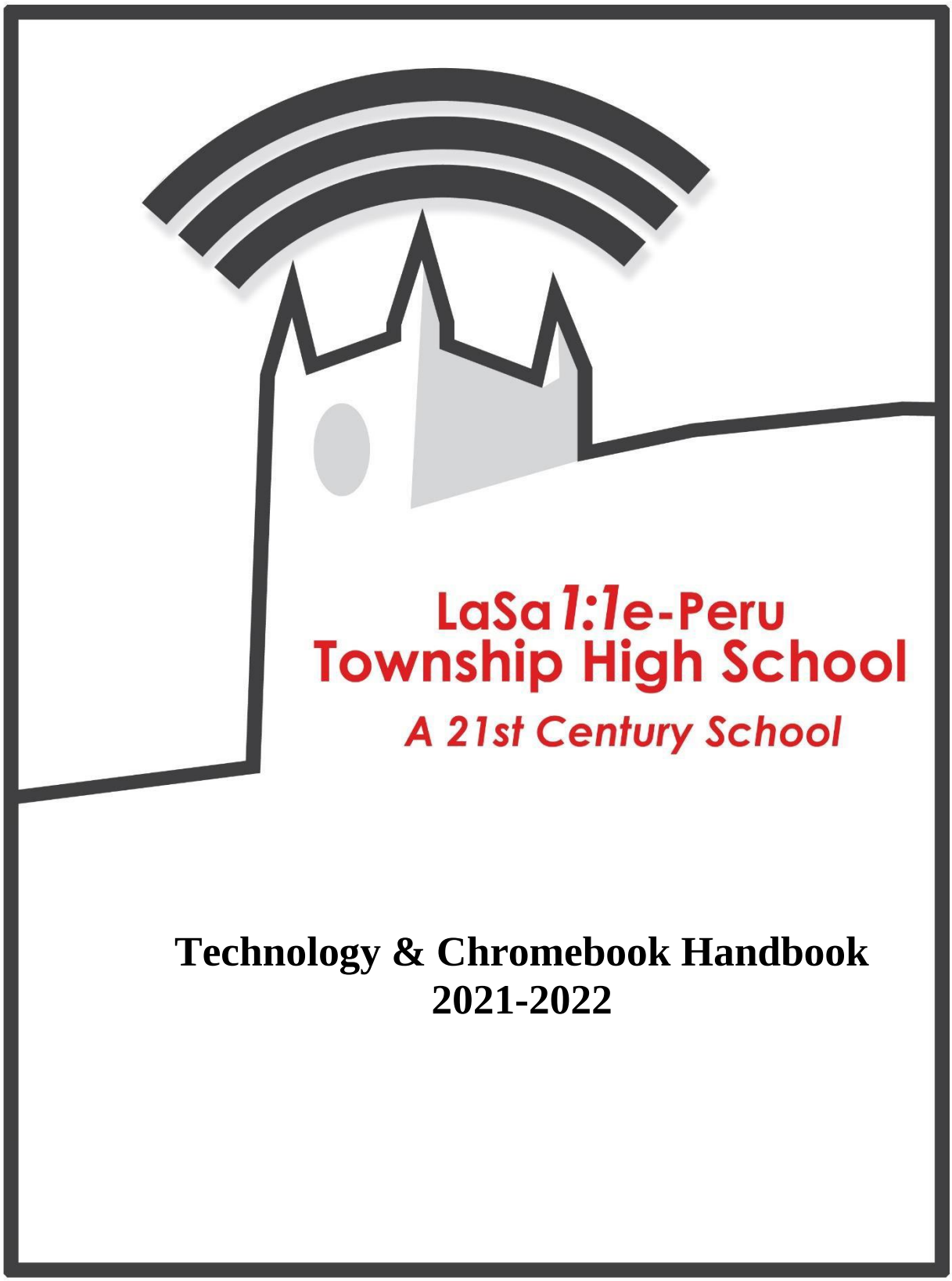

Technology & Chromebook Handbook
2021-2022

Contents

Overview – Vision

The LaSalle-Peru Township High School, District #120 (LPHS) recognizes that access to technology resources in the school, home, and community settings provide students with greater and more frequent opportunities to learn, engage, communicate, and develop the necessary skills to be career and college-ready in the 21st century. LPHS is committed to revitalizing the curriculum into a technological format that builds and sustains an engaged and collaborative learning environment for all students. A structured digital environment that is safe yet demanding will enable and support students and teachers as they explore transformative uses of technology.

Use of Technology

All students will be issued a Chromebook for educational use. With this privilege and the extraordinary opportunity to explore digital resources comes responsibilities for each student and his/her parents/guardians. This handbook provides students and their parents/guardians with information about the general use of available technologies, "ownership," rights and responsibilities for use of school devices including the Chromebook, for possession of the Chromebook, care of the Chromebook, and expectations as a digital citizen. Along with the efforts of parents/guardians, LPHS will follow its policies in maintaining an environment that promotes ethical and responsible conduct in all electronic resource activities and uses.

