# Acceptable Use Policy for Technology: All Users

*Learning must extend beyond the walls of our schools for students to compete with their peers. We must provide students with any time, anywhere access to the curriculum and the necessary tools to personalize their education.*

Leicester Public Schools (LPS) provides access to technology devices, Internet, and data systems to employees and students for educational and school-business purposes. This Acceptable Use Policy (AUP) governs all electronic activities of users accessing the district's technology, network, and data systems regardless of their physical location.

## Guiding Principles

- Online tools, including social media, should be used in our classrooms, schools, and central offices to increase community engagement, staff, and student learning, and core operational efficiency.
- LPS has a legal and moral obligation to protect the personal data of our students, families, and staff.
- LPS should provide a baseline set of policies and structures to allow schools to implement technology in ways that meet the needs of their students and fulfill district goals.
- All students, families, and staff should know their rights and responsibilities outlined in the Acceptable Use Policy and government regulations.
- Nothing in this policy shall be read to limit an individual's constitutional rights to freedom of speech or expression or to restrict an employee's ability to engage in concerted, protected activity with fellow employees regarding the terms and conditions of their employment.

## Student Responsible Use

Links to a Student-Friendly Acceptable Use Policy, as well as this document, are distributed to all students at the beginning of the school year in their student handbooks. The Acceptable Use Policy for Technology must be completed and signed by all students and their parents/guardians after going over the AUP together. Staff members should make themselves aware of the contents of this document, and assist students in adhering to the policy while using technology resources in the classroom.

## Compliance Requirement for Employees

The Acceptable Use Policy is reviewed and updated annually. Employees are required to verify that they have read and agree to abide by the policy.

## Online Communications/Social Media & Confidentiality

Employees and students are provided with district email accounts and online tools to improve the efficiency and effectiveness of communication, both within the organization and with the broader community. Communication should be consistent with professional practices used for all correspondence. When using online tools and sharing information, use appropriate behavior:

- When acting as a representative or employee of the Leicester Public Schools.
- When the communication impacts or is likely to impact the classroom or working environment in the Leicester Public Schools.
- When the information has not yet been made public by the Superintendent, or their designee.

All communication sent by an employee using district property or regarding district business could be subjected to public access requests submitted through the Freedom of Information Act (FOIA). Users need to be aware that data and other material/files maintained on the school district's systems may be subject to review,

disclosure, or discovery. Use of personal email accounts and communication tools to conduct school business is strongly discouraged and may open an individual's personal account to be subject to FOIA inquiries. LPS will cooperate fully with local, state, and federal authorities in any investigation concerning or related to any illegal activities or activities not in compliance with school district policies or government regulations.

Web announcements and online communication promoting a business are prohibited. The Superintendent's Office may make exceptions if benefits are judged sufficient to merit an exception. An "opt-in" email group called "The Water Cooler" may be used to promote items such as but not limited to yard sales, concerts, and non-LPS fundraisers. Staff members that use this tool are expected to maintain professionalism.

- Communication with students should not include the content of a personal nature.
- Whenever possible, use established, educational systems such as district email, Google Classroom, and Remind.
- Contact students collectively, rather than individually. All voice and digital communications by coaches/advisors/chaperones, etc... with team members/student groups shall be sent to all members of the group, except for messages concerning medical or academic privacy matters, in which case the messages will be copied to the school principal.
- When communicating with parents/guardians of students, employees should use email addresses and phone numbers listed in the Student Information System (SIS) unless steps have been taken to verify that the communication is occurring with a parent/guardian that has educational rights for the student.
- When communicating with a parent/guardian, refrain from discussing any non-related students when possible.
- Employees who use internal or external social media (Facebook, Twitter, etc.) are expected to refrain from discussing confidential information and/or discussing specific students. Information that can be traced back to a specific student or could allow a student to be publicly identified should not be posted on any social media sites.
- When using social media, employees are expected to refrain from posting any negative comments online about students, school groups or colleagues that could have a detrimental impact on the educational community.
- Employees are required to notify their principal before setting up an online site to facilitate student learning that is outside of established educational tools. Employees are encouraged to monitor/moderate online communication to the best of their abilities. Staff members will only use their district assigned email address to set up any digital tools being used for communication with students, or facilitation of the educational process. The district reserves the right to terminate and/or seize these accounts at any time.
- Employees will not accept or initiate friend requests with current LPS students or their parents/guardians on personal networking sites. Once students have graduated, they are no longer "current" students. It is understood that many LPS staff members have children and/or relatives as current LPS students, and may want to interact with them and their "friends" on social networking sites. On these occasions, LPS staff are expected to maintain professionalism.

