West Bloomfield School District

Acceptable Use Policy

RULES FOR THE ACCEPTABLE USE OF TECHNOLOGY RESOURCES AND PERSONAL TECHNOLOGY DEVICES

Purpose:

West Bloomfield School District ("the District or WBSD") recognizes that advancements in technology affect the manner in which information may be accessed, communicated, and transferred by members of society, provide a vast and diverse array of educational resources, and impacts how we learn. Therefore, the District provides student, teachers, employees and administrators with access to the School district's Technology Resources, which includes access to the Internet. The School District's Technology Resources have not been established as a public access service or a public forum, limited or full. The Board has the right to place restrictions on its use to assure that the School District's Technology Resources are used in accordance with its limited educational purpose. The primary, and only, purpose of providing Technology Resources is to support the educational objectives of West Bloomfield School District and the educational community in general.

In an effort to increase access, the School district allows approved personal technology devices (PTD - as defined below) on our WBSD guest network and school grounds, in accordance with these procedures. The use of PTD is optional. Users who do not elect to use PTD will not be penalized and alternate modes of participation will be available.

Students shall receive education about safety and security while using email, social media, and other forms of electronic communications, the dangers inherent with the online disclosure of personally identifiable information, and the consequences of unauthorized access, cyber bullying and other unlawful or inappropriate activities. The School district will review cyber-safety rules with students throughout the course of the school year, and will offer reminders and reinforcement about safe and appropriate online behaviors.

It is the responsibility of the user of WBSD technology equipment, Network, resources, or other electronic or social media to read, understand, and follow the Acceptable Use Policy(AUP) . In addition, users are expected to exercise reasonable judgment and common sense in interpreting the Acceptable Use Policy and in making decisions about the appropriate use of WBSD technology equipment, Network, resources, or other electronic or social media.

The intent of this policy is to ensure that users have robust access to Technology Resources and utilize access in a manner consistent with the educational objectives of WBSD. Users should understand that the AUP is in place *primarily* to address *malicious intent, or illegal, immoral, and unethical activities.* In any specific situation we rely upon each individual's judgement, role in the district or the educational purpose when making decisions about appropriate conduct.
Any user with questions regarding the application or meaning of the Acceptable Use Policy should

seek clarification from the WBSD Technology Services Department. All persons using the WBSD network, technology equipment, resources, or other electronic or social media, further known as Users, are expected to be familiar with the provisions in this document and shall adhere to the policies, procedures, rules and regulations of the School District, including but not limited to: the Student Code of Conduct, Board of Education policies, the Acceptable Use Policy, Caring For a District-Provided Device and Using Personal and District Provided-Devices at School policies. Users shall sign the Acceptable Use Policy as a prerequisite to the use of School District Technology Resources and PTD.

Definitions:

Personal Technology Devices, or "PTD": PTD is defined as an electronic device owned by the student, staff, or volunteer user, including, but not limited to, a user's own laptop, smartphone, eReader, iPad, Chromebook or similar device, etc., that is used on school property, and is approved for such use. Not all devices are approved for use on school property. Devices that are dangerous or potentially dangerous are not approved for use at any time. The school district reserves the right to limit the types of devices that are approved for use on school property.

Technology Resources: Includes, but is not limited to, the WB guest network, Internet, electronic mail ("e-mail"), Computer Systems (as defined below), cameras, televisions, video cassette recorders, DVDs, telephones, WB-issued cellular/smartphones and all other voice, video and data systems.

Computer System and/or System: Includes, but is not limited to, computer hardware, disk drives, printers, iPads, Chromebooks, scanners, software (operation and application), the network and any and all other associated equipment.

School property: Includes on school premises, on a school bus or other school-related vehicle, or at a school-sponsored activity or event whether or not it is held on school premises.

Users Include: Students, Teachers, Parents & Guests

Procedures and Guidelines for the Use of Technology Resources and PTD:

All use of the West Bloomfield Schools Technology Resources must be consistent with the purpose stated above. This policy does not attempt to articulate all required or proscribed behaviors by users of this network.

