match EDUCATION | Match Charter Public School

Acceptable Use Policy For:

MATCH CHARTER PUBLIC SCHOOL

1. Purpose and Acceptable Use

a. Match Charter Public School ("Match") provides and maintains computer systems and network resources to support the delivery of education and the administration of Match's operations. These include desktop workstations, laptops, handheld smart devices, applications, internal networks (both wired and wireless), servers, online databases, and access to outside networks, including the internet (collectively referred to herein as "computing systems"). This policy applies to all users of Match computing systems, including Match employees, volunteers, independent contractors, students and guests.

b. Match permits its employees and volunteers to use the Match computing systems for incidental personal use as long as the computing systems are not used in a manner that violates this policy and such use is limited to times before or after work hours, during non-assigned teaching or duty time, and lunch periods.

c. This policy describes acceptable and unacceptable uses of Match computing systems, but these descriptions are not exhaustive lists of all acceptable or unacceptable uses. Any user who has a question regarding whether or not a particular activity is acceptable should seek guidance from the user's supervisor (for staff), or principal (for students).

2. Access to Match Computing Systems

a. Staff. New staff members will receive this policy via the Match Employee Handbook. With supervisor permission, Match staff members will have access to the following computing resources through their classrooms, offices, library media centers, and/or computer and mobile labs: e-mail including conferencing and collaboration tools, web hosting, online subscription databases and information services, Match servers for secure file storage, and all resources and tools found on the internet/world wide web. Computing resources at Match may change as technology develops. These changes will fall within the purview of this policy as well.

b. Students. Students will have appropriate access to the internet and the Match networks through the schools' computers to fulfill school related tasks. Students may only use Match computing systems for educational purposes. Students (and, for Match students, their families) will receive this policy via the Student and Family Handbook or it will be separately distributed.

c. Other Users. Guest accounts may be established. Temporary staff or independent contractors, for example (e.g., long term substitutes, service vendors, interns, student teachers, community education instructors, therapy specialists, volunteers), may have guest accounts. A guest's access may be limited.

3. **Disclaimer**

a. Match makes no warranties of any kind, either express or implied, that services provided through its computing systems will be error–free or without defect. Match is not responsible for the accuracy or quality of the information obtained through its computing systems. Users of Match's computing systems assume full responsibility for their use including, but not limited to, loss of data, interruptions of service, costs, liabilities, or damages.

4. Ownership/Privacy

a. Match computing systems are the property of Match. As such, a user's activities and files are subject to inspection by certain staff members at any time. Match has the right to monitor and log the usage of any and all aspects of its computing systems, including, but not limited to, monitoring internet usage, file downloads, and all communications. Match actively maintains and updates its networks and computing environment by integrating appropriate controls in support of this policy. Tools used may include, but are not limited to: monitoring devices, content filtering, virus protection, log-on utilities, virtual networks, user access profiles, and security settings.

b. Users should not have an expectation of privacy regarding any use of Match computing systems. To be specific, any document, email or other communication that is creates, accessed, stored, sent or received on Match computing systems, including communications on personal email accounts (Gmail, Yahoo, etc.) or on social media sites such as Facebook, Instagram and Twitter which are accessed using Match computing systems, are not private.

c. E-mail that is created or received by an employee of Match is a matter of public record and may be subject to public production in accordance with Massachusetts public records laws.

5. Unacceptable Uses

a. Match computing systems may not be used for political advocacy.

b. Match computing systems may not be used for entertainment, illegal purposes (or support of illegal activities), or commercial purposes such as, but not limited to, offering, providing or purchasing goods and/or services for personal use or gain. In addition, Match computing systems cannot be used as a public access service or a public forum. As such, Match reserves the right to place reasonable restrictions on the materials users can access or post through the Match computing systems.

c. Users may not use Match computing systems to obtain or share information about staff, students or families for any non-school purpose.

d. Users are prohibited from copying copyrighted material without authorization from the copyright holder unless the copies are used for teaching (including multiple copies for classroom use), scholarship or research. If there is uncertainty as to the extent of copyright protection for internet materials, users must obtain permission to use material from the copyright holder.

e. Users shall not attempt to gain unauthorized access to files or accounts using Match computing systems.

f. Users shall not vandalize Match computing systems by, for example, causing physical damage, reconfiguring a computer operating system, attempting to degrade or disrupt Match computing systems, or destroying data by spreading computer viruses or by any other means. Anyone found to intentionally vandalize Match computing systems shall be subject to disciplinary measures and shall be responsible for the costs associated with hardware, software, equipment, materials, data recovery and/or system restoration.

g. Users shall not pretend to be someone else when sending or receiving electronic communications.

h. Use of another person's password or account is strictly prohibited.

i. It is unacceptable to attempt to read, delete, copy, or modify the electronic communications of other users or to interfere with other users' ability to send or receive communications.

j. Users shall not access, send, or forward materials or communications that are defamatory, pornographic, obscene, sexually explicit, threatening, harassing, profane, or inflammatory.

k. Users shall not download or install any commercial software, shareware, freeware, or similar types of materials on Match computing systems without prior approval and authorization from the Director of Technology or designee.

l. Users shall refrain from actions or language via email, instant messaging, or any other online mode of communication that is discriminatory, or harassing or threatening to others and which may be in violation of Match's Bullying Prevention Plan, Code of Conduct or Harassment and Discrimination Policy. Users shall refrain from swearing, using vulgarities or using any other inappropriate language or images.