During the registration process, each school year, all students and their respective parents/guardians must agree to all policies listed in this handbook to receive and utilize a Chromebook, access to the LPHS network, and all other District-owned technology-related devices.

Failure to follow the terms of the policies will result in disciplinary action, including but not limited to confiscation of any Chromebook and accessories lent to the student and revocation of student access to LPHS technology, as well as any other disciplinary action deemed appropriate by LPHS administration.

Ownership

LPHS retains sole right of possession and ownership of the Chromebook (Device) and all other District-owned technology-related devices and grants permission to the student to use the device according to the rules and guidelines outlined in this document and the **Student Authorization for Electronic Network Access & Acceptable Use Policy # 6:235**. The Chromebook is not the property of the student. LPHS loans the Chromebook to the student only for educational purposes during the academic year. The student will be held responsible for the proper care of the Chromebook and accessories. LPHS reserves the right to monitor and log students' use of the District's technology and network and to examine user (student) files and materials as necessary. Moreover, LPHS administrative staff retains the right to collect and inspect the Device at any time, including via electronic remote access; and to alter, add, or delete installed software or hardware. There is no reasonable expectation of privacy while using LPHS computers, networks, or technology.

Chromebook Distribution

The student will be issued a Chromebook, a protective carrying case, and power adapter at the time of walk-in registration. Students not attending walk-in registration will pick up a Chromebook from the Technology Help Desk upon completing the registration process with the school registrar. Both the student and their parent/guardian MUST sign & agree to the terms and conditions outlined in this Technology Handbook at the time of registration. Chromebooks will be collected at the end of each school year, and students will retain their original Chromebook each year while enrolled at LPHS. At his time, Students are not allowed to bring a personal Chromebook or laptop to use during classroom instruction and learning.

Chromebook Collection & Related Fees

End of Year- The student's Chromebook, protective carrying case, and power adapter will be collected at the end of each school year for maintenance, inspection, cleaning and software updates. The District will set a Chromebook Collection Day. If a Chromebook and accessories are not returned, damaged or defaced, the student will be charged a replacement fee. If the fee is not paid at the time the Chromebook and accessories are collected, it will be applied to the student's following school years registration fee.

Transfer out of District- Any student who transfers out of District during the school year will be required to return their Chromebook protective carrying case, and or power adapter. If a Chromebook and accessories are not returned, damaged or defaced, the student will be charged a replacement fee respectively. The parent/guardian will be held responsible for payment in full. If payment is not received, the parent/guardian may be turned over to a collection agency. The District may also file a report of stolen property with the local law enforcement agency.

Chromebook Warranty and Repair Costs

The Chromebook has a limited warranty covering normal use, mechanical breakdown or faulty construction. The limited warranty only covers the Chromebook; it does not include coverage for the accessories, which include the work-in carrying case and the power adapter & cord.

- If the Chromebook is accidentally damaged, the first incident will be repaired by the District at no cost to the student or family. Subsequent damage to the Chromebook after the first documented incident will result in the student being charged 100% of the repair cost.
- The warranty does NOT cover intentional misuse, abuse, or neglect of the Chromebook and accessories. If the student does not exercise proper care, and this negligence results in damage to or loss of the Chromebook and or accessories, he/she may be subject to discipline, and 100% of the cost of the repair or replacement will be the responsibility of the parent/student.
- The parent/student must pay the repair or replacement cost for the first required payment before the Chromebook is repaired and returned to the student. The parent/student may set up a payment plan with the school to clear bills if needed.
- It will be the right of the building principal, technology director or his/her designee to determine if damages were due to negligence or accidental.
- The administration will review all damages determined to be from negligence and will assess whether or not the student has continued privilege of taking the Chromebook to and from School.
- The District will not be obligated to replace a student Chromebook in the case of intentional damage, negligence or repeat incidents.

Repair/Replacement Costs - *Costs are estimates and subject to change without prior written notice.*

Motherboard	$150.00
Screen repair or replacement	$ 50.00
Battery	$ 50.00
Palm rest with Keyboard & Touchpad	$ 50.00
LCD Bezel	$ 20.00
Top or bottom cover	$ 15.00
Camera or wireless adapter	$ 15.00
Power adapter with cord replacement	$ 30.00
Miscellaneous plastics & cables	$ 7.00-$20.00
Work-in carrying case	$ 25.00
Asset & Inventory tag replacement	$ 15.00
Chromebook	$ 280.00

Lost or Stolen Equipment

If any equipment is lost, the student or parent/guardian must report the loss to the school immediately. Reports should be filed with the Security Office. The circumstances of each situation involving lost equipment will be investigated individually. Students may be billed for lost equipment.

If the equipment is stolen, a police report must be filed, and a copy of the report must be provided to the school by the student or parent/guardian promptly. If there is not clear evidence of theft or the equipment has been stolen due to student negligence, the student and parent/guardian will be responsible for the full cost of replacement.

The District may use its discretion to replace a student Chromebook if and only if it is determined by the District that the student acted in a reasonable manner when storing and taking care of the Chromebook. And that the student acted in good faith to find the Chromebook, such as filing a police report and reporting the loss or theft to the District. The District will not be obligated to replace a student Chromebook in the case of negligence and failure to use diligence with District property.

