



Making Waves Academy Student Technology Acceptable Use Policy for Digital Information, Communication, and Technology Resources Agreement

Introduction

Making Waves Academy (MWA) provides access to technology devices, the internet, and data systems to the student(s), for educational purposes. This Acceptable Use Policy (AUP) governs students' electronic activity using Making Waves Academy technology, internet, and data systems regardless of location.

For example, MWA technology, internet, and data systems include but is not limited to:

- Chromebooks
- Laptops
- Laptop & Chromebook Chargers
- Headphones
- Internet
- Wifi HotSpots
- Built-in Webcams
- MWA Network
- MWA Email Account
- MWA Subscription to Digital Educational Programs

Those resources will thereafter be referred to as "MWA Technology." The purpose of this policy is to ensure a safe and appropriate environment for all students. This policy notifies students and families about the acceptable ways in which MWA Technology may be used.

Students must comply with this policy at all times when using MWA Technology (including but not limited to all items listed above), whether inside or outside of MWA campuses. No student may use MWA Technology until the agreement at the end of this policy has been signed by the student and their parent(s) or guardian(s) as applicable and returned to MWA. MWA reserves the right to change this policy at any time and will inform students and families of any material change by e-mail and notice in the next available mailing. Continued use of MWA Technology following MWA's notification of revisions to this policy constitutes acceptance of those revisions.

Guiding Principles

- Online tools are used in our classrooms, school, and central office to increase community engagement, student learning, and core operational efficiency.
- MWA has a legal and moral obligation to protect the personal data of our student(s).
- Nothing in this policy shall be read to unlawfully limit an individual's constitutional rights to freedom of speech or expression or to unlawfully restrict a student's ability to engage in concerted, protected activity with a fellow student regarding the terms and conditions during their time at Making Waves Academy.



Making Waves Academy Student Technology Acceptable Use Policy for Digital Information, Communication, and Technology Resources Agreement

IT & Device Support

MWA provides basic installation, synchronization, and software support for MWA-issued electronic devices. Devices must be connected to the MWA network on a regular basis to receive up-to-date software and antivirus updates and for inventory purposes. Password protection is required on all MWA-issued electronic devices to prevent unauthorized use in the event of loss or theft. All requests for support should be emailed to ithelpdesk@mwacademy.org or make an appointment on the [IT Curbside Support Calendar](#)

Passwords

Students must adhere to password requirements set forth by Making Waves Academy when logging into or using MWA Technology. Students are provided with MWA email addresses and passwords to support their use of MWA Technology. Students MUST not share their passwords and must use extra caution to avoid email scams that request passwords or other personal information.

Compliance Requirement for Students

The AUP is reviewed annually by MWA Leadership and is issued to student families via SchoolMint during registration and re-registration at the beginning of each school year. Students are required to verify that they have read and will abide by the AUP annually. MWA encourages parents/guardians to discuss this policy with their children to ensure their children understand and comply with this policy.

Student AUP & Agreement

Copies of the Acceptable Use Policy and the Student Chromebook Use Agreement are also included in the electronic registration packets for families & student(s). These packets are given to all student(s) at the beginning of the school year. Among the packet forms, student(s) are provided the Student Chromebook Use Agreement. This form must be completed and signed by all student(s) and their parents/guardians after going over the AUP together. The signed contract must be returned to the school before the student may begin using the Internet.

Procedures Governing Travel with a MWA Student Device Travel

While cell phones, laptops, and other electronic devices have become necessities, traveling with such devices occasionally poses challenges.

MWA students **shall not** travel with their MWA devices. Travel with MWA devices shall be permitted in limited circumstances, in compliance with the following procedures. The procedures outlined herein are implemented to ensure MWA devices and the safety of student information are not compromised.

