise its right to determine:

- who may use the VPN,
- from what locations the VPN may be accessed,
- what services and experiences are offered through the VPN,
- the extent of individual access rights when using the VPN, and
- to limit or block connections not originating from the VPN.

Exclusions to this policy provision may be made to vendors and affiliates who maintain private connections to the University network.

All users establishing a connection to the University network through the VPN or by any other means are responsible to ensure antivirus software is present on their computer, and that its protection signatures are up to date.

Irresponsible/Wasteful Use

Users may not use information systems irresponsibly, wastefully or in a manner that adversely affects the work or equipment of others at Liberty or on the Internet.

Specific Prohibitions on Use of Information Systems

- Harass, threaten, defame, slander or intimidate any individual or group;
- Generate and/or spread intolerant or hateful material, which in the sole judgment of the University is directed against any individual or group, based on race, religion, national origin, ethnicity, age, gender, marital status, sexual orientation, veteran status, genetic makeup, or disability;
- Transmit or make accessible material, which in the sole judgment of the University is offensive, violent, pornographic, annoying or harassing, including use of Liberty information systems to access and/or distribute obscene or sexually explicit material unrelated to University sanctioned work or bona fide scholarship;
- Generate unsolicited electronic mail such as chain messages, unsolicited job applications or commercial announcements;
- Generate falsely identified messages or content, including use of forged content of any description;
- Transmit or make accessible password information;
- Attempt to access information systems and/or resources for which authority has not been explicitly granted by the system owner(s);
- Capture, decipher or record user IDs, passwords, or keystrokes;
- Manipulate or tamper with uniform resource locators (URLs);
- Intercept electronic communications of any kind;
- Probe by any means the security mechanisms of any resource on the Liberty network, or on any other network through a connection to the Liberty network;
- Disclose or publish by any means the means to defeat or disable the security mechanisms of any component of a Liberty University Information System or network;
- Alter, degrade, damage or destroy data;
- Transmit computer viruses or malicious/destructive code of any description;
- Conduct illegal, deceptive or fraudulent activity;
- Obtain, use or retransmit copyrighted information without permission of the copyright holder;
- Engage in crypto-currency mining using Liberty electronic or network resources;
- Communicate in a manner that could be utilized for academic cheating;
- Place bets, wagers or operate games of chance; or
- Tax, overload, impede, interfere with, damage or degrade the normal functionality, performance or integrity of any device, service or function of Liberty information systems, content, components, or the resources of any other electronic system, network, service or property of another party, corporation, institution or organization.

The above enumeration is not all-inclusive. If there is a question as to whether a specific use is appropriate or acceptable under this policy, the University's sole determination will prevail. For additional information, contact the HelpDesk.

University Rights and Responsibilities

General Rights of the University

To protect Liberty information systems against unauthorized or improper use, and to protect authorized users from the effects of unauthorized or improper usage, the University reserves the right with or without notice, to monitor, record, limit or restrict any user account, access and/or usage of account. The University may also monitor, record, inspect, copy, remove or otherwise alter any data, file or system resources in its sole discretion. The University further reserves the right to periodically inspect systems and take any other actions necessary to protect its information systems. The University also retains access rights to all files and electronic mail on its information systems. Anyone using these systems expressly consents to such monitoring.

Right to Seize/Inspect University-Owned Computing Devices

The University reserves the right at any time, with or without prior notice or permission from the user or users of a computer or other University-owned computing device, to seize such device and/or copy or have copied, any and all information from the data storage mechanisms of such device as may be required in the sole discretion of the University in connection with investigations of possible wrongdoing or legal action. In addition to the foregoing, privately owned devices connected to the University network are also subject to inspection by authorized University personnel.

Right to Block Content

The University reserves the right to reject from the network or block electronic communications and content deemed not to be in compliance with policies governing use of University information systems.