Asset Tags

An asset tag is a barcode-like sticker placed on the device for inventory and monitoring purposes.

- All Chromebooks have an inventory tag and asset tag.
- Tags may not be modified or tampered with in any way.
- A student may be charged up to the full replacement cost of a Chromebook for tampering with a school asset tag logo or turning in a Chromebook without a school asset tag.

Discipline/Violations

The use of any technology is a privilege and not a right. Students are expected to use technologies in accordance with the classroom rules set by the teacher; this Handbook which includes Board Policy 6:235 Student Authorization for Electronic Network Access and Acceptable Use Policy; and, any applicable local, state, and federal laws. Violations of these policies will result in disciplinary action, subject to the consequences outlined in Board Policy 6:235 and repossession of the Chromebook and its accessories. Administration may also refer the matter to law enforcement if the violation involves an illegal activity.

Classroom Intervention - For low-level violations, classroom interventions will be the first level of discipline. This includes, but is not limited to, verbal warnings, seating changes, loss of privilege to use the device during the class period, teacher contact with home, and any other intervention deemed appropriate for the violation(s). Documentation of these infractions along with intervention attempts will be recorded by the classroom teacher.

Progressive Discipline - Discipline will be imposed on an escalating scale ranging from a verbal warning to a possible expulsion based on the number of previous violations and the nature of or circumstances surrounding a particular violation. If multiple offenses occur, a student may lose his/her computer privilege for a designated length of time or on a permanent basis. Progressive discipline will be handled by the administration after referral from classroom teachers, School Resource Officer, computer services, or administration.

Student Responsibilities

The rules and regulations are provided here so that students and parents/guardians are aware of the responsibilities students accept when they use a district-owned Device. In general, use of technology requires efficient, ethical, and legal utilization of all digital resources. ***Violations of these rules and guidelines will result in disciplinary action.***

The student will assume responsibility for the following.

1. **Bringing the Chromebook to School**

a. Students must bring their Chromebook to school every day that classes are in session.
b. Students hold and maintain responsibility for ensuring their Device is charged before school each day. Students who leave their Chromebook at home will not be issued another device for that day, and they are responsible for all missed activities and assignments due to lack of a Device.
c. Students may bring a wireless mouse if preferred and earbuds/headphones as needed. The District assumes no responsibility for the provision or maintenance of these personal items.

2. Carrying Chromebooks in a Safe and Secure Manner

a. Transport the Chromebook in the carrying case provided by LPHS at all times.
b. The Chromebook should not be put in another bag for transport, i.e. backpack, athletic bag, etc.
c. Transporting Chromebooks with care and with the screen closed.
d. Never lift Chromebooks by the screen.

3. **Chromebook Securit**y

a. When not in the student's possession, the Chromebook and its accessories are required to be locked in the student's school-issued locker.
b. Under no circumstances should Chromebooks or accessories be left in unsupervised areas. Unsupervised areas include the bathrooms, cafeteria, computer labs, hallways, Library/Media Center, unlocked classrooms, unlocked locker rooms, or any other area deemed insecure. Any Chromebook left in these areas is in danger of being stolen or tampered with by unauthorized individuals. If a Chromebook is found in an unsupervised area, it should be taken immediately to the Tech Center located in the Library.
c. The Chromebook is not allowed in the cafeterias when food or drink is being served.

4. **General Care** - The student is responsible for ensuring the following precautions:

a. Never leaving the Chromebook unattended.
b. Never loaning the Chromebook or its accessories to another student.
c. Keeping the Chromebook on a flat, solid surface so air can circulate. (Using a device directly on a bed or carpet can cause damage due to overheating.)
d. Never setting books or stack heavy objects on top of the Chromebook.
e. Never setting food or drink next to Chromebooks.
f. Never leaving the Device exposed to direct sunlight, extreme temperatures, or moisture sources for extended periods of time.
g. Always carefully inserting cords, cables, and removable storage devices into the Chromebook.
h. Never defacing the Chromebook and its accessories through use of writing, drawing, stickers, labels, or by any other means.
i. Never using the Chromebook to charge a cell phone.
j. Always charge the Chromebook with the issued power adapter. Charging with the wrong power adapter will damage the battery.

5. Screen Care

The Chromebook screen can be damaged if subjected to heavy objects, rough treatment, some cleaning solvents, and other liquids. The screens are particularly sensitive to damage from excessive pressure, heat, and light. The student is responsible for ensuring the following screen precautions:

- Never putting pressure on the top of a Chromebook when it is closed.
- Never storing a Chromebook with the screen open.
- Always making sure there is nothing on the keyboard before closing the lid (e.g. pens, pencils, or disks).
- Only clean the screen with a soft, dry microfiber cloth or anti-static cloth.

6. Chromebook Problems/Repair

If the device is not working properly, the student needs to take the device to the Tech Center located in the Library.