## Use of Copyrighted Materials

Violations of copyright law that occur while using the LPS network or other resources are prohibited and have the potential to create liability for the district as well as for the individual. LPS staff and students must comply with regulations on copyright plagiarism that govern the use of material accessed through the LPS network. Users will refrain from using materials obtained online without requesting permission from the owner if the use of the material has the potential of being considered copyright infringement. LPS will cooperate with copyright protection agencies investigating copyright infringement by users of the computer systems and network of the Leicester Public Schools.

## Network Usage, Filtering & Monitoring

Network access and bandwidth are provided to schools for academic and operational services. LPS reserves the right to prioritize network bandwidth and limit certain network activities that are negatively impacting academic

and operational services. Users are prohibited from using the LPS network to access content that is inappropriate or illegal, including but not limited to content that is pornographic, obscene, illegal, or promotes violence.

As required in the Children's Internet Protection Act (CIPA), LPS is required to protect students from online threats, block access to inappropriate content, and monitor the Internet use by minors on school networks. OIIT is responsible for managing the district's Internet filter and will work with the LPS community to ensure the filter meets the academic and operational needs of each school while protecting minors from inappropriate content.
By authorizing the use of technology resources, LPS does not relinquish control over materials on the systems or contained in files on the systems. There is no expectation of privacy related to information stored or transmitted over the LPS network or in LPS systems. LPS reserves the right to access, review, copy, store, or delete any files (unless other restrictions apply) stored on LPS computers and all employee and students communication using the LPS network. Electronic messages and files stored on LPS computers or transmitted using LPS systems may be treated like any other school property. District administrators and network personnel may review files and messages to maintain system integrity and, if necessary, to ensure that users are acting responsibly.

## Personal Use of the Network, Devices, & Storage

LPS recognizes that users may use LPS email, devices, and network bandwidth for limited personal use; however, personal use should not interfere with or impede district business and/or cause an additional financial burden on the district. Excessive use or abuse of these privileges can be deemed in violation of the AUP.

Classroom use of personal wireless electronic devices such as laptops, iPads, and cell phones are permitted and encouraged. All personal devices may only connect to the guest network. No staff member shall connect a wired device such as a router, access point, or computer to the network without the prior approval of the district technology staff. Additionally, personal printers in classrooms or offices are prohibited. LPS is not responsible for the maintenance and security of personal electronic devices and assumes no responsibility for loss, theft, or damage. The district reserves the right to enforce security measures on personal devices and remove devices found to be in violation of the AUP, when used to access LPS systems.

LPS will provide an appropriate amount of cloud-based storage for all of its users. This should be the primary location for users to save data. If a staff member chooses to use personal local media such as USB devices, hard drives, CDs, flash drives, etc, they should be backed up to the cloud frequently, and is the responsibility of the user. Student information, such as IEP's, grades, and personally identifiable information should never be transferred or saved to a personal local media device or a personal (non-LPS) cloud storage system.

## Network Security

The LPS Wide Area Network (WAN) infrastructure, as well as the building-based Local Area Networks (LANs) are implemented with performance planning and appropriate security measures in mind. Modifications to an individual building network infrastructure and/or use will affect LAN performance and will reduce the efficiency of the WAN. For this reason, any additional network electronics including, but not limited to, switches, routers, and wireless access points must be approved, purchased, installed, and configured solely by our staff to ensure the safety and efficiency of the network. Users are prohibited from altering or bypassing security measures on electronic devices, network equipment, and other software/online security measures without the written consent of the Technology Director.

## Data & Systems Access by Non-employees

Access to view, edit, or share personal data on students and employees maintained by LPS by persons acting for the district must abide by local, state, and federal regulations, including the Family Educational Rights and Privacy Act. Student and staff data will only be shared with individuals, where it is deemed necessary for the person to work on behalf of the district. To maintain ongoing access to data through LPS systems persons may be required to have a designated LPS staff member who will act as a "sponsor" to ensure the safety of the data.

## Passwords & Security

Users are required to adhere to password requirements set forth by the Leicester Public Schools when logging into school computers, networks, and online systems. Users are not authorized to share their passwords and must use extra caution to avoid email scams that request passwords or other personal information.