Although MWA generally prohibits travel with MWA devices, MWA recognizes that there are situations that require a student to travel with a MWA device. To support MWA students' needs, while also ensuring the



Making Waves Academy Student Technology Acceptable Use Policy for Digital Information, Communication, and Technology Resources Agreement

secure use of MWA devices and the safety of student information and data, all students who need to travel with a MWA device shall follow the following procedures:

- Students or their parent(s)/guardian(s) are required to communicate travel plans to the school administration at least **15 days prior** to the trip to determine the type of technology support needed.
- If students do not have Chromebook insurance, we recommend that it is purchased **at thirty-five dollars (\$35)** before traveling to cover any loss or damages. *(If you have purchased Chromebook insurance during registration/re-enrollment, student devices are automatically covered.)* **If an MWA device is damaged or lost and the student's parent/guardian has not purchased Chromebook insurance prior to the damage or loss, the student's parent/guardian will be responsible for the full replacement costs as set forth below.**
- Students are required to comply with all terms and conditions of the MWA Student Technology Acceptable Use Policy for Digital Information, Communication, and Technology Resources Agreement when traveling with a MWA device.
- Students and their parent/guardian are required to review the following recommendations prior to the scheduled trip. To the extent possible, MWA students should comply with the recommendations outlined below to practice safe and secure technology use.

During travel, we recommend you consider the following:

Connect only to known Wi-Fi networks. Anyone can create a network and give the network a legitimate sounding name to lure unsuspecting travelers. These connections allow criminals to capture personal information transmitted through the network. This is especially common at public cafés, hotel lobbies, and airports.

Know what technologies, goods, and devices are subject to restrictions and export control licensing. If traveling to sanctioned countries or destinations that are otherwise impacted by export control restrictions.



Making Waves Academy Student Technology Acceptable Use Policy for Digital Information, Communication, and Technology Resources Agreement

Know what technologies and devices are subject to restrictions. If traveling to sanctioned countries or destinations that are otherwise impacted by export control restrictions. Know that when traveling with devices, be aware of which countries restrict or require licenses for importation of such devices/software (e.g., Cuba, Belarus, Burma/Myanmar, China, Hungary, Iran, Israel, Kazakhstan, Moldova, Morocco, Russia, Saudi Arabia, Tunisia, Ukraine)

*** For example, Zoom video conferencing is prohibited/ restricted in the following countries; use this [LINK](#) to see the document in its entirety. ***

- Cuba: For regulatory reasons, users in this country are currently unable to access Zoom services.
- Iran: For regulatory reasons, users in this country are currently unable to access Zoom services.
- North Korea: For regulatory reasons, users in this country are currently unable to access Zoom services.
- Syria: For regulatory reasons, users in this country are currently unable to access Zoom services.
- Ukraine (Crimea Region): For regulatory reasons, users in this region are currently unable to access Zoom services.

Do not leave your device unattended. Physically having control of your device is the easiest way for someone to access your data. If you ever leave your computer, make sure to secure it. Turn it off completely rather than using sleep mode. This makes unauthorized access more difficult.

Do not use untrusted accessories. Never plug in an untrusted accessory, including charging tools. Additionally, never use gifted or found USB or thumb drives.

Do not enter your credentials on untrusted or public access computers. Public computers, such as those at a hotel business center or internet café, are often poorly managed and provide minimal security protection for users.



Making Waves Academy Student Technology Acceptable Use Policy for Digital Information, Communication, and Technology Resources Agreement

Connect only to known Wi-Fi networks. Anyone can create a network and give the network a legitimate sounding name to lure unsuspecting travelers. These connections allow criminals to capture personal information transmitted through the network/internet.

***This is especially common at public cafés, hotel lobbies, and airports.*

Turn off your Wi-Fi and Bluetooth when not in use. Some devices connect to Wi-Fi automatically. Make sure that this feature is disabled on your device. The best practice is to turn off both Wi-Fi and Bluetooth when not in use.