The student is responsible for ensuring the following:

- The student will never attempt to repair or reconfigure the device.
- The student will not attempt to open or tamper with the internal components of the device; nor should the student remove any screws; doing so will render the warranty void.
- The student and parent/guardian will NEVER take school-owned Chromebooks to an outside computer service for any repairs or maintenance.

7. Appropriate Classroom, Library, and Study Hall Routines

When at school the student will use the Chromebook and/or any of the school's technology equipment strictly for educational purposes. Using the Chromebook for recreational use during class time, while in the Library, or during study hall periods is prohibited. Students are expected to participate fully in all classroom activities as directed by their teacher. In addition to the rules and guidelines set in this handbook, students must abide by all rules and guidelines set by the classroom teacher. Violation of this responsibility will result in disciplinary action.

Student Accessibility

1. Logging into a Chromebook

- The student will log into their Chromebooks using their school issued *Google Apps for Education* account.
- The student will never share account passwords with other students.

2. Managing and Saving Digital Work with a Chromebook

- The majority of student work will be stored in cloud-based applications and can be accessed from any computer with an Internet connection and most mobile devices.
- The student may elect to store a small number of files on the Chromebook's hard drive.
- The student should always remember to save frequently when working on digital media. Not all Google tools/apps automatically update.
- The school will not be responsible for the loss of any student work.
- The District strongly encourages the student to maintain backups of important work on a portable storage device or by having multiple copies stored in different Internet storage solutions.
- When using G Suite for Education or Office 365 the student will use language that is considered appropriate and polite. The student will not submit, post, publish, or share any defamatory, inaccurate, abusive, obscene, profane, sexually oriented, threatening, racially offensive, harassing, or illegal material. Violation of this responsibility will result in disciplinary action.

3. Listening to Music

- The sound must be muted at all times unless permission is obtained from a teacher.
- Headphones/earbuds may be used at the discretion of the teachers.
- Students should have their personal set of headphones for sanitary reasons.

4. Watching Movies

- Watching movies on a Chromebook is not allowed during school hours unless permission from the teacher has been provided to complete a school assignment.

5. Webcams

- Webcams are to be used for educational purposes only, as determined under the direction of a teacher.

6. Gaming

- Online gaming is not allowed during school hours unless the student has been given permission by a teacher to complete a school assignment.

7. **Backgrounds and Themes**
    - Inappropriate media may not be used as backgrounds or themes. The presence of guns, weapons, pornographic materials, inappropriate language, alcohol, drugs, gang-related symbols, or any other content deemed inappropriate by the administration will result in disciplinary actions.

8. **Printing**
    - Students will be encouraged to publish digitally and share their work with their teachers and peers when appropriate.
    - Students may print using their Chromebook to the Library printer.

9. **Chrome Web Apps and Extensions**
    - Students are allowed to install District approved Chrome web apps and extensions from the Chrome Web Store or School Chrome Library.
    - Students are responsible for the web apps and extensions they install on their Chromebooks. The downloading of inappropriate material will result in disciplinary action.

10. **Using Your Chromebook & Account Outside of School**

Students are encouraged to use their Chromebooks at home and other locations outside of school.A Wi-Fi connection will be required for the majority of Chromebook use. However, some applications can be used while not connected to the internet. Students are bound by the LPHS **Student Authorization for Electronic Network Access & Acceptable Use Policy # 6:235** and all other guidelines in this document whenever they use their Chromebook outside of school.

Internet Safety & Content Filter

The District utilizes two forms of web and content filtering to maintain a safe and appropriate digital space for our students. The District's Internet access has a filtering device called iBoss that blocks entry to visual depictions that are (1) obscene, (2) pornographic, or (3) harmful or inappropriate for students, as defined by the Children's Internet Protection Act, HIPAA regulations and as determined by the district personnel. A second program used is Gaggle, which ensures the safety of students when utilizing Microsoft's O365 & Google's G Suite. Gaggle will notify the proper personnel when there is questionable and suspicious content in the online file storage, inbound and outbound email attachments, and links to websites.

Parent/Guardian Responsibilities

LaSalle-Peru Township High School, District #120 makes every effort to equip parents/guardians with the necessary tools and information to ensure the safe use of the Chromebooks in the home and community. There are several responsibilities assumed by the parent/guardian, which are outlined below:

1. **Sign the Student/Parent Technology Agreement**
   In order for students to be issued a Chromebook, a student, and his/her respective parent/guardian must sign the *Student/Parent Technology Agreement*.

2. **Attend a Student/Parent Chromebook Orientation**
   In order for students to be issued a Chromebook, a parent/guardian must attend a Student and Parent/Guardian Training.

3. **Accept Liability**
   The parent/guardian and student are responsible for the cost of repair or replacement at the date of loss if the property is any of the following:
    - Not returned
    - Intentionally damaged

- Lost because of negligence
- Stolen, but not reported to school and police in a timely manner

4. Monitor Student Use

The parent/guardian must agree to monitor student use at home and in any setting that is not the school. The best way to keep a student safe and on-task is through parent/guardian presence and continuous involvement, which can be done by completion of the following actions:

- Investigate and apply parental controls available through the home's Internet service provider and wireless router.
- Develop a set of rules/expectations for Chromebook use at home and in the community. Some websites provide parent/child agreements for you to sign.
- Only allow Chromebook use in common rooms of the home (e.g. living room or kitchen) and not in bedrooms.
- Demonstrate a genuine interest in what the student is doing on the Chromebook. Ask questions and request that they show you his/her work often.

