Mission of ITS

To define the 21st Century learning space,
to assure universal access to that space,
for all learners to master new frontiers in
communications, information & literacy.

FILTERING:

The Children's Internet Protection Act (CIPA)

requires that we deploy a Content Filter and maintain policies that prohibit access to objectionable materials by minors using district resources. LPS conforms with this requirement on both our wired and wireless network services. However, the presence of the filter does not replace adult supervision. It is the responsibility of all LPS staff to adequately supervise access and immediately address misuse according to the student code of conduct.

All staff have the authority to override the Internet Content Filter which is a provision of CIPA. All overrides are logged and can be administratively reviewed. The following describes how:

- At the restricted access page, click "Further Options"
- Select the "Option 1" link
- Enter the same login name & password as your PC
- A pop-up will give the override command to the server
- Close all browser windows when done to end override

Wireless in LPS: what it means for you

All schools in LPS have wireless access thanks to support from the LPS Foundation and the Board of Education. When using wireless, you will discover two networks.

LPS-1 (LPS Devices)

This fully secured network uses WPA2 encryption and requires password information and database entries made by ITS. This wireless network supports district owned Windows laptops. Network access is the same as wired computers.

PODNet (Personally Owned Devices)

This fully open network does not require any security setup for connectivity. Only Filtered Internet access is available. Any web-based services will work over PODNet including Infinite Campus, Fileway, Web-Outlook etc. A splash screen appears on each connection detailing the risks associated with using PODNet. Please take the time to read the conditions before use.

Need more technology information?
Visit the Staff Intranet:

http://insidelps.littletonpublicschools.net/

- Use the logins you use for your PC
- Training videos
- Filter change requests
- Forms and recommended documents
- Access other ESC services

Littleton Public Schools
5776 South Crocker Street
Littleton, CO 80120
www.littletonpublicschools.net

Information Security Guide

Help keep information safe!

In a day and age when information is more conveniently available than ever before, it is imperative that professionals understand how to keep information appropriately secure.

Access online resources

The Children's Internet Protection Act requires that we block objectionable Internet content and that teaching staff have the ability to override school Internet content filters for bonafide purposes. Inside, we'll show you how…

Wireless access

Understand the wifi services in LPS…

Information Technology Services

Dan Maas, CIO

Mark Lindstone, Asst. Director

Mike Porter, Asst. Director

Mike Zehner, Network Manager

Information security guidelines.

INFORMATION IS POWERFUL… USE AND PROTECT IT WISELY.

The following guide is intended to provide general advice and is not exhaustive in nature. Contact ITS with questions.

Security Level	SAFEST LEVEL Access control is strictly managed by system administrators in LPS. Secure Socket Layer (SSL) encryption is in place for off-site access services.	SAFE LEVEL Access control is managed by system administrators (G:) and LPS employees (H:) on servers that LPS owns and stores. Careful rules are maintained to prevent unauthorized access. Access control precision is not as strong as the SAFEST LEVEL.	MODERATE LEVEL Access to LPS servers and archives are controlled by system administrators, but message forwarding is controlled by LPS employees and potentially others. Storage devices can be lost or stolen creating increased risk.	LOW LEVEL Third-party system administrators (non-LPS employees) manage security. Subscribers can invite and exclude individuals. LPS cannot validate or change access controls.	OPEN LEVEL No security features. Information at this level is considered published and public. Care should be given to copyright issues in this zone as students and teachers are subject to "fair use" requirements of any materials copied from other sources.
Exemplars	Infinite Campus, JD Edwards, Tranquility, MAP reporting, LARS, Central Records, IFAS	Network Shared Folders (H: and G:)	Email, Outlook functions, USB memory keys, laptops, zip drives, backup appliances	Collaborative tools including Google Docs, Gmail, private wikis, closed social networking pages, text messaging	Web sites, anonymous blogging, open wikis
Appropriate Uses	Store and share specific, uniquely identifiable information about employees and students, unauthorized release of which would violate privacy and law. Examples include grades, attendance, leave requests, disciplinary data, achievement data, special services, immunization, free and reduced lunch eligibility. Information of this type is only safe in this type of system… DO NOT save this kind of information to your hard drive or a thumb drive!	You can store and share documents that specifically pertain to employees and students. Examples include disciplinary notices, memos with names etc. H: drive folders are for your personal documents related to LPS business. G: drive folders are for collaborative document sharing among multiple LPS employees. Data is backed up on the network and strong security is in place.	Communicate with colleagues and others about issues related to LPS business. Email is subject to Open Records requests unless privacy concerns arise. Email sent outside the district is equivalent to sending a post-card. Do not include identifiable information about employees and students but you can use for coordination of activities related to employees and students. Treat an email message as if it might end up in the news media.	Store and share documents that are pertinent to the business of school activities but DO NOT specifically identify employee and/or student information that is confidential. Access to materials can be somewhat controlled but such is unverifiable by ITS staff. Use for collaboration, but realize that someone you did not intend might someday read what you place here.	Share information with the public, engage in public dialog. DO NOT use for any information that can, in any way, be deemed confidential or private. If a controversial issue arises, information of this type will almost certainly be found by the news media. Honor intellectual property and tune your activities to age-appropriate levels.

At ITS, SERVICE is the last word around here… How can we help you?

Our vision is that LPS will support the necessary technology for World-class student learning and professional practice.