Please read the packet and complete this form. Turn in THIS FORM ONLY, along with technology fee.

---------- ----------

Student Name (Please Print) Grade

East Prairie R2 School District Technology User Agreement

Please initial next to each statement, acknowledging that you have read and understand each component of the EPR2 Technology User Agreement.

Student Initials		Guardian Initials
---------	We have read the Chromebook User/Care Agreement and have accepted the terms set forth by the agreements.	---------
---------	We have read the **Internet Usage Agreement (P 6320)** and understand that I am to avoid inappropriate material and activities, and will adhere to the provisions set forth by the EPR2 school district regarding what is deemed inappropriate.	---------
---------	We have read the **Internet Usage Agreement, Part 2 (R 6320)** and agree to adhere to the principles and procedures listed within. I also understand that additional rules and regulations may be added from time to time and that they may become part of this agreement. Should I break this agreement, I understand that I may lose all computer/Internet privileges and other penalties may be assessed. I also understand that inappropriate or illegal use of computer facilities could result in civil or criminal lawsuits. Parents/guardians may be held accountable for inappropriate use of the network by their child.	---------
---------	I understand that **photos** celebrating student success may be published on the district website and/or app. In addition, I understand that through the use of distance learning technology my student's image, voice, and/or educational products (school work) may be transmitted to and viewed by their teachers and/or other students. *If I do not want audio or video of my child or their work published, transmitted, or viewed, I will submit a written request to the appropriate school's office stating such.*	---------

Parent Signature: _____ Date: _____

Student Signature: _____ Date: _____

Chromebook Issued: _____ Technology Fee Collected: _____

East Prairie Schools

Technology User Agreement

I. East Prairie R-II School District Chromebook User/Care Agreement

A. The East Prairie School District is expanding its use of technology by furnishing Chromebooks for designated classes. Students have certain responsibilities in the use and care of these devices. Upon signing the Chromebook agreement, you are acknowledging that you understand and accept the information in this document.

1. All users of the East Prairie R-2 network and equipment must comply at all times with the East Prairie R-2 Board Policy on Technology Usage.
2. Chromebooks, cases, and charging cords are on loan to the students and remain the property of the district.
3. Students are expected to keep the Chromebooks in good condition and in the district-provided case. Failure to do so may result in parents/guardians being required to pay for repair or replace the device.
4. Heavy objects should not be placed on top of the Chromebooks.
5. If the Chromebook is not working correctly, seems to be malfunctioning, or is damaged, it should be reported to the teacher. Students should not disassemble any part of the Chromebook or attempt any repairs themselves or take the Chromebook to a third-party for repair. The Chromebook is the property of the district and should only be serviced by district technology department personnel.
6. The replacement value of the Chromebook will include the Chromebook, the case and the charging cord, and prices are subject to change according to current replacement costs..
7. Chromebooks should be in a student's possession or in a designated secure area at all times. Do not leave the Chromebook unattended. Designated secure areas include a specific teacher during his/her class time or administrative office. Students and parents/guardians are responsible for the security of the Chromebook when students are off campus and should take all reasonable precautions for the storage of the Chromebook. Chromebooks should not be left in unattended vehicles or in an area where it could be easily stolen.
8. If the Chromebook is stolen, parents/guardians should immediately report the theft to the administration and the police department. A police report must be filed within 24 hours.

B. We understand we are accepting responsibility for any damage, destruction, or loss of the assigned Chromebook. We understand that a $30 technology user fee will be collected for each Chromebook. This fee will cover:

1. One occurrence of replacement of the Chromebook screen due to breakage. There will be no charge for the first breakage, unless it is determined that the Chromebook has been removed from its school-purchased protective case. If the Chromebook screen has to be replaced more than once, the parent/guardian will be charged $50 for each occurrence after the first replacement of the broken screen.
2. If the Chromebook is lost or stolen in the student's time in the district, a $150 fee will be charged to the parent/guardian. A second instance of loss or theft will result in the parent/guardian being charged the full cost of replacement. Restricted use may result if it is determined that the loss or theft was due to neglect on the part of the student or parent/guardian.
3. While the technology fee will be collected each year the student uses the Chromebook, occurrences will be accumulated. For example, a student's Chromebook screen is replaced (for free) in the 11th grade. The screen is cracked again in the 12th grade. The crack that occurs in the 12th grade will be seen as the second occurrence and the $50 fee will be collected.