1. All individual users of Technology Resources and PTD shall accept responsibility for the acceptable use thereof.

2. The use of all Technology Resources and of PTD on school property is a privilege, not a right, and the School district has the right to limit, restrict, or prohibit the use of Technology Resources, and/or limit, restrict, or prohibit the use of PTD on school property.

3. Failure to follow the policies, procedures, rules and regulations of the School district may result in termination of the user's privilege to use Technology Resources and/or legal action. Reports will be made to law enforcement of suspected violations of State and/or Federal law. In addition, the user may be subject to disciplinary action.

4. Users have no right or expectation of privacy when using Technology Resources, including, but not limited to, network communications, e-mail, data on a workstation or server, Internet use, telephone, voice mail, and video recording.

5. The School District is the owner of the Technology Resources and therefore all users understand that their use of the Technology Resources can and may be strictly monitored electronically by the School District personnel at any time.

6. The School District may collect and examine a student's PTD - while logged into the District's network - and there is a reasonable suspicion that, through the use of the PTD, a student is violating or has violated the law, and/or the policies, procedures, rules and regulations of the School District.

7. In accordance with all applicable laws, the School district may collect and examine a non-student user's PTD - while logged into the District's network - and there is cause to believe the PTD was used in the commission of a crime and/or the commission of a violation of the policies, procedures, rules and regulations of WB.

8. Users shall not knowingly or intentionally disclose, transmit, disseminate or otherwise distribute with PTD or Technology Resources, copyrighted, private, confidential or privileged information.

9. Users shall not make copies of software from the School District's Computer Systems. Use of Technology Resources for fraudulent or illegal copying, communication, taking or modification of material in violation of law is prohibited and will be referred to federal authorities. The illegal use of copyrighted software is prohibited. The School District upholds the copyright laws of the United States, as it applies to computer programs or licenses owned or licensed by the School District.

10. Users shall not install software programs or apps on the School district computers, servers or any Technology Resources without the approval of the administration or administrative designee.

11. Users shall not modify any of the Technology Resources without the approval the administration or administration designee.

12. Users shall promptly report any problems or malfunctions with Technology Resources or Computer Systems to the Ready Desk and teacher/building principal.

13. Users shall not create or use web technology services or social media for School District-related business that cannot be monitored or controlled by the School District. Any and all web technology services, web pages, or social media used for or representing the School district or School district-related business shall be used, designed and published in accordance with the guidelines outlined in this policy.

14. Users shall not give computer software to others unless it is clearly identified in the public domain as freeware, or if they have written permission from the copyright owner.

15. Users shall not knowingly or intentionally introduce a virus, worm, Trojan horse, rootkit, or engage in any other malicious action that affects Technology Resources. The School District

may collect and examine any Technology Resource or PTD that is suspected of causing technology problems or was the source of an attack, rootkit, worm, Trojan horse, or virus infection.

16. Users shall not bypass the network filters and security policies, or process or access information related to the network filters and security policies. The School District may collect and examine any Technology Resource or PTD that is suspected of bypassing the network filters and security, or processing or accessing information related to the network filters and security policies.

17. Users shall not infiltrate, "hack into", attempt to access or actually access Technology Resources, data, materials, or files that they are not authorized to access or the individual knows or reasonably believes may negatively affect the integrity of Technology Resources.

18. Users shall understand that they are responsible for any uses of their PTD and shall immediately notify administrators or teachers if a security problem is suspected or identified.

19. Users shall not attempt to obtain any other user's password(s) and shall not read, copy or alter other user's data without their permission, unless it is required to perform the user's job function. Users shall not intentionally seek information, obtain copies of, or modify files, other data or passwords belonging to other users, or misrepresent other users on the Internet.

20. Users shall not knowingly or intentionally damage or alter any aspect of the Technology Resources or alter or modify the Technology Resources.

21. Users shall not use Technology Resources for purposes other than for School district-related business. The Internet and Technology Resources shall not be used for illegal activity, for-profit purposes, lobbying, campaigning, advertising, fundraising, transmitting offensive materials, hate mail, mass e-mailing, discriminating remarks, or obtaining, possessing, or sending sexually explicit, obscene, or pornographic material.