5. Support Internet Safety & Etiquette

Internet safety is about helping your child use the Internet productively and practice safe responsible online behavior. The following are a few basic guidelines to share with your child:

- Follow your family's rules about when and where to use the Internet.
- Be polite, kind, and respectful in all digital forums and whenever accessing technology.
- Understand a website's rules, and know how to flag other users for misbehavior.
- Recognize "red flags," including someone asking personal questions such as your name and address. Encourage your child never to share his/her name, the school's name, his/her age, his/her phone number, or his/her email or home address with strangers.
- Never send pictures to strangers.
- Keep passwords private (except from parents, school technology staff, and school administrators).
- Never open a message from a stranger; it may contain a virus that can harm a computer.
- Immediately tell an adult if something makes you feel uncomfortable or suspicious happens.
- Visit *Common Sense Education Connecting Families* a website designed to support and empower families in raising kids who think critically, participate responsibly, and behave ethically in their online lives.

Annual Notice to Parents about Educational Technology Vendors Under the Student Online Personal Protection - SOPPA

School districts throughout the State of Illinois contract with different educational technology vendors for beneficial K-12 purposes such as providing personalized learning and innovative educational technologies and increasing efficiency in school operations.

Under Illinois' Student Online Personal Protection Act, or SOPPA (105 ILCS 85/), educational technology vendors and other entities that operate Internet websites, online services, online applications, or mobile applications that are designed, marketed, and primarily used for K-12 school purposes are referred to in SOPPA as *operators*. SOPPA is intended to ensure that student data collected by operators is protected, and it requires those vendors, as well as school districts and the Ill. State Board of Education, to take a number of actions to protect online student data.

Depending upon the particular educational technology being used, our District may need to collect different types of student data, which is then shared with educational technology vendors through their online sites, services, and/or applications. Under SOPPA, educational technology vendors are prohibited from selling or renting a student's information or from engaging in targeted advertising using a student's information. Such vendors may only disclose student data for K-12 school purposes and other limited purposes permitted under the law.

In general terms, the types of student data that may be collected and shared include personally identifiable information (PII) about students or information that can be linked to PII about students, such as:

- Basic identifying information, including student or parent/guardian name and student or parent/guardian contact information, username/password, student ID number
- Demographic information
- Enrollment information
- Assessment data, grades, and transcripts
- Attendance and class schedule
- Academic/extracurricular activities
- Special indicators (e.g., disability information, English language learner, free/reduced meals or homeless/foster care status)
- Conduct/behavioral data
- Health information
- Food purchases
- Transportation information
- In-application performance data
- Student-generated work
- Online communications
- Application metadata and application use statistics
- Permanent and temporary school student record information

Operators may collect and use student data only for K-12 purposes, which are purposes that aid in the administration of school activities, such as:

- Instruction in the classroom or at home (including remote learning)
- Administrative activities
- Collaboration between students, school personnel, and/or parents/guardians
- Other activities that are for the use and benefit of the school district

Educational technologies used in the District shall further the objectives of the District's educational program, as set forth in Board policy 6:10, *Educational Philosophy and Objectives*, align with the curriculum criteria in policy 6:40, *Curriculum Development*, and/or support efficient District operations. The Superintendent shall ensure that the use of educational technologies in the District meets the above criteria.

The District and/or vendors under its control may need to collect and maintain data that personally identifies students in order to use certain educational technologies for the benefit of student learning or District operations.

Federal and State law govern the protection of student data, including school student records and/or *covered information*. The sale, rental, lease, or trading of any school student records or covered information by the District is prohibited. Protecting such information is important for legal compliance, District operations, and maintaining the trust of District stakeholders, including parents, students and staff.

Definitions

Covered information means personally identifiable information (PII) or information linked to PII in any media or format that is not publicly available and is any of the following: (1) created by or provided to an operator by a student or the student's parent/guardian in the course of the student's or parent/guardian's use of the operator's site, service or application; (2) created by or provided to an operator by an employee or agent of the District; or (3) gathered by an operator through the operation of its site, service, or application.

Operators are entities (such as educational technology vendors) that operate Internet websites, online services, online applications, or mobile applications that are designed, marketed, and primarily used for K-12 school purposes.

Breach means the unauthorized acquisition of computerized data that compromises the security, confidentiality or integrity of covered information maintained by an operator or the District.

Operator Contracts

The Superintendent or designee designates which District employees are authorized to enter into written agreements with operators for those contracts that do not require separate Board approval. Contracts between the Board and operators shall be entered into in accordance with State law and Board policy 4:60, *Purchases and Contracts,* and shall include any specific provisions required by State law.