*Practice safe web browsing. The websites you visit online hold valuable data about you. **Do not click through system or application warnings or error messages.***

*Be aware of targeted social engineering. ** This can take many forms, such as a dining invitation, shared ride, calendar invite, or an appeal to your helpfulness.***

*Note: **Providing details about your plans or personal life on social media makes targeting even easier. Avoid providing any travel details online in a publicly accessible format.***

After travel, we recommend you consider the following:

***Reset Passwords Used.** On a trusted device that you have access to, make sure to reset the password you used during the trip.*

If there are any technical difficulties with the MWA device and/or the loss of a MWA device while traveling with a MWA device, whenever possible, students or their parent/guardian shall notify the MWA IT Team emailing ithelpdesk@mwacademy.org with the details of the technical difficulties and/or information about the loss of the device. Students or their parent/guardian shall also contact the Chromebook insurer, and comply with all applicable requirements pursuant to the insurance coverage.



Making Waves Academy Student Technology Acceptable Use Policy for Digital Information, Communication, and Technology Resources Agreement

Consequences of Breach of Policy

Use of all MWA technology resources is a privilege, not a right. By using MWA's Internet Systems and devices, the student agrees to follow all MWA regulations, policies, and guidelines. Students are encouraged to report misuse or breach of protocols to appropriate personnel, including building administrators, direct supervisors, and the Instructional, Applied Tech, and Information Technology teams. Abuse of these privileges may result in one or more of the following consequences:

- Suspension or cancellation of use or access privileges.
- Payments for damages or repairs.
- Discipline under appropriate School Division policies, subject to any collective bargaining obligations.
- Liability under applicable civil or criminal laws.

Communication & Social Media

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

- a) when a student of the Making Waves Academy is communicating by sending an email*
- b) when the communication impacts or is likely to impact the classroom or working environment at Making Waves Academy.*

All communication sent by a student using district property or district business could be subjected to public access requests submitted through the Freedom of Information Act (FOIA). Student (s), staff, and faculty need to be aware that data and other material/files maintained on the school district's systems may be subject to review, disclosure, or discovery. Use of personal email accounts and communication tools to conduct school business is strongly discouraged and may open an individual's account and search history are subject to FOIA inquiries. MWA will cooperate fully with local, state, and federal authorities in any investigation concerning or related to any illegal activities or activities not in compliance with school district policies or government regulations

Important Laws¹

Freedom of Information Act (FOIA) - The FOIA is a law that allows for the release of government documents at an individual's request. An FOIA request can be made to the Making Waves Academy for electronic documents/communications stored or transmitted through district systems unless that

¹ The list of definitions (laws and other relevant definitions) is not exhaustive



Making Waves Academy Student Technology Acceptable Use Policy for Digital Information, Communication, and Technology Resources Agreement

information could be detrimental to governmental or personal interests. For more information, visit <http://www.foia.gov/>

Family Educational Rights and Privacy Act (FERPA) - The FERPA law protects the privacy, accuracy, and release of information for students and families of the Making Waves Academy. Personal information stored or transmitted by agents of the Making Waves Academy must abide by FERPA laws. MWA is required to protect the integrity and security of student and family information. For more information, visit <http://www.ed.gov/policy/gen/guid/fpco/ferpa/index.html>

Children's Internet Protection Act (CIPA) - requires schools that receive federal funding through the E-Rate program to protect student(s), staff, and faculty from content deemed harmful or inappropriate. Making Waves Academy is required to filter internet access for inappropriate content, monitor minors' internet usage, and educate students on safe and appropriate online behavior.

Cost of Equipment

If a violation of this policy results in willful damage to school devices or accessories, pursuant to Education Code Section 48904, the parent or guardian of a minor student shall be liable for the replacement cost for the school devices or accessories, up to an amount not to exceed ten thousand dollars (\$10,000), adjusted annually for inflation. The Division Director or his/her designee will decide the amount that needs to be reimbursed, which will not exceed the device's original cost or equipment. MWA may, after affording a pupil who has willfully cut, defaced, or otherwise injured MWA devices or accessories his or her due process rights and notifying his or her parent in writing, withhold the grades, diploma, and transcripts of the pupil responsible for the damage or loss until the pupil or the pupil's parent or guardian has paid for the damages. When the minor and parent are unable to pay for the damages, MWA will provide a voluntary work program for the minor in place of monetary damages. A student over the age of majority shall be liable for the same and shall have the same voluntary work option.