22. Users shall not use Technology Resources to harass, bully or intimidate.

23. Messages sent by users via Technology Resources shall not contain profanity, obscene comments, sexually explicit material, expressions of bigotry, racism or hate, nor shall they contain personal information the user would not want made available to strangers such as the users name, address, telephone number, social security number, pictures or other personally identifiable information.

24. Disclosure, use and/or dissemination of personally identifiable information of students is prohibited, except as expressly authorized by the minor student's parent or guardian or by the eligible student as permitted by law.

25. The content, use and maintenance of a user's electronic (e-mail) mailbox, (if they have been assigned one), is the user's responsibility.

    Perform basic email management/best practices.

    1. Check and respond to messages as contract requires

2. Regularly remove/archive unwanted or unneeded messages
3. Maintain all parent, staff and student communication in archiving folders
4. Be aware of email threats to the network and computer security (ie do not download viruses, SPAM and malware). Do not open attachments from suspicious or questionable sources.

*NOTE: All school email/digital communication is matter of public record (See FOIA) and is, at any time, available to anyone upon request

26. The School district in its sole discretion reserves the right to terminate the availability of Technology Resources and/or PTD, including Internet access, at any time.

27. Students shall not use PTD on school property for purposes other than for educational purposes.

28. The School District reserves the right to:

a. Make determinations as to whether specific uses of its Technology Resources and/or PTD are inconsistent with the goals, educational mission, policies and/or procedures of the School district.

b. Monitor and keep records of Internet use and to monitor fileserver space utilization by users.

c. Terminate a user's privilege to access Technology Resources and/or the use of PTD to prevent further unauthorized activity.

d. Subject a user to disciplinary action for conduct that causes a substantial disruption to the educational environment, in accordance with the policies, procedures, rules and regulations of the School district and applicable law.

29. Users shall not play video games, visit chat rooms or social media sites or otherwise use PTD on school property for non-academic purposes or non school-related purposes.

30. It is the responsibility of teachers and staff to monitor the use of PTD on school property by students that they are supervising.

31. Administration has the discretion to prohibit, allow, and otherwise regulate the use of PTD during the school day.

32. Each teacher has the discretion to allow and regulate the use by students of PTD in the classroom and on specific projects.

33. In the classroom, if given permission, students may use PTD only for the purpose of accessing materials that are relevant to the classroom curriculum.

34. The school's network filters will be applied to a PTD's connection to the Internet and other Technology Resources.

35. Users are expected to charge PTD prior to school and run PTD on battery power while at

school.

36. The School district will not service any PTD, which includes troubleshooting, software or hardware issues.

37. Each user is responsible for his/her own PTD, and should treat it and use it responsibly and appropriately. The School District takes no responsibility for stolen, lost or damaged PTD, including lost or corrupted data on PTD. Please check with your homeowner's policy regarding coverage of PTD, as many insurance policies can cover loss or damage.

38. Each user shall be responsible for any and all damages to their PTD resulting from their deliberate or willful acts.

39. Users shall maintain PTD in silent mode at all times when on school property, unless otherwise permitted by school staff.

40. Users shall not record, transmit or post images or video of a person or persons on campus during school activities and/or hours, unless provided with authorization by a teacher, administrator, or administrative designee.

41. Use of PTD is prohibited in the following areas/situations:

    a. Locker rooms
    b. Bathrooms
    c. Any private areas used for the purpose of changing clothes
    d. Any other areas as designated by administration

42. Students shall not use PTD to cheat on assignments or tests.

43. Users shall not print from PTD to School district printers for educational purposes without permission from administration or administrative designee.

44. No user may connect any non-approved device of any kind, including routers, switches or other devices into the network.

45. Users are not allowed to enable "hot spots", connect to an external proxy, and tether while in the school building.

Network Considerations:

Users should strive to maintain appropriate bandwidth for school-related work and communications when using the WB Guest network. The School district does not guarantee connectivity or quality of connection with PTD, but will provide documentation on how to connect with a variety of operating systems and devices.