6. Employee Guidelines for Social Media Use

a. When Match employees post content on social media, regardless of whether Match computing systems of personal computing systems are being used, the following guidelines apply:

i. Employees may not post personal identifying information about current or former students or other staff members.

ii. Employees may not post information that can be considered discriminatory, offensive, obscene, threatening, harassing, intimidating, offensive, disruptive, or may constitute bullying. Employees are personally and legally responsible for the information posted.

iii. Employees are strongly encouraged to manage their privacy settings to prevent public viewing of any social media presence that they would not want students, families, parents or colleagues to see.

iv. Employees may not communicate with Match students using personal social media accounts, including adding students as "friends" or "following" students on social media networks such as Facebook or Instagram.

v. Employees may not create a link from a personal blog, website, or other social media site to Match's website unless it is authorized by the employee's supervisor.

vi. Use of the Match logo or letterhead on a blog, website, or other social media site is strictly prohibited.

vii. Employees may not represent themselves as spokespersons for Match. If an employee publishes a blog or post online related to the employee's work at Match, such employee must clearly state that the employee is not speaking on behalf of Match. It is best to include a disclaimer such as "The postings on this site are my own and do not necessarily reflect the views of Match."

viii. Employees should refrain from using social media during work hours either on Match computing systems or on personal devices, unless such use is work-related and authorized by the employee's supervisor.

7. Internet Safety

a. Use of the internet has potential dangers. All users and parents of Match students are encouraged to read information that the Massachusetts Office of the Attorney General has published on Cyber Crimes and Internet Safety which is found on the Commonwealth of Massachusetts government website

www.mass.gov. Search "Attorney General" to find the website of the Office of the Attorney General, where you will find "Cyber Crimes and Internet Safety" under the "Public Safety" heading. Additionally, all students will participate in the Match anti-bullying curriculum as set forth in the Bullying Prevention Plan.

b. All users are granted individual accounts and agree to keep passwords secure. Users are responsible for their accounts, credentials, security codes, and passwords and will not share or allow others access to them. Users are responsible for keeping these secured and for reporting any suspected breach to their supervisor (for staff) or principal (for students).

c. Users will refrain from revealing private information (e.g., addresses, phone numbers) in any school-related electronic communications including communications via email, the internet, or other network tools. Specifically, all users should refrain from revealing personal or private information on any commercial or other internet media sharing site (e.g., Facebook; Instagram, TikTok, Twitter, chat rooms), particularly if these are not school sponsored or hosted sites. Match computing systems should not be used to meet or arrange to meet unknown people.

d. When accessing the school's resources and data from any systems (including when outside the Match networks), staff and volunteers will use due caution to protect the privacy and integrity of student data.

e. Match reserves the right to use filtering technologies to help control users' access to inappropriate internet content and websites while using its networks.

f. Students may only use the internet for educational purposes. Personal use of social media websites (e.g. Facebook, Twitter, Instagram, TikTok, etc.) and chat rooms is strictly prohibited.

g. Any Match employee who wishes to implement the use of certain educational websites in the classroom must follow these procedures:

    a. The employee shall submit a request to the principal, and the principal will inform the staff member whether the educational use of a certain website in the classroom is permitted.

    b. Upon approval, the principal will inform the website coordinator at the school. The website coordinator of each school shall maintain a list of educational websites that are being used by students for educational purposes on its website, which shall be updated from time to time.

    c. In the event that students must be registered for an account in order to use a particular website, staff members shall obscure student information to the extent practicable (i.e., first name, last initial; or initials, matcheducation, etc.).

8. Data and Control

a. Match has the right to re-image any computer as necessary.

b. Match is responsible for the provision, installation, maintenance, and licensing of all software deployed in its computing systems.

c. No personal data or files may be stored on a Match network or computer.

d. Match provides all users with network accounts and data storage. It is the users' responsibility to ensure that all files and data are stored in their appropriate locations. Match conducts regularly scheduled backups to prevent against loss or corruption. However, Match cannot guarantee that all information can be recovered in the event of a catastrophic failure.

e. Responsibility for backing up any hand held or mobile device issued to a user falls upon the user. Match is not responsible for providing backups for these devices.

9. Hardware/Software

a. Any and all equipment issued by Match for use by any user must be treated with due care. All users are responsible for ensuring equipment is not damaged or stolen. Abuse, damage or improper use should be reported immediately to a user's supervisor or the Director of Technology (for staff) or principal (for students).

b. Any and all issues or problems related to any hardware, software, system or network must be reported to the Director of Technology.

10. **Violations**

a. Access to Match's computing systems is a privilege and not a right. Match reserves the right to deny, revoke, or suspend specific user privileges, and/or to take disciplinary action up to, and including, suspension, expulsion (for students), and dismissal (for staff and volunteers for violations of this policy.

b. Match will advise appropriate law enforcement agencies of any illegal activities conducted using Match's computing systems. Match also will cooperate fully with local, state and/or federal officials in any investigation related to any illegal activities conducted through the Match computing systems.

c. Match prohibits retaliation against any staff member for reporting a possible violation of this policy or for cooperating in an investigation. Any staff member who retaliates against another user for reporting a possible violation of this policy or for cooperating in an investigation will be subject to disciplinary action, up to and including termination.

Updated: June 2023