Roles and Responsibilities

1. The Information Technology (IT) Director, or their designee, will serve as the coordinator to oversee access to MWA technology and MWA responsibility, limitations, and rights contained in this policy.
2. The Sr. School Director, or their designee, will be responsible for disseminating this policy and enforcement of the student responsibilities in their division.



Making Waves Academy Student Technology Acceptable Use Policy for Digital Information, Communication, and Technology Resources Agreement

Student Responsibilities When Using MWA Technology:

	I will	I will not
General Use	<ul style="list-style-type: none"> ● Use MWA technology for educational purposes only ● Follow teacher and administrator instructions at all times ● Exclusively use the e-mail account provided by MWA ● Check my MWA e-mail daily ● Comply with state and federal law² 	<ul style="list-style-type: none"> ● Use MWA technology for non-educational purposes such as, but not limited to, commercial, illegal, religious, recreational, or political activities. ● Use my personal email account.
Digital Citizenship	<ul style="list-style-type: none"> ● Use appropriate, professional language in all digital communication ● Report any inappropriate (vulgar, profane, sexually explicit, hate-based, discriminatory, derogatory, or offensive) content to a teacher or administrator ● Report any suspicion of digital harassment or cyberbullying to a teacher or administrator 	<ul style="list-style-type: none"> ● Create, search, save, display, use or circulate inappropriate material, which includes, but is not limited to: <ul style="list-style-type: none"> ○ Vulgarity ○ Profanity ○ Sexually explicit content ○ Hate-based, discriminatory, derogatory, or offensive content ● Harass or bully others online ● Make public a message that was sent privately to me without authorization from the sender. ● Download large files unless necessary for educational purposes

² See the [Important laws](#) section for more details



Making Waves Academy Student Technology Acceptable Use Policy for Digital Information, Communication, and Technology Resources Agreement

	<ul style="list-style-type: none"> ● Notify a teacher or an administrator immediately if I believe my student account has been compromised ● Take any digital citizenship course required by teachers or administrators, including but not limited to: cyberethics, cybersecurity, digital safety, and cyberbullying ● Always cite the source of information I find online ● Check if the materials I find online are protected by copyright before using it 	<ul style="list-style-type: none"> ● Send chain letters or engage in spamming ● Plagiarize others' work without proper citation or permission ● Claim to be the author of material created by others ● Illegally download materials protected by licensing, copyright, or other intellectual property laws, including music and movies ● Load software without permission ● Engage in or support cyberbullying
Student Safety	<ul style="list-style-type: none"> ● Protect my password ● Log off at the end of every session ● Keep in mind that all my digital and online activities cannot be permanently erased. ● Pay attention to all security warning messages. ● Notify a teacher or administrator if I receive any digital communication that makes me feel unsafe or uncomfortable ● Notify a teacher or administrator if I see anything on the internet that makes me feel unsafe 	<ul style="list-style-type: none"> ● Allow others to use my account ● Send my password by e-mail or digital messaging ● Share personal information (address, phone, SSN, date of birth, photos, etc.) with strangers, or make it public. ● Meet in person with someone I met online. ● Accept a friend invitation on social networks from someone I don't know ● Post photos of others without their permission ● Post private information about another person ● Opening e-mail from people who I don't know and don't work at MWA ● Click on links or open files sent by people who I don't know and don't work at MWA
Devices and Network	<ul style="list-style-type: none"> ● Report security problems or breaches to a teacher or administrator ● Keep in mind that the school 	<ul style="list-style-type: none"> ● Bypass security or internet filters (install or utilize proxies) ● Attempt to capture others' password ● Attempt to modify unauthorized



Making Waves Academy Student Technology Acceptable Use Policy for Digital Information, Communication, and Technology Resources Agreement