C. This fee will not cover the loss of the provided charger. It will be the responsibility of the student to pay the replacement cost of the lost or stolen charger.

D. Estimated Chromebook Repair Charges: (Repaired Chromebook will not be returned to you until you have paid the charges or set up a payment plan and made an effort to pay for the repair).

Keyboard $60
Screen $50
Charger $25
Battery $50
Case $35
Chromebook Replacement $150-300
*Prices fluctuate with current market value

I. Internet Usage Agreement (P 6320) [09.2015]

A. **Introduction**—It is the policy of the District to: (a) prevent user access over its computer network to, or transmission of, inappropriate material via Internet, electronic mail, or other forms of direct electronic communications; (b) prevent unauthorized access and other unlawful online activity; (c) prevent unauthorized online disclosure, use, or dissemination of personal identification information of minors; and (d) comply with the Children's Internet Protection Act [Pub. L. No. 106-554 and 47 USC 254(h)].

B. **Access to Inappropriate Material**--To the extent practical, technology protection measures shall be used to block or filter Internet, or other forms of electronic communications, access to inappropriate information. Specifically, as required by the Children's Internet Protection Act, blocking shall be applied to visual depictions of material deemed obscene or child pornography, or to any material deemed harmful to minors. Subject to staff supervision, technology protection measures may be disabled or, in the case of minors, minimized only for bona fide research or other lawful purposes.

C. **Internet Safety Training**—In compliance with the Children's Internet Protection Act, each year, all District students will receive internet safety training which will educate students about appropriate online behavior, including interacting with other individuals on social networking sites and in chat rooms, and cyberbullying awareness and response. Such training will include Internet, cell phones, text messages, chat rooms, email and instant messaging programs. (See also Policy 6116 – State Mandated Curriculum – Human Sexuality).

D. **Inappropriate Network Usage**—To the extent practical, steps shall be taken to promote the safety and security of users of the District's online computer network when using electronic mail, chat rooms, instant messaging, and other forms of direct electronic communications. Specifically, as required by the Children's Internet Protection Act, prevention of inappropriate network usage includes: (a) unauthorized access, including so-called "hacking," and other unlawful activities; and (b) unauthorized disclosure, use, and dissemination of personal identification information regarding minors.

E. **Supervision and Monitoring**—It shall be the responsibility of all District employees to supervise and monitor usage of the online computer network and access to the Internet in accordance with this policy and the Children's Internet protection Act. Procedures for the disabling or otherwise modifying any technology protection measures shall be the responsibility of *the Technology Coordinator* or designated representatives.

II. Internet Usage Agreement, Part 2 (R 6320) [05.2013]

A. Personal Responsibility

1. Access to electronic research requires students and employees to maintain consistently high levels of personal responsibility. The existing rules found in the District's Behavioral Expectations policy (Board Policy/Regulation 2610) as well as employee handbooks clearly apply to students and employees conducting electronic research or communication.
2. One fundamental need for acceptable student and employee use of District electronic resources is respect for, and protection of, password/account code security, as well as restricted databases files, and information banks. Personal passwords/account codes may be created to protect students and employees utilizing electronic resources to conduct research or complete work.
3. These passwords/account codes shall not be shared with others; nor shall students or employees use another party's password except in the authorized maintenance and monitoring of the network. The maintenance of strict control of passwords/account codes protects employees and students from wrongful accusation of misuse of electronic resources or violation of District policy, state or federal law. Students or employees who misuse electronic resources or who violate laws will be disciplined at a level appropriate to the seriousness of the misuse.