Security Standards

The Superintendent or designee shall ensure the District implements and maintains reasonable security procedures and practices that otherwise meet or exceed industry standards designed to protect covered information from unauthorized access, destruction, use, modification, or disclosure. In the event the District receives notice from an operator of a breach or has determined a breach has occurred, the Superintendent or designee shall also ensure that the District provides any breach notifications required by State law.

LaSalle-Peru Township High School, District #120
Student Authorization for Electronic Network Access and Acceptable Use Policy #6:235

Introduction

LaSalle-Peru Township High School, District #120 (herein referred to as District) recognizes that access to technology in school gives students greater opportunities to learn, engage, communicate, and develop skills that will prepare them for work, life, and citizenship. We are committed to helping students develop 21st- century technology and communication skills. To that end, we provide access to technologies for student and staff use.

This Authorization & Acceptable Use Policy (AUP) does not attempt to state all required or proscribed behavior by users. However, some specific examples are provided.

The signature(s) at the end of this document is legally binding and indicates the party who signed has read the terms and conditions carefully and understands their significance.

Technologies Covered

The District may provide Internet access, desktop computers, mobile computers or devices, videoconferencing capabilities, online collaboration capabilities, message boards, email, and more. As new technologies emerge, the District will attempt to provide access to them. The policies outlined in this document are intended to cover *all* available school technologies, not just those specifically listed, and shall also cover the use of personally-owned devices on the school campus.

Data Security, Confidentiality and Privacy

All users of information technology resources are advised to consider the open nature of information disseminated electronically, including external websites/resources/apps/extension/digital personal assistants and should not assume any degree of privacy or restricted access to such information. LPHS strives to provide the highest degree of security when transferring data, but cannot be held responsible if these measures are circumvented and information is intercepted, copied, read, forged, destroyed or misused by other

Internet Safety

Internet access is limited to only those "acceptable uses" as detailed in these procedures. Internet safety is almost assured if users will not engage in "unacceptable uses," as detailed in this Authorization, and otherwise, follow this Authorization.

Staff members shall supervise students while students are using School Internet access to ensure that the students abide by the Terms and Conditions for Internet access contained in this Authorization. The School District shall endeavor to provide for the education of minors about appropriate online behavior, including interacting with other individuals on social networking websites and in chat rooms and cyberbullying awareness and response.

The District's Internet access has a filtering device that blocks entry to visual depictions that are (1) obscene, (2) pornographic, or (3) harmful or inappropriate for students, as defined by the Children's Internet Protection Act and as determined by the District. (Note: the filtering device is not guaranteed to block all inappropriate sites. Even the most sophisticated and current technology tools cannot block all inappropriate sites one hundred percent.)

Terms and Conditions

1. **Acceptable Use** - Access to the District's electronic networks must be for the purpose of education, research or communication, and be consistent with the educational objectives of the District.

2. **Privileges** - The use of the District's electronic networks is a privilege, not a right, and inappropriate use will result in a cancellation of those privileges. The system administrator or
School or District administrators will make all decisions regarding whether or not a user has this *Authorization* and may deny, revoke, or suspend access at any time.

3. **Network Etiquette** - You are expected to abide by the generally accepted rules of network etiquette. These include, but are not limited to, the following:
    a. Be polite. Do not become abusive in your messages to others.
    b. Use appropriate language. Do not swear, or use vulgarities or any other inappropriate language.
    c. Do not reveal the personal information, including the addresses or telephone numbers, of students or colleagues.
    d. Do not use the network in any way that would disrupt its use by other users.
    e. Consider all communications and information accessible via the network to be private property.

4. **Unacceptable Use** - The user (i.e., student) is responsible for his or her actions and activities involving the network. Some examples of **MAJOR** unacceptable uses are:
    a. Using the network for any illegal activity, including violation of copyright, violation of contractual rights, or transmitting any material in violation of any U.S. or State law;
    b. Using the network for commercial or private advertising;
    c. Using the network for private financial or commercial gain;
    d. Unauthorized downloading of software, regardless of whether it is copyrighted or de-virused;
    e. Wastefully using resources, such as file space;
    f. Hacking or gaining unauthorized access to files, resources or entities;
    g. Invading the privacy of individuals, which includes the unauthorized disclosure, dissemination, and use of information about anyone that is of a personal nature;
    h. Using the Internet and District resources in any way that would disrupt its use by others;
    i. Using another user's account or password;
    j. Intentionally posting of material authored or created by another;
    k. Intentionally posting anonymous messages and/or misrepresenting one's own identity to others;
    l. Accessing, submitting, posting, publishing, or displaying any defamatory, inaccurate, abusive, obscene, profane, sexually oriented, threatening, racially offensive, harassing, or illegal material. (See Board Policy 7.180 Preventing Bullying, Intimidation, and Harassment)
    m. Capture, record or transmit the words and or images of any student, staff member, or another person in the school without express prior notice and explicit consent.
    n. Using the network while access privileges are suspended or revoked and
    o. Deleting data, hiding, or attempting to interfere with the discovery of a violation of this policy.