	<p>owns the device and networks, and there is no expectation of privacy while I'm using them, inside or outside of MWA campuses</p> <ul style="list-style-type: none"> ● Take good care of all devices 	<p>settings</p> <ul style="list-style-type: none"> ● Impersonate or pretend to be someone else online ● Attempt to gain access to restricted or unauthorized accounts, network services, or devices (hacking) ● Tamper with computer hardware or software ● Vandalize data, devices, or any technology resources provided by MWA ● Invoke computer viruses or malware ● Attempt to interfere with the device antivirus or any security application present on any device or system. ● Attempt to modify or obscure my IP address, or that of others ● Work directly on teacher or MWA websites without express written permission from Making Waves Academy IT Director ● Create unauthorized wireless networks to access MWA's network. MWA networks include establishing wireless access points, wireless routers, and open networks on personal devices
<p>Device Care</p>	<ul style="list-style-type: none"> ● Close the lid and use both hands when transporting it ● Put it inside a backpack to transport it outside of school ● Power down when not using it ● If I take it home, charge it at home every night <ul style="list-style-type: none"> ○ In case I'm unable to charge it at home for reasons outside of my control, I will notify a teacher or administrator. 	<ul style="list-style-type: none"> ● Loan it to other individuals; ● Place heavy objects on top of it ● Alter its appearance or function in any way (including stickers, magnets, etc.) ● Eat or drink while using it ● Leave it unattended (including inside a car) ● Place it in locations prone to be damaged, i.e., on a playground, sports field, or thoroughfare. ● Keep it near young children or pets ● Remove factory or MWA tags ● Intentionally damage or disrupt it



Making Waves Academy Student Technology Acceptable Use Policy for Digital Information, Communication, and Technology Resources Agreement

	<ul style="list-style-type: none"> • Inform IT immediately of any malfunction by reporting the issue to a teacher or administrator or who can direct me to the IT office for support • Keep it in a secure place at all times • Use it on stable surfaces • File a police report in case of theft and provide it to MWA within two (2) business days of the incident • Return it to MWA when requested 	<ul style="list-style-type: none"> • Connect unauthorized equipment to it, including USB devices and SD cards • Disassemble or attempt to repair it
Loss/Theft	<ul style="list-style-type: none"> • Students must take reasonable measures to prevent a device from being lost or stolen. 	<ul style="list-style-type: none"> • Suppose an electronic device is lost or stolen. In that case, the student is required to immediately notify appropriate school staff and their direct supervisor, local authorities, and the MWA IT Service Desk via email ithelpdesk@mwacademy.org or schedule an appointment using the IT Curbside Support Calendar.
Distant Learning /Video Meetings	<ul style="list-style-type: none"> • Disable cameras and microphones before entering a video meeting • Only enable cameras and microphones when instructed • Use the appropriate tools to ask a question • Be the only person on camera • Be in a safe and appropriate environment • Report any unsafe behavior to the Dean of Students 	<ul style="list-style-type: none"> • Display inappropriate content on cameras • Screenshare inappropriate content • Say inappropriate content on microphones • Write inappropriate messages • Spam chat



Making Waves Academy Student Technology Acceptable Use Policy for Digital Information, Communication, and Technology Resources Agreement

General use

MWA will provide students access to technology for educational purposes. MWA reserves the right to revoke or restrict student usage of technology anytime to apply disciplinary actions for this policy's violations.

Limitation of Liability

1. MWA makes no warranties of any kind, either express or implied that the functions or the services provided by MWA technology would be error-free or without defect. MWA will not be responsible for any damage students may suffer, including but not limited to loss of data, missed deliveries, or interruptions of service. The student and parent agree not to hold MWA for the accuracy or quality of the information obtained through or stored on MWA technology or for any claim of damage, negligence, or breach of duty resulting from the use of MWA technology. MWA will not be responsible for financial obligations arising from a student's unauthorized use of the system.
2. Students will indemnify and hold MWA harmless from any losses sustained by MWA due to intentional misuse of the student's system.
3. MWA will not support MWA technology when the school is not operating (after school hours, holidays, and school breaks).
4. Parents/guardians are required to supervise and monitor their child's use of MWA Technology, including but not limited to their child's access to the internet and any online services through MWA Technology any and all times during which any MWA Technology is being used by their child outside school facilities or school hours to ensure compliance with this policy.