B. Acceptable Use

1. The use of the District technology and electronic resources is a privilege, which may be revoked at any time. Staff and students are only allowed to conduct electronic network-based activities which are classroom or workplace related. Behaviors which shall result in revocation of access shall include, but will not be limited to: damage to or theft of system hardware or software; alteration of system hardware or software; placement of unlawful information, computer viruses or harmful programs on, or through the computer system; entry into restricted information on systems or network files in violation of password/account code restrictions; violation of other users' rights to privacy; unauthorized disclosure, use or dissemination of personal information regarding minors; using another person's name/password/account to send or receive messages on the network; sending or receiving personal messages on the network; and use of the network for personal gain, commercial purposes, or to engage in political activity.
2. Students and employees may not claim personal copyright privileges over files, data or materials developed in the scope of their employment, nor may students or employees use copyrighted materials without the permission of the copyright holder. The Internet allows access to a wide variety of media. Even though it is possible to download most of these materials, students and staff shall not create or maintain archival copies of these materials unless the source indicates that the materials are in the public domain.
3. Access to electronic mail (E-mail) is a privilege and designed to assist students and employees in the acquisition of knowledge and in efficiently communicating with others. The District E-mail system is designed solely for educational and work related purposes. *E-mail files are subject to review by District and school personnel.* Chain letters, "chat rooms" or Multiple User Dimensions (MUDs) are not allowed, with the exception of those bulletin boards or "chat" groups that are created by teachers for specific instructional purposes or employees for specific work related communication.

4. Students or employees who engage in "hacking" are subject to loss of privileges and District discipline, as well as the enforcement of any District policy, state and/or federal laws that may have been violated. Hacking may be described as the unauthorized review, duplication, dissemination, removal, damage, or alteration of files, passwords, computer systems, or programs, or other property of the District, a business, or any other governmental agency obtained through unauthorized means.
5. To the maximum extent permitted by law, students and employees are not permitted to obtain, download, view or otherwise gain access to "inappropriate matter" which includes materials that may be deemed inappropriate to minors, unlawful, abusive, obscene, pornographic, descriptive of destructive devices, or otherwise objectionable under current District policy or legal definitions. Similarly, the use of any District computer to access sites which allow the user to conceal their objective of accessing inappropriate material is not permitted.
6. The District and school administration reserve the right to remove files, limit or deny access, and refer staff or students violating the Board policy to appropriate authorities or for other disciplinary action.

C. **Internet Access**

1. In compliance with the Children's Internet Protection Act ("CIPA"), 47 U.S.C. § 254, the District uses technological devices designed to filter and block the use of any District computer with Internet access to retrieve or transmit any visual depictions that are obscene, child pornography, or "harmful to minors" as defined by CIPA and material which is otherwise inappropriate for District students.
2. Due to the dynamic nature of the Internet, sometimes Internet websites and web material that do not fall into these categories are blocked by the filter. In the event that a District student or employee feels that a website or web content has been improperly blocked by the District's filter and this website or web content is appropriate for access by District students, the process described below should be followed:
    1) Follow the process prompted by the District's filtering software (or to remain anonymous, log in under log in name: 123anonymous) and submit an electronic request for access to a website, or:
    2) Submit a request, whether anonymous or otherwise, to the District's Superintendent/the Superintendent's designee.
    3) Requests for access shall be granted or denied within three days. If a request was submitted anonymously, persons should either attempt to access the website requested after three days or log back in at 123anonymous to see the status of the request.
    4) Appeal of the decision to grant or deny access to a website may be made in writing to the Board of Education. Persons who wish to remain anonymous may mail an anonymous request for review to the Board of Education at the School District's Central Office, stating the website that they would like to access and providing any additional detail the person wishes to disclose.
    5) In case of an appeal, the Board of Education will review the contested material and make a determination.
    6) Material subject to the complaint will not be unblocked pending this review process.
3. In the event that a District student or employee feels that a website or web content that is available to District students through District Internet access is obscene, child pornography, or "harmful to minors" as defined by CIPA or material which is otherwise inappropriate for District students, the process described set forth in Regulation 6241 should be followed.
4. Adult users of a District computer with Internet access may request that the "technology protection measures" be temporarily disabled by the chief building administrator of the building in which the computer is located for lawful purposes not otherwise inconsistent with this Policy.