Staff members are expected to be security conscious when accessing district systems such as email. Be suspicious of spam or phishing attempts that require a user to click on links or to provide any account information. Note: users are advised to report any suspicious requests for account information directly to the district technology staff.

## Personally Identifiable Information (PII) and Data Security

LPS is committed to helping teachers, students and parents better safeguard PII and all student data at all levels. FERPA does not require specific security controls, but it does require the use of "reasonable methods" to safeguard student records and data. LPS, and its systems comply with all federal and state laws that govern PII and Data Security.

> **Freedom of Information Act (FOIA) -** The FOIA allows for the release of government documents at the request of an individual. A FOIA request can be made to the Leicester Public Schools for electronic documents/communications stored or transmitted through district systems unless that information could be detrimental to governmental or personal interests.
> http://www.foia.gov/
>
> **Family Educational Rights and Privacy Act (FERPA) -** The FERPA law protects the privacy, accuracy, and release of information for students and families of the Leicester Public Schools. Personal information stored or transmitted by agents of the Leicester Public Schools must abide by FERPA laws and the LPS is required to protect the integrity and security of student and family information. For more information, visit http://www.ed.gov/policy/gen/guid/fpco/ferpa/index.html
>
> **Children's Internet Protection Act (CIPA) -** Requires schools that receive federal funding through the E-Rate program to protect students from content deemed harmful or inappropriate. The Leicester Public Schools is required to filter internet access for inappropriate content, monitor the internet usage of minors, and provide education to students and staff on safe and appropriate online behavior.
> https://www.fcc.gov/consumers/guides/childrens-internet-protection-act
>
> **Children's Online Privacy Protection (COPPA) -** Spells out what operators of websites and online services must do to protect children's privacy and safety online. COPPA requires websites and online services to establish and maintain reasonable procedures to protect the confidentiality, security, and integrity of personal information collected from children.
> https://www.ftc.gov/tips-advice/business-center/privacy-and-security/children's-privacy

The technology department will supply a list of screened and approved learning applications, and publish them on the technology department webpage here: http://lpsma.net/departments/technology. It is understood that most approved applications used will collect a reasonable amount of PII, such as first and last name, and email address of the user. It is the staff members' responsibility to notify parents, and provide a link to the privacy policy of any application (not on this list) that they use in the classroom that has age requirements, collects PII, or requires an account/log in to access. District-owned and licensed curricular resources such as digital textbooks and learning platforms are exempt from this requirement.
Browser extensions in grades PK-8, will be disallowed, except for the ones on the pre-approved list. Extensions used in grades 9-12 and by staff members will also need to meet a standard for data security, but may or may not

be prescreened prior to use. Students and staff members should be aware of the amount of PII they share with browser extensions.

### Device Support & Energy Management

LPS provides basic installation, synchronization, and software support for LPS-issued electronic devices. Devices must be connected to the LPS network on a regular basis to receive up-to-date software and antivirus updates and for inventory purposes and to reduce loss or theft.

LPS strives to reduce our environmental footprint by pursuing energy conservation efforts and practices. The district reserves the right to adjust power-saving settings on electronics to reduce the energy consumption and reduce the cost to the district of the devices used. In certain circumstances, the use of personal devices and products may not be allowed, due to energy concerns.

### Termination, Transfer, & Return of Electronic Devices

Any and all equipment assigned to employees or students must be returned prior to leaving their position in the district or at the request of the district technology staff. All equipment must be returned directly to building administration, or the district technology staff. A copy of data saved in district systems such as email, and cloud-based storage, may be transferred to a secondary account, prior to the termination date with the approval of the district technology staff. LPS will maintain a copy of all digital communications and documents saved in district cloud-based storage systems for compliance with state and federal laws.

### Consequences of Breach of Policy

Use of LPS technology resources is a privilege, not a right. By using LPS systems, devices, and networks, the user agrees to follow all regulations, policies, and guidelines outlined in this policy. Students and staff are encouraged to report misuse or breach of protocols to the appropriate personnel. Abuse of these privileges may result in one or more of the following consequences:

- Suspension or cancellation of use or access privileges.
- Payments for damages or repairs.
- Discipline under appropriate LPS policies, up to and including termination of employment, subject to any collective bargaining obligations.
- Liability under applicable civil or criminal laws.

Leicester Acceptable Use Policy - All Users
Leicester Acceptable Use Policy - Student Friendly Language
Chromebook Care and Use Guide