Content filtering

MWA has installed Internet filtering software in a best-effort attempt to block student access to inappropriate and/or harmful content on the Internet. No filtering technology is perfect, and this technology may occasionally fail. In the event that the filtering software is unsuccessful and student(s), staff, and faculty gain access to inappropriate and/or harmful material, MWA will not be liable.

MWA filtering systems adhere to the US Congress enacted CIPA (Children's Internet Protection Act) guidelines, updated 2011: <http://www.fcc.gov/guides/childrens-internet-protection-act>

Guidelines for Online Communication

MWA advises students:

- Never share passwords, personal data, or private photos online.



Making Waves Academy Student Technology Acceptable Use Policy for Digital Information, Communication, and Technology Resources Agreement

- Think about what they are doing carefully before posting and emphasizing that comments cannot be retracted once posted.
- That personal information revealed on social media can be shared with anyone, including parents, teachers, administrators, and potential employers. Students should never disclose information that would make them uncomfortable if the world had access to it.
- To consider how it would feel to receive such comments before making comments about others online.

Solicitation

Web announcements and online communication promoting a business are prohibited by the MWA Solicitation Policy, exceptions if benefits are judged sufficient and adhere to MWA policies.

Privacy

Student(s) should not expect privacy while using MWA technology.

1. MWA reserves the right to monitor the use of the internet through its system at all times.
2. As required by the Children's Internet Protection Act ("CIPA"), MWA will monitor students' online activities. Such monitoring may lead to a discovery that the student has violated or may be violating, MWA Technology Acceptable Use Policy, the Student-Family Handbook, discipline policies, or the law.
3. MWA reserves the right to employ and review the results of software that searches, monitors, and/or identifies potential violations of the Technology Acceptable Use Policy.
4. Students of MWA technology should be aware that their files may be discoverable in court and administrative proceedings and accordance with public records laws.
5. Students of MWA technology should have no privacy expectation in the contents of their files and records of their online activity while on MWA technology. MWA does not encourage student(s), staff, and faculty to store personal data on MWA technology - MWA cannot be responsible for the loss or damage of such data.
6. MWA will cooperate fully with local, state, or federal officials in any lawful investigation concerning or relating to illegal activities conducted through MWA technology.

Important Laws³

³ The list of definitions (laws and other relevant definitions) is not exhaustive



Making Waves Academy Student Technology Acceptable Use Policy for Digital Information, Communication, and Technology Resources Agreement

1. Relevant Laws:

- a. **Copyright** - A form of protection provided by the United States laws for "original works of authorship," including literary, dramatic, musical, architectural, cartographic, choreographic, pantomimic, pictorial, graphic, sculptural, and audiovisual creations. Violations of copyright law that occur while using the MWA network or other resources are prohibited and can create liability for the district and the individual. MWA student(s), staff, and faculty must comply with regulations on copyright plagiarism that govern the use of material accessed through the MWA's network. "Copyright" literally means the right to copy but has come to mean that body of exclusive rights granted by law to copyright owners for protection of their work. Copyright protection does not extend to any idea, procedure, process, system, title, principle, or discovery. Similarly, names, titles, short phrases, slogans, familiar symbols, mere variations of typographic ornamentation, lettering, coloring, and listings of contents or ingredients are not subject to copyright.⁴ student(s), staff, and faculty will refrain from using materials obtained online without requesting permission from the owner of the material's use has the potential of being considered copyright infringement. MWA will cooperate with copyright protection agencies investigating copyright infringement by students of Making Waves Academy's computer systems and network.
- b. **Plagiarism** - To plagiarize is⁵:
 - i. to steal and pass off (the ideas or words of another) as one's own
 - ii. to use (another's production) without crediting the source
 - iii. to commit literary theft
 - iv. to present as new and original an idea or product derived from an existing source
 - v. unauthorized collaboration with peers or others

In other words, plagiarism is an act of fraud. As defined in section 3294 of the California Civil Code, "Fraud" means an intentional misrepresentation, deceit, or concealment of a material fact known to the defendant with the intention on the part of the defendant of thereby depriving a person of property or legal rights or otherwise causing injury.