Right to Disclosure Information

The University may disclose information, including pursuant to an internal or external investigation of alleged misconduct or wrongdoing, and may provide information to third parties, including law enforcement. By accessing Liberty information systems, users give Liberty permission to conduct each of the operations described above.

Detection of Plagiarism/Academic Dishonesty

The University reserves the right to use, and intends to use manual and/or automated means to assess materials submitted as academic work submitted electronically for indications of plagiarism or other form(s) of academic dishonesty.

Actions to be Taken When a Policy Violation is Identified

When a potential violation is identified, the appropriate system manager or unit head, the Information Security Office, and any other University employees or agents as are deemed appropriate, are authorized to investigate and initiate action in accordance with University policy. Repeated violations may result in suspension or termination of service(s). In addition, the University may require restitution for any use of information systems that violates this policy. The University may also provide evidence of possible illegal or criminal activity to law enforcement authorities.

Noncompliance to these standards will be subject to disciplinary actions outlined in the academic honor code and personal conduct that applies to them, such as The Liberty Way, Residential Graduate Honor Code and LU Online Code of Honor (for students), the Faculty Staff Handbook or the LU Online Faculty Handbook (for faculty) and/or the Employee Handbook (for staff).

Noncompliance to these standards by any guest may result in the revocation of all access to Liberty University computing resources.

Consequences of Policy Violation

Any unauthorized, inappropriate, illegal or illegitimate use of the University's information systems, or failure to comply with this policy will constitute a violation of University policy and will subject the violator to disciplinary action by the University up to and including separation of employment or relationship, and may result in legal action.

For infractions not outlined in an applicable academic honor code or personal conduct code, disciplinary actions will be at the discretion of the Office of Student Conduct (for students), the Department's Chair or Dean and/or Human Resources (for faculty) and/or the Department's manager and/or Human Resources (for staff).

Termination of Access to University Systems and Services

Notwithstanding any other provision of this policy, authorization to access the information systems and resources of Liberty University ends at the termination of employment, end of a recognized role or relationship or loss of sponsorship. Electronic mail accounts can be an exception with the understanding that all Liberty Usernames and E-mail accounts are property of Liberty University and as such Liberty University retains exclusive rights to the creation, assignment, revocation, usage and content management of all Liberty Usernames and E-mail accounts.

Confidentiality/Privacy Sections

Electronic Content Property of the University Right of University to Monitor Content

University information systems and the messages, e-mail, files attachments, graphics and Internet traffic generated through or within these systems are the property of the University. They are not the private property of any University employee, faculty, staff, contractor, student or any other person. No user of University systems should have an expectation of privacy in their electronic communications. All electronic communications, files and content presented to and/or passed on the Liberty network, including those to, from or through Internet connection(s) may be monitored, examined, saved, read, transcribed, stored or retransmitted by an authorized employee or agent of the University, in its sole discretion, with or without prior notice to the user. The University reserves and intends to exercise the right to do so. Electronic communications and content may also be examined by automated means.

Confidentiality of Content

The confidentiality of any content should not be assumed. Even when a message or material is deleted, it may still be possible to retrieve and read the message or material. Further, use of passwords for security does not guarantee confidentiality. Messages read in HTML may identify the reader to the sender. Aside from the right of the University to retrieve and read any electronic communications or content, such messages or materials must be treated as confidential by other students or employees and accessed only by the intended recipient. Without prior authorization, no person is permitted to retrieve or read electronic mail messages not sent to them.

Responsibility to Maintain Confidentiality

Notwithstanding the University's right to audit or monitor its information systems, all users are required to observe the confidentiality and privacy of others' information accessed through Liberty information systems and records of every description, including information pertaining to University programs, students, faculty, staff and affiliates. Without proper authorization, users are not permitted to retrieve or read content not intentionally addressed to them. With proper authorization, the contents of electronic mail or Internet messages or materials may be accessed, monitored, read or disclosed to others within the University or otherwise.

