

Legal Services Alabama Eligibility and Acceptable Use Policy

The information-technology Eligibility and Acceptable Use Policy begins with a few principles, defines several categories into which users and applications of information technology fall, and specifies which users may use LSA information technology for which applications.

Principles

Two general principles underlie eligibility and acceptable-use policies for information technology:

- LSA information technology is for LSA advocates to use for core LSA purposes.
- Any use counter to this, or which interferes with core use by others, is unacceptable.

Definitions

- **LSA Information Technology**
Any computer, networking device, telephone, copier, printer, fax machine, or other information technology which
 - is owned by LSA or
 - is licensed or leased by LSAis subject to LSA policies. In addition, any information technology which
 - connects directly to LSA data or telephone networks,
 - connects directly to a computer or other device owned or operated by LSA, and/or
 - otherwise uses or affects LSA information-technology facilitiesis subject to LSA information-technology policies, no matter who owns it.[2](#)
- **Users**
Three broad classes of potential users have different privileges:
 - *Regular Users*, who are entitled to use all or most LSA technology and services,
 - *Special Users*, who are entitled to use specific limited services for specific purposes under specific conditions, and
 - *Excluded Users*, who are not entitled to use LSA information technology.

Regular Users

In general, only current LSA employees are Regular Users. Employee status *does not extend to family members or colleagues who are not themselves Regular Users.*

Special Users

Special Users comprise certain individuals and specified classes of LSA affiliates to whom LSA provides a tightly limited subset of LSA information technologies and services. The specified special-user classes consist primarily of certain organizations affiliated with LSA and their staff. They also include certain individuals working temporarily at LSA under the explicit sponsorship of LSA .[5](#) The Information Technology manager authorizes special-user classes and individual special users, under the authority of the Director of Operations. The Director of Operations determines which individuals or organizations are responsible for use (or misuse) of information technology by Special Users and any associated costs. Special Users abide by all relevant LSA policies. In general, they reimburse LSA or pay directly for the cost of the services they receive. Special User privileges may end without notice. Special Users in a specified class retain no LSA information-technology privileges once they leave that class. Individual Special Users receive privileges only for a period specified at the outset.

Excluded Users

These are all individuals or organizations that are not Regular Users or Special Users.

- **Applications**

Here again three distinct categories are important:

- *Core* applications, those clearly associated with LSA's core advocacy mission,
- *Restricted* applications, those clearly unrelated to the LSA's core purposes, or which violate general LSA policies, jeopardize its tax-exempt or other circumstances, or otherwise interfere with core applications, and
- *Ancillary* applications, which do not fall clearly into either of the preceding two categories and which do not interfere with Core applications.

Core Applications

These support LSA advocacy mission, research, outreach and administration.

Restricted Applications

Restricted applications of LSA information technology primarily include

- those that threaten LSA's tax-exempt status, such as certain kinds of political activity and most commercial activity,
- those that are illegal, such as fraud, harassment, copyright violation, and child pornography,
- those that deprive other users of their fair share of LSA information technology or interfere with the functioning of central networks and systems, such as mass mailings, chain letters, unauthorized high-bandwidth applications, or denial-of-service attacks, and
- those that violate more general LSA policies.

Disclaimers do not render Restricted applications acceptable. The only recourse available to someone interested in such applications is to use non-LSA computers, networks, and other technologies.

Ancillary Applications

Ancillary applications are easy to list, but difficult to define. Examples are plentiful: using a LSA phone to make a dentist appointment, a LSA-connected personal computer to host small-scale personal (but non-commercial) Web pages, LSA servers to send and receive for modest amounts of personal electronic mail, a LSA fax machine to get a vacation itinerary from a travel agent, and the like. In general, Ancillary applications are those neither explicitly permitted nor explicitly restricted, and with one other essential attribute: they are invisible to other users, to network and system administrators, and to other LSA offices. Ancillary applications consume only resources that would otherwise go to waste, and never require any action or intervention by anyone at LSA other than their user. As a rule, Ancillary applications that become visible to others or burden systems are *ipso facto* no longer Ancillary, but Restricted.

Eligibility and Acceptable Use

No one may use LSA information technology for Restricted purposes without explicit written authorization from the Executive Director, who consults the Director of Operations, the Information Technology Manager, and other officials as appropriate.

Except for the preceding restriction, *Regular Users* may use the full array of LSA information technology for Core applications. Only Regular Users are eligible to use most centrally-funded technology, including help desks and technical support.