- c. **Cyberbullying** - is the "willful and repeated harm inflicted through the use of computers, cell phones, and other electronic devices." The key elements include the following:
 - i. Willful: The behavior has to be deliberate, not accidental.
 - ii. Repeated: Bullying reflects a pattern of behavior, not just one isolated incident.
 - iii. Harm: The target must perceive that harm was inflicted.

⁴ Source: [US Copyright Office](#)

⁵ Source: [Plagiarism.org](#)



Making Waves Academy Student Technology Acceptable Use Policy for Digital Information, Communication, and Technology Resources Agreement

iv. Computers, cell phones, and other electronic devices: This, of course, is what differentiates cyberbullying from traditional bullying⁶

The most common places where cyberbullying occurs are⁷:

1. Social Media platforms, such as Facebook, Instagram, Snapchat, and Twitter
2. SMS (Short Message Service), also known as Text Message sent through devices Instant Message (via devices, email provider services, apps, and social media messaging features)
3. Email - Bullying in all forms, including cyberbullying, is regulated by the California Education Code,⁸ and student(s), staff, and faculty found responsible for engaging in any form of bullying are subject to disciplinary action per the Family Handbook and Suspension and Expulsion Policy.

d. **Hacking** - is an unauthorized intrusion into a computer or a network. The person engaged in hacking activities is generally referred to as a hacker. This hacker may alter system or security features to accomplish a goal that differs from the original purpose of the system⁹. Accessing a computer system without authorization is illegal under various circumstances, under the United States Code, Title 18, Chapter 47, Sec 1030¹⁰.

e.

2. Other Relevant Definitions

a. **Chain emails** - are those that ask the recipient to forward the email to multiple people in the body or subject of the message. Many chain letter emails are hoaxes and/or scams and are often considered to be a security and privacy risk. If a person forwards the message on, it will usually show the names and email addresses of everyone you have sent it to, and possibly the addresses of everyone the last person (from which you received it) also sent it to. The risk is that you do not know if an unscrupulous or malicious person will receive the email with all the email addresses and what they might choose to do with that list. Many consider chain e-mail to be a type of spam¹¹.

b. **IP address** - A unique number assigned by an Internet authority that identifies a computer on the Internet. The number consists of four groups of numbers between 0 and 255, separated by periods (dots). For example, 195.112.56.75 is an IP address¹².

⁶ Source: [Cyberbullying Research Center](#)

⁷ Source: [Stopbullying.gov](#)

⁸ Source: Stopbullying.gov, [California State information](#). The California Code of Education can be found [here](#)

⁹ Source: [Techopedia](#)

¹⁰ Source: [Office of the Law Revision Counsel](#)

¹¹ Source: [Webopedia](#)

¹² Source: [Gartner IT Glossary](#)



Making Waves Academy Student Technology Acceptable Use Policy for Digital Information, Communication, and Technology Resources Agreement

- c. **Malware** - In full malicious software, malicious computer programs, or “malicious software,” such as viruses, trojans, spyware, and worms. Malware typically infects a personal computer (PC) through email, Web sites, or attached hardware devices¹³.
- d. **Phishing** - Act of sending e-mail that purports to be from a reputable source, such as the recipient’s bank or credit card provider, and that seeks to acquire personal or financial information. The name derives from the idea of “fishing” for information¹⁴.
- e. **Proxy or proxy sites** - A proxy or proxy site hides the person’s identity using them and allows access to content or websites blocked by the MWA firewall or content filters.
- f. **Spam** - Usenet messages flooded many newsgroups indiscriminately. The term is also loosely applied to junk mail¹⁵.

¹³ Source: [Encyclopedia Britannica](#)

¹⁴ Source: [Encyclopedia Britannica](#)

¹⁵ Source: [Gartner IT Glossary](#)