Disclaimer:

The School district will make every effort to provide appropriate Technology Resources and services, however, the School District makes no warranties of any kind, whether expressed or implied, for the

Technology Resources it is providing. The school district will not be responsible for any damages incurred by a user of the Technology Resources, including loss of data resulting from delays, non-deliveries, mis-deliveries, or service interruptions. The School district does not endorse or guarantee the accuracy or quality of information obtained via the Internet or electronic mail. The School District shall not be held responsible for any possible charges to an account that might be incurred during approved school-related use of PTD.

In no event shall the School district be liable for any damages (whether direct, indirect, special or consequential) arising out of the use of the Internet, accuracy or correctness of databases or information contained therein, or related directly or indirectly to any failure or delay of access to the Internet or other network application.

GSuite For Education Account Permission

The West Bloomfield School District provides students with unique learning opportunities via our collaborative and technology enhanced learning environment. Through the use of GSuite for Education, students engage in activities and projects that promote creativity, critical thinking, and collaboration, which we feel are essential skills for the development of a well-rounded learner.

These activities include, but are not limited to the following.

- Email- an individual email account for school use managed by the District.
- Google Apps – productivity tools commonly used for education.
- Google Meet - video collaboration with teachers, parents and students.
- Managed Social Networking: social bookmarking, video sharing, blogging, etc.

The District uses GAFE for the purposes of:

- Providing students with access to current technology applications and free tools designed for collaboration with other students and teachers
- Giving students the ability to work on their documents both in school and at home - anytime and anywhere from any Internet connected device
- Helping students to work collaboratively, engage in peer-editing of documents, and publish for a wider audience within the District
- Facilitating “paperless” transfer of work between students and teachers
- Providing adequate long-term digital storage space for student work

Your child will access these tools through a Google Account. After you complete and submit this permission form, your child will receive their unique username and password under the District’s domain.

Access Restriction

Access to GSuite for Education is considered a privilege accorded at the discretion of the district. The district maintains the right to immediately withdraw the access and use of Google Apps when there is reason to believe that violations of law or district policies have occurred. In such cases, the alleged violation will be referred to the principal for further investigation and account restoration, suspension, or termination. As part of the agreement with Google, the

school also reserves the right to immediately suspend any user account suspected of inappropriate use. Pending review, a user account may be terminated as part of such action.

Technology use in the District is governed by federal laws including:

- Children's Online Privacy Protection Act (COPPA)
    - COPPA applies to commercial companies and limits their ability to collect personal information from children under 13.
    - By default, advertising is turned off for the District's presence in Google Apps for Education. No personal student information is collected for commercial purposes.
    - This permission form allows the school to act as an agent for parents in the collection of information within the school context. The school's use of student information is solely for education purposes.
    - COPPA – http://www.ftc.gov/privacy/coppafaqs.shtm

      https://www.ftc.gov/enforcement/rules/rulemaking-regulatory-reform-proceedings/childrens-online-privacy-protection-rule
- Family Educational Rights and Privacy Act (FERPA)
    - FERPA protects the privacy of student education records and gives parents the rights to review student records.
    - Under FERPA, schools may disclose directory information (See Board Policy) but parents may request the school not disclose this information. Parents are provided the opportunity
    - FERPA - http://www2.ed.gov/policy/gen/guid/fpco/ferpa/index.html
- Child Internet Protection Act (CIPA)
    - Requires the school to have filters in place to protect students from harmful materials including the obscene.
    - CIPA - http://fcc.gov/cgb/consumerfacts/cipa.html

I understand that by participating in GSuite for Education, information about my child will be collected and stored electronically. Privacy policies on GSuite for Education accounts can be found at https://edu.google.com/why-google/privacy-security/?modal_active=none. Please note, you may opt out at any time by sending written notice to your student's building administrator.

Caring For A District Provided Device

Students are responsible for the general care of the District Provided Device they have been issued by the district.