There is one major exception to Regular Users' general rights to use information technology for Core applications. *If any application of information technology, however permissible otherwise, disables computers or network services, consumes*

disproportionate enough resources that other users are denied reasonable access to information technology, or induces substantial costs outside the user's Department and/or office, then that application is Restricted.[7](#)

In general, Regular Users also may use LSA telephones, the LSA network, and personally or departmentally owned computers for Ancillary applications.[8](#) However, even Regular Users may not use information technology in ways that interfere with others,[9](#) or that consume LSA resources other than those directly under the user's control.[10](#) In general, any Ancillary use of the LSA network that becomes apparent to other users thereby becomes Restricted, and unacceptable.

Special Users may use LSA information technology only insofar as they are specifically authorized to do so.

Except for certain materials and facilities LSA explicitly makes available to the general public, *Excluded Users* may not use LSA information technology in any way.

Where definitions of user or application status are unclear, or where patterns of use appear to be out of compliance with this policy, the Director of Operations provides interpretations or direction as appropriate on behalf of the Executive Director. Where necessary, the Director of Operations consults the Executive Director, other Officers of LSA, and the Technology Planning Committee for further advice and guidance.

Roles and Responsibilities

LSA

LSA owns all of the computers and all of the internal computer networks used by LSA. LSA also has various rights to the software and information residing on, developed on, or licensed for these computers and networks. LSA administers, protects, and monitors this aggregation of computers, software, and networks. In its management of information technology, LSA and its administrative and IT department take responsibility for

- Focusing LSA information technology resources on activities connected with LSA's core advocacy mission;
- Protecting LSA networks and other shared facilities from malicious or unauthorized use;
- Ensuring that LSA computer systems do not lose important information because of hardware, software, or administrative failures or breakdowns;[11](#)
- Managing computing resources so that the LSA community are not denied fair access to them;[12](#)

- Establishing and supporting reasonable standards of security for electronic information that community members produce, use, or distribute, and ensuring the privacy and accuracy of administrative information that LSA maintains;
- Delineating the limits of privacy that can be expected in the use of networked computer resources and preserving freedom of expression over this medium without countenancing abusive or unlawful activities;
- Monitoring policies and communicate changes in policy as events or technology warrant; and
- Enforcing policies by restricting access and initiating disciplinary proceedings as appropriate.[13](#)

The Individual

LSA supports networked information resources to further its core advocacy mission. All members of LSA community must be cognizant of the rules and conventions that make these resources secure and efficient. Users of LSA information technology take responsibility for

- Using resources efficiently, and accepting limitations or restrictions on computing resources - such as storage space, time limits, or amount of resources consumed - when asked to do so by systems administrators;
- Protecting passwords and respecting security restrictions on all systems;[14](#)
- Backing up files and other data regularly;[15](#)
- Preventing unauthorized network access to or from their computers or computer accounts;[16](#)
- Recognizing the limitations to privacy afforded by electronic services;[17](#)
- Respecting the rights of others to be free from harassment or intimidation, to the same extent that this right is recognized by LSA; and
- Honoring copyright and other intellectual-property rights.

Privacy

All Legal Services Alabama users should have **no** expectation of privacy while using and/or creating content within or while connected to any LSA technology resource.

Sanctions and Procedures

When any use of information technology at LSA presents an imminent threat to other users or to LSA's technology infrastructure, system operators may take whatever steps are necessary to isolate the threat, without notice if circumstances so require. This may include changing passwords, locking files, disabling computers, or disconnecting specific

devices or entire sub-networks from LSA, regional, or national voice and data networks. System operators restore connectivity and functionality as soon as possible after they identify and neutralize the threat.

Telephones, computers, network connections, accounts, usernames, authorization codes, and passwords are issued to Regular Users and Special Users to identify them as eligible users of LSA information technology. Users are responsible for not sharing their privileges with others, and especially for ensuring that authorization codes and passwords remain confidential. Users of computers connected to the LSA network, permanently or temporarily, are responsible for ensuring that unauthorized users do not thereby gain access to the LSA network or to licensed resources.

Use of information technology that violates this Policy and rules based on it may result in disciplinary proceedings and, in some cases, in legal action. Disciplinary proceedings involving information technology are the same as those for violations of other LSA policies, and may have serious consequences. Unauthorized use of LSA information technology by Excluded Users may result in police intervention or legal action.

June 2007