D. **Privileges**--The use of District technology and electronic resources is a privilege, not a right, and inappropriate use will result in the cancellation of those privileges. All staff members and students who receive a password/account code will participate in an orientation or training course regarding proper behavior and use of the network. The password/account code may be suspended or closed upon the finding of user misuse of the technology system or its resources.

E. **Network Etiquette and Privacy**--Students and employees are expected to abide by the generally accepted rules of electronic network etiquette. These include, but are not limited to, the following:

- ➔ System users are expected to be polite. They may not send abusive, insulting, harassing, or threatening messages to others.
- ➔ System users are expected to use appropriate language; language that uses vulgarities or obscenities, libels others, or uses other inappropriate references is prohibited.
- ➔ System users may not reveal their personal addresses, their telephone numbers or the addresses or telephone numbers of students, employees, or other individuals during E-mail transmissions.
- ➔ System users may not use the District's electronic network in such a manner that would damage, disrupt, or prohibit the use of the network by other users.
- ➔ System users should assume that all communications and information is public when transmitted via the network and may be viewed by other users. The system administrators may access and read E-mail on a random basis.
- ➔ Use of the District's electronic network for unlawful purposes will not be tolerated and is prohibited.

F. **Services**--While the District is providing access to electronic resources, it makes no warranties, whether expressed or implied, for these services. The District may not be held responsible for any damages including loss of data as a result of delays, non-delivery or service interruptions caused by the information system or the user's errors or omissions. The use or distribution of any information that is obtained through the information

system is at the user's own risk. The District specifically denies any responsibility for the accuracy of information obtained through Internet services.

G. **Security**

1. The Board recognizes that security on the District's electronic network is an extremely high priority. Security poses challenges for collective and individual users. Any intrusion into secure areas by those not permitted such privileges creates a risk for all users of the information system.
2. The account codes/passwords provided to each user are intended for the exclusive use of that person. Any problems, which arise from the user sharing his/her account code/password, are the responsibility of the account holder. Any misuse may result in the suspension or revocation of account privileges. The use of an account by someone other than the registered holder will be grounds for loss of access privileges to the information system.
3. Users are required to report immediately any abnormality in the system as soon as they observe it. Abnormalities should be reported to the classroom teacher or system administrator.
4. The District shall use filtering, blocking or other technology to protect students and staff from accessing internet sites that contain visual depictions that are obscene, child pornography or harmful to minors. The District shall comply with the applicable provisions of the Children's Internet Protection Act (CIPA), and the Neighborhood Internet Protection Act (NCIPA).

H. **Vandalism of the Electronic Network or Technology System**--Vandalism is defined as any malicious attempt to alter, harm, or destroy equipment or data of another user, the District information service, or the other networks that are connected to the Internet. This includes, but is not limited to: the uploading, or the creation of, computer viruses; the alteration of data; or the theft of restricted information. Any vandalism of the District electronic network or technology system will result in the immediate loss of computer service, disciplinary action and, if appropriate, referral to law enforcement officials.

I. **Consequences**--The signatures on this agreement are legally binding, and consequences for violating the District's Acceptable Use Policy include, but are not limited to, one or more of the following:

- ➔ Suspension of District Network privileges;
- ➔ Revocation of Network privileges;
- ➔ Suspension of Internet access;
- ➔ Revocation of Internet access;
- ➔ Suspension of computer access;
- ➔ Revocation of computer access;
- ➔ Legal action, when appropriate;
- ➔ School disciplinary action, at the discretion of administrators;
- ➔ School suspension;
- ➔ Expulsion; or
- ➔ Employee disciplinary action up to and including dismissal.

**After reading this agreement, please complete the attached form.
Keep this agreement for your records, and bring the completed form, along with your technology fee, to the Chromebook station.

Family Size	Chromebook Technology Fee
1	$30
2	$25 each
3+	$20 each

**Cash/Check only. Checks made payable to East Prairie R-2 Schools. Must include driver's license # and date of birth. Thanks!
STUDENTS ARE REQUIRED TO PAY THIS BEFORE TAKING DEVICE HOME FROM SCHOOL