    Some examples of **MINOR** unacceptable uses are:

    a. Searching the internet off topic/task;
    b. Using technology for non-educational purposes.

5. **No Warranties** - The District makes no warranties of any kind, whether expressed or implied, for the service, it is providing. The District will not be responsible for any damages the user suffers. This includes loss of data resulting from delays, non-deliveries, missed-deliveries, or service interruptions caused by its negligence or the user's errors or omissions. Use of any information obtained via the Internet is at the user's own risk. The District specifically denies any responsibility for the accuracy or quality of information obtained through its services.

6. **Indemnification** - The user agrees to indemnify the District of any losses, costs, or damages, including reasonable attorney fees, incurred by the District relating to, or arising out of, any breach of this *Authorization*, school policy, or rules and procedures.

7. **Unauthorized Access** – Users shall not tamper with or attempt to gain access to computer data for which the user has no security authorization. This includes, but is not limited to, financial, employee, or student information and documents.

8. **Security** - Network security is a high priority. If you can identify a security problem on the Internet, you must notify Tech Services or a School administrator. Do not demonstrate the problem to other users. Keep your account and password confidential. Do not use another individual's account. Attempts to log-on to the Internet as a system administrator will result in cancellation of user privileges. Any user identified as a security risk may be denied access to the network.

9. **Vandalism** - Vandalism will result in cancellation of privileges and other disciplinary action. Vandalism is defined as any malicious attempt to harm or destroy data of another user, the Internet, or any other network component. This includes, but is not limited to, the uploading or creation of computer viruses.

10. **Telephone/Cell Phone charges** – The District assumes no responsibility for any unauthorized charges or fees, including telephone charges, long-distance charges, per minute surcharges, and/or equipment or line costs.

11. **Copyright & Copyright Web Publishing Rules** - Copyright law and District policy prohibit the re- publishing of text or graphics found on the Web or on School Web sites or file servers, without explicit written permission.
    a. Student work may only be published if there is written permission from both the parent/guardian and student.
    b. For each re-publication (on a Web site or file server) of a graphic or a text file that was produced externally, there must be a notice at the bottom of the page crediting the original producer and noting how and when permission was granted. If possible, the notice should also include the Web address of the original source.
12. **Use of Electronic Mail -** The District's electronic mail system, and its constituent software, hardware, and data files, are owned and controlled by the District. Users of the student e-mail system are responsible for their use of the e-mail. Use of the District's electronic mail system constitutes consent to the following guidelines. Failure to do so will result in the termination of e-mail privileges for the user.
    a. The use of the e-mail must be in support of education and research and must be consistent with academic actions of the District.
    b. The e-mail user will use language that is considered appropriate and polite. The user will not send information that other users would find offensive.
    c. The purpose of the email should be restricted for educational purposes and not to "chat" or send "random" messages to other students or friends outside the school.
    d. Any message received from an unknown sender via the Internet should either be immediately deleted or forwarded to computer services. Downloading any file attached or contained within to any Internet-based message is prohibited unless the user is certain of that message's authenticity and the nature of the file so transmitted.
    e. The District reserves the right to access and disclose the contents of any account on its system, without prior notice or permission from the account's user. The account user has no expectation of privacy with regard to any electronic mail account or other aspect of the District's electronic mail system. Unauthorized access by any student or staff member to an electronic mail account is strictly prohibited.
    f. Students will not be allowed to use any other personal e-mail accounts such as Hotmail, Yahoo, Gmail, Live, etc.

Consequences for Violation of Polices

The failure of any user to follow the terms of the agreement will result in the loss of privileges, disciplinary action, and/or appropriate legal action. The following consequences will be administered based on the severity of the violation:

Consequences for Minor Violations

A single consequence or any combination of the following may be administered per discretion of the teacher:

- Warning by the teacher
- Loss of technology privilege in the class for a timeframe designated by the teacher.
- General discipline steps for misconduct in class (refer to Student Handbook).

Consequences for Major Violations

1. First Offense
    - The student is revoked of all computer privileges for two weeks.
    - Computer Services is notified and the student's account is suspended for those two weeks.
    - Teachers, counselors and parents are notified of violation and consequences.
    - Student holds responsibility for completion of all assigned classwork or assignments that require digital access (e.g., student may need to complete work using home or public library networks).
2. Second Offense
    - The student is revoked of all computer privileges for nine weeks.
    - Computer Services is notified and the student's account is suspended for those nine weeks.
    - Teachers, counselors and parents are notified of violation and consequences.
    - Student holds responsibility for completion of all assigned classwork or assignments that require digital access (e.g., student may need to complete work using home or public library networks).
3. Third Offense
    - The student is revoked of all computer privileges for the remainder of the school year and possibly longer, dependent upon consequences and time remaining in the school year.
    - Computer Services is notified and the student's account is suspended for determined time period of revocation.
    - Teachers, counselors and parents are notified of violation and consequences Parents are notified of violation and consequences.
    - Student holds responsibility for completion of all assigned classwork or assignments that require digital access (e.g., student may need to complete work using home or public library networks).

