Melbourne School District
Acceptable Use Policy (AUP)

Melbourne School District has policies in place that address all CIPA and FERPA laws. Guidelines regulating the use of the District technology (Acceptable User Policy) also include policies and consequences for violation of policies posted on the MSD website and in the student handbook. The AUP has been adopted by the Board of Education on ***06/22/2020.***

Melbourne School District is committed to promoting ethical and responsible use of computer and network resources.

- Instruction by, and not limited to, Library media specialists and technology instructors, and classroom instructors.
- All users will read and sign the acceptable user policy prior to logging in to any device. Parents of minors will also be required to sign the AUP acknowledging their awareness of student responsibility for district technology.

General

1. This policy governs the acceptable use of district technology by all users. The use of technology resources is a privilege, not a right, and should be treated as such. Access to the Internet and technology is provided for conducting school business and for the educational development of students and staff. They are not intended for private or personal use. By accessing and using technology, users acknowledge that inappropriate use is prohibited and may result in disciplinary action.
2. The Melbourne School District reserves the right to monitor or log all network activity with or without notice, including files, email and all web site communications, and therefore, users should have no reasonable expectation of privacy in the use of these resources. Routine maintenance and monitoring of the systems may lead to the discovery that a violation of law or regulation has occurred.
3. Users of the network are responsible for following local, state and federal laws. This includes copyright laws.
4. Users are responsible for the use of their own account, including security and proper use. Staff and students agree to keep his/her password private and agree to log out correctly. Users are not to allow others to use their username and password. Access to other user profiles is reserved for authorized network administrators.
5. Users may not store student or employee personal data on their personal computing, mobile or storage device.
6. Since students may use the school's computers in various classrooms, in labs, or in the library, it is his/her responsibility to know and understand the specific computer use rules (written or oral) applicable to each location.
7. Users may not gain unauthorized access or attempt to gain unauthorized access to other users' accounts, computer, or devices.
8. Users may not deliberately damage or attempt to damage or disrupt (otherwise known as hacking) a network, computer or computer related device, telephonic or other communication device, and/or removable media that they have been given authorized use. System components such as hardware, software, or other property will not be installed, removed, destroyed, modified or abused. Examples of activities that are prohibited: altering security codes or passwords, introducing viruses and/or malware, removing memory chips, hard drives and other hardware components.
9. No MSD network, phone, mobile device or computer system will be used to terrorize, intimidate, bully, threaten or harass.
10. Users will not use MSD resources for financial or commercial gain to advertise, promote or endorse products or personal services.
11. The district will not be responsible for financial obligations or legal infractions arising from unauthorized use of the technology.
12. All users (staff members, students and their parents) must sign an Acceptable Use Agreement to access the network and use district computers. This agreement must be renewed on an annual basis. Parents can withdraw approval at any time.

Hardware

1. Only authorized individuals will service or maintain District owned hardware, including relocation.
2. All personal hardware connected at any time to district systems are subject to MSD polices and must be authorized by the technology department.
3. Users are not permitted to connect to the Internet using a detected hot spot or 3G or 4G account while at school.

Software

1. Only software that is authorized by the District may be installed on computer hardware.
2. Only authorized individuals will install or remove software on District equipment. The district holds the right to remove any software that violates district software policy, software that is deemed illegal or inappropriate, or degrades system performance.
3. Authorized users of student and employee data will take proper care to guard the privacy of such information.
4. Software, apps, plugins, must be submitted for approval to ensure compatibility and safety.

Internet Access and Email

1. Before a student is allowed to access the Internet, the AUP must be signed by both the student and parent and will be kept on site.
2. School e-mail accounts will be issued to District employees and students grades 9-12. Students' in grades kindergarten through 8th grade will **not** be issued individual school email accounts, but may be provided access to email through a classroom account.
3. Users are not allowed to intentionally transmit or receive obscene, pornographic or inappropriately suggestive content or language in the form of images, files or multimedia file types through any synchronous or asynchronous communication device or software used in Melbourne School District.
4. All users should observe network etiquette. Users are expected to be polite and use appropriate language. Using vulgar or profane language is not appropriate. Engaging in flaming or spamming is not appropriate. Students are prohibited from using chat rooms and instant messenger services unless authorized for educational purposes. Participation in **cyber bullying** (original, secondary, or distributed is prohibited.
5. Users should report any inappropriate, illegal behavior or misuse of district technology to the technology department and building principals.