District Provided Devices that are broken or fail to work properly must be repaired by the person it is issued to. The district provides optional insurance for the District Provided Device. If one does not participate in the district insurance option, they are responsible for the full cost of repairs by the district device service provider. Failure to state whether you are or aren't participating in the district provided insurance option will automatically mean you are not participating.

District Provided Devices should never be taken to an outside computer service for any type of repairs or maintenance.

General Precautions

- No food or drink should be next to the District Provided Device.
- Cords, cables, and removable storage devices must be inserted carefully into the District Provided Device.
- District Provided Devices should not be exposed to extreme temperatures such as an overly hot or cold car.
- Heavy objects must never be placed on top of the District Provided Device.
- District Provided Devices must remain free of any **writing, drawing, stickers, and labels.**
- District Provided Devices must be properly shut down daily to allow for updates and to prolong battery life.

Carrying District Provided Devices

- Always transport your District Provided Device with care.
- Never lift the District Provided Device by the screen.
- Never carry the District Provided Device with the screen open.

Screen Care

The District Provided Device 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.

- Do not put pressure on the top of a District Issued Device when it is closed.
- Do not store a District Issued Device with the screen open.
- Make sure there is nothing on the keyboard before closing the lid (e.g. pens, pencils).

Asset Tags

- All District Provided Devices will be labeled with a District asset tag.
- Asset tags may not be modified or tampered with in any way.
- Students may be charged up to the full replacement cost of a District Issued Device for tampering with a District asset tag or turning in a District Issued Device without a District asset tag.

Printing

- Students are encouraged to digitally publish and share their work with their teachers and peers when appropriate.

Logging into a District Issued Device

- Students will log into their District Issued Device using their school issued Google Apps for Education account.
- Students should never share their account passwords with others, unless requested by an administrator.

Using Your District Issued Device Outside of School

A WiFi Internet connection will be required for the majority of District Issued Device use, however, some applications can be used while not connected to the Internet. ***Students are always bound by the district Use of Technology Policy, Administrative Procedures, acceptable use agreement, and all other guidelines wherever they use their District Issued Device***.

Updates

The District Issued Device operating system, updates itself automatically. Students do not need to manually update their District Issued Device. Devices need to be powered down daily for automatic updates.

Content Filter

The district utilizes an Internet content filter that is in compliance with the federally mandated Children's Internet Protection Act (CIPA). All District Issued Devices, regardless of physical location (in or out of school), will have all Internet activity protected and monitored by the district. If a website is blocked in school, then it will be blocked out of school. If an educationally valuable site is blocked, students should contact their teachers or the iCenter staff.

Software

District Issued Devices seamlessly integrate with the current education suite of productivity and collaboration tools. All work is stored in the cloud.

District Issued Device Identification

Records :
The district will maintain a log of all District Issued Devices that includes the District Issued Device serial number, asset tag code, and name and ID number of the student assigned to the device.

Users :
Each student will be assigned a specific District Issued Device to be used only by them.

District Issued Device Troubleshooting

A loaner District issued device may be issued when the assigned District Issued Device is being repaired.

Theft, Loss, and Repair

District Provided Devices that are broken or fail to work properly must be repaired by the person it is issued to. The district provides an optional insurance option. If one does not participate in the district insurance option, they are responsible for the full cost of repairs by the district device service provider. This also applies to loss and theft.

No Expectation of Privacy

Students have no expectation of confidentiality or privacy with respect to any usage of aDistrict Issued Device, regardless of whether that use is for district-related or personal purposes, other than as specifically provided by law. The District may, without prior notice or consent, log, supervise, access, view, monitor, and record use of District Provided Devices at any time for any reason related to the operation of the district.

By using a District Provided Device, students agree to such access, monitoring, and recording of their use.

Monitoring Software

Teachers, school administrators, and the technology department staff may use monitoring software that allows them to view the screens and activity on District Provided Devices.

Disciplinary Actions

Disciplinary actions for such violations will follow the Student Code of conduct and may include, but are not limited to:

- Confiscation of device.
- Restoration/Restitution.
- Student discipline pursuant to District discipline policies and procedures, including but not limited to suspension and expulsion.