Appropriate Uses and Digital Citizenship

While working in a digital and collaborative environment, students should always conduct themselves as good digital citizens by adhering to the following:

1. Respect Yourself.
   I will show respect for myself through my actions. I will select online names that are appropriate. I will use caution with the information, images, and other media that I post online. I will carefully consider what personal information about my life, experiences, or relationships I post. I will not be obscene. I will act with integrity.

2. Protect Yourself.
   I will ensure that the information, images, and materials I post online will not put me at risk. I will not publish my personal details, contact details, or a schedule of my activities. I will report any attacks or inappropriate behavior directed at me while online. I will protect passwords, accounts, and resources.

3. Respect Others.
   I will show respect to others. I will not use electronic mediums to antagonize, bully, harass, or stalk people. I will show respect for other people in my choice of websites: I will not visit sites that are degrading to others, pornographic, racist, or inappropriate. I will not enter other people's private spaces or areas.

4. Protect Others.
   I will protect others by reporting abuse and not forwarding inappropriate materials or communications. I will avoid unacceptable materials and conversations.

5. Respect Intellectual Property.
   I will request permission to use copyrighted or otherwise protected materials. I will suitably cite all use of websites, books, media, etc. I will acknowledge all primary sources. I will validate information. I will use and abide by the fair use rules.

6. Protect Intellectual Property.
   I will request to use the software and media others produce. I will purchase, license, and register all software or use available free and open source alternatives rather than pirating software. I will purchase my music and media and refrain from distributing these in a manner that violates their licenses.

Copyright and File Sharing

Students are required to follow all copyright laws around all media including text, images, programs, music, and video. Downloading, sharing, and posting online illegally obtained media is against the Acceptable Use Policy.

LaSalle-Peru Township High School, District #120

Student and Parent/Guardian Technology & Chromebook Agreement 2021-2022

Student Agreement:

In order to receive and utilize a LP network account and a Chromebook and its accessories on the District network, the student must agree to the following:

- I will bring my issued Chromebook to school EVERY day that I am in attendance.
- I will not use the issued Chromebook for non-academic purposes (e.g., games, downloads, chat rooms, instant messaging, viewing websites not related to the assignment, etc.) during school hours (i.e., 7:55 am - 2:55 pm).
- I will charge the issued Chromebook's battery daily and will NOT loan out the Chromebook or any of its accessories to other individuals, and know that I will be issued the same Chromebook each year.
- I will transport the Chromebook in its issued protective bag/sleeve. The Chromebook bag/sleeve should be securely closed before transporting the Device to another location. I will not add books and supplies to the bag/sleeve, since undo pressure on the Chromebook may cause damage.
- I will keep the issued Chromebook off the floor where it could be stepped on or tripped over. I will keep food and beverages away from the Chromebook since they may cause damage to the Chromebook.
- I will not disassemble any part of my issued Chromebook or attempt any repairs.
- I will not deface the issued Chromebook or its accessories in any way. This includes, but is not limited to, attaching stickers, marking painting, drawing or marring any surface of the Chromebook.
- I understand that obscene language and/or materials, including music, screen savers, backdrops, and/or pictures are prohibited.
- I understand that my Chromebook is subject to inspection at any time without notice and remains the property of the district.
- I will follow the expectations outlined in the ***Student/Parent Technology Handbook,*** **the** ***Student Authorization for Electronic Network Access and Acceptable Use Policy*****, and the District's Code of Conduct as outlined in the Student Handbook.** As such, the student is subject to all discipline measures for violation of same.

Parent/Guardian Agreement:

In order for the student to receive and utilize a Chromebook and its accessories on the District network, the parent/guardian must agree to the following:

- I will be responsible for the repair or replacement costs in the event of loss or damage of the laptop, accessories or bag if damage or loss is negligent or deliberate.
- I will be responsible for monitoring my child's use of the Internet when he/she is not at school.
- I acknowledge that fraudulent reporting of theft will be turned over to the police prosecute.
- I agree to immediately return the Chromebook and accessories in good working condition upon request.
- I acknowledge that my student and I are to follow the expectations in the ***Student/Parent Technology Handbook,*** **the** ***Student Authorization for Electronic Network Access and Acceptable Use Policy,*** **and the District's Code of Conduct as outlined in the Student Handbook** and that my student is subject to discipline for violation of the expectations outlined in these documents.

Technology & Chromebook Agreement-Signature Sheet

By signing the Student and Parent Technology & Chromebook Agreement, the student and parent agrees to the conditions outlined in the Student/Parent Technology Handbook and the Student Authorization for Electronic Network Access and Acceptable Use Policy**.**

Print Student Name: _____

Student Signature:_____ Date:_____/____/_____

THE ELECTRONIC SIGNATURE MADE DURING THE ONLINE E-REGISTRATION PROCESS REPLACES THIS SIGNATURE.

Print Parent/Guardian Name: _____

Parent/Guardian Signature:_____ Date:_____/____/_____

THIS SIGNATURE SHEET MUST BE SIGNED BEFORE THE STUDENT IS ISSUED A LP NETWORK ACCOUNT AND CHROMEBOOK.