Technology Protection Measures

- The District is dedicated to protecting students from materials on the Internet that are inappropriate, obscene, or otherwise harmful to minors; therefore, it is the policy of the District to protect each device with Internet filtering software that is designed to prevent students from accessing such materials. The District will participate in the Arkansas Department of Information Systems (DIS) filtering system as an active restriction measure. District teachers and staff will make reasonable efforts to supervise student use of the network and Internet Access; however, they must have student cooperation in exercising and promoting responsible use of the technology.

Access to Programs

- Due to increased demand of data reporting in the district, it becomes necessary to allow certain personnel access to programs. These programs include, but are not limited to Teacher Access Center, Home Access Center, Eschool, Etrition, website, and social media. The access holds an incredible amount of responsibility due to the privacy issues of student records and users granted permission must abide by FERPA restrictions. The District technology department and Superintendent will determine and document using the following procedures:
    - Identify the school personnel that needs access
    - Document the purpose of the access
    - Document written approval by supervisor and/or superintendent
    - Length of time access should be granted
    - What rights are necessary and limited only to allow completion of job duty for user
    - Yearly review of users who have access to programs

Melbourne School District Social Media

The technology coordinator or his/her designee will be responsible for the creation of social media pages, web pages or the association of web pages to the district's home page. On occasion, a student's name and/or picture may appear on a school web page.

All users must maintain a high level of respect when using social media as a district employee or as students. Educators should follow the Arkansas Department of Education Rules Governing the Code of Ethics for Arkansas Educators when dealing with students in online activities.

Your Rights

- Users should expect only limited privacy in the contents of their personal files and email on the districts or schools network; they must realize that any information stored electronically on school-owned equipment is subject to Arkansas' Freedom of Information Act. The situation is similar to the rights staff and students have in regard to their lockers, desks, or other storage systems.

Disciplinary Actions:

All violations will be handled as any other infraction of school board policy. Disciplinary actions may include:

1. Revocation of computer access.
2. Financial restitutions.
3. Students: suspension, expulsion, academic failure due to lack of course completion, or other penalties as may be appropriate.
4. Employees: Up to and including termination of employment.
5. Possible referral for prosecution.

Limitations of Liability

The Melbourne School District makes no guarantees that the functions of the services provided by or through the network will be error-free or without defect. The district will not be responsible for any damage the user may suffer, including but not limited to, loss of data or interruptions of service. The district is not responsible for the accuracy or quality of the information obtained through or stored on the network. The district will not be responsible for financial obligations arising through the unauthorized use of the network.

This policy may be revised at any time by a vote of the Melbourne School Board of Directors or as state and federal law dictates.

Date: June 15, 2020
Revised: June 15, 2020
Approved: June 22, 2020
Melbourne School District

MELBOURNE PUBLIC SCHOOLS
Acceptable Use Policy (AUP) Authorization Form

STUDENT SECTION

School_____

Student Name_____Grade_____
(Please print)

I have read, understood and agree to abide by the terms of the foregoing Acceptable Use Policy. I understand and agree that access to the Melbourne School District's computer network and the Internet is a privilege and is designed for education purposes. It is further understood that violations of the regulations are unethical and may constitute disciplinary actions including revocation of access to technology, school disciplinary and/or appropriate legal action may be taken.

Student Signature_____ Date_____

PARENT or GUARDIAN SECTION

I have read the District Acceptable User Policy.

I hereby release the District, its operators, and any institutions with which they are affiliated from any and all claims and damages of any nature arising from my child's use of, or inability to use, the system, including without limitation, the type of damage identified in the procedures above. In addition, if the need arises, I agree to allow the above named student's name and/or picture to appear on authorized school web pages.

I will emphasize to my child the importance of following the rules for personal safety.

(PLEASE Check the appropriate box which indicates Parental choice)

☐ Permission granted for computer and Internet access

☐ Permission denied for computer and Internet access
(Students will be unable to access computers or the Internet in any location in the school setting.)

Parent Signature_____

Parent/Guardian Name (please print)_____

Date: _____/_____/_____

MELBOURNE PUBLIC SCHOOLS

Acceptable Use Policy (AUP) Authorization Form

Faculty

Employee Name_____
(Please print)

School/Location_____

I have read the Acceptable Use Policy for Melbourne Public School District. I understand and agree to abide by the stated terms and conditions set forth in this document. It is further understood that violations of the regulations are unethical and may constitute disciplinary actions including revocation of access to technology, termination of employment, or legal actions in the case of criminal activities.

It is extremely important that faculty **NEVER** share their passwords with students, because teachers and staff have more rights on the network than students. To protect the security of your own and other's files, please NEVER share your password with anyone and always log out when you leave your computer. Do not allow a student to use the computer with your log in name and password unless you are supervising them the entire time. This could lead to a breach of security.

User Signature:_____Date:_____