Electronic Privacy Right

The electronic privacy rights of others should be respected at all times. Use of audio, video, cell phone, web cam or related technologies, for the purpose of capturing images and/or recording speech in locations or circumstances where a reasonable expectation of privacy exists is prohibited without the consent of the subject(s) depicted and/or recorded. This provision should not apply to lawful surveillance conducted by law enforcement agencies. The University reserves the right to impose additional restrictions on use of electronic recording devices, in its sole discretion. Questions about the applicability of this provision to a particular situation should be referred to the Office of General Counsel or the Director of Information Security.

Handling of Sensitive Information Disposal of Equipment and Storage Media

Printed materials, computer equipment and storage media containing sensitive and/or protected information should be handled in accordance with Information Disposal Requirements, Asset Disposition procedures, and hazardous materials regulations.

No Guarantee of Protection Against Unauthorized Access

Prohibition on Accessing/Moving Data Belonging to Another Account holder

While the University attempts to protect electronic communication and files from unauthorized access, this cannot be guaranteed. Users may not access, copy or move files including, but not limited to programs, data and electronic mail belonging to another account, without prior authorization from the account holder. Files may not be moved to other computer sites without permission from the account holder whose account under which the files reside.

Compliance with Laws Sections

Requirement to Comply with Applicable Local, State and Federal Laws Concerning Use, Dissemination and Disclosures of Information

The University strives to maintain the security and privacy of electronic communications. Use of Liberty University information systems or resources, dissemination, and disclosures of information, must comply with the provisions of applicable local, state and federal laws, regulation and University policy.

Lawful Use

Liberty information systems may be used for lawful purposes only. It is prohibited to use Liberty information systems for unlawful purposes, including, but not limited to the installation of fraudulently or illegally obtained software, harmful software, illegal dissemination of licensed software, sharing of content where the disseminator does not hold lawful intellectual property rights, propagating chain messages, pyramid, ponzi, other unlawful or deceptive schemes, or for any purpose contrary to local, state, federal law or University policy.

Compliance with Copyright Law

Use of University information systems must comply with provisions of copyright law and fair use. Copyright law limits the rights of a user to decrypt, copy, edit, transmit or retransmit another's intellectual property, including written materials, images, sounds, music, and performances, even in an educational context, without permission, except where such use is in compliance with Fair Use or TEACH Act provisions.

Compliance with Export Control Regulations

Exports of computing equipment and information technologies from the University must be in compliance with US Export Control Regulations.

Notice of Right to Change Acceptable Use Policy

The University reserves the right to change this policy or any portion of the policy, at any time, with or without prior notice. Changes to this policy are effective upon posting in the University Policy Directory, where the most current version resides. The AUP was last revised on September 6, 2019. This policy replaced previous PG0017.

SCOPE

All University Students (Residential and Online), Faculty, Staff and guests who may utilize University information systems.

PURPOSE

The policy is based on the principle that the electronic information environment is provided to support University business and its mission of education, research and service. Other uses are secondary. Uses that threaten the integrity of the system; the function of nonUniversity equipment that can be accessed through the system; the privacy or actual or perceived safety of others; or that are otherwise illegal are forbidden.

By using University electronic information systems you assume personal responsibility for their appropriate use and agree to comply with this policy and other applicable Liberty University policies, as well as City, State and Federal laws and regulations.

DEFINITIONS

VPN - Virtual Private Network. Technology used for secure communication from a remote location to a network resource.

National Institute of Standards and Technology Cybersecurity Framework (NIST CSF) - Provides a policy framework of computer security guidance for how private sector organizations in the United States can access and improve their ability to prevent, detect and respond to cyber attacks

International Organization for Standardization (ISO) 27000 - Part of the system for worldwide standardization

REFERENCES

ISO/IEC 27001 2013 (More information available upon request)

8.1.3 Acceptable use of assets

NIST 800-53: [More information here](#)

PS-6 Access Agreements

[1] ?ISO 27000: 8.1.3 (Policy 020121)

[2] ?NIST 800-53 PS-6