File: IJNDBA

MARBLEHEAD PUBLIC SCHOOLS

INTERNET ACCEPTABLE USE POLICY FOR FACULTY/STAFF

Responsibility

Access to Marblehead Public Schools' ("MPS") network systems, email, Internet, intranet, student records, and other computer or technological resources (collectively, the "MPS Network Systems") is provided for educational and MPS administrative use exclusively. This AUP governs all use of the MPS Network Systems and includes the use of personal equipment and accounts on the MPS Network Systems.

Prohibited Uses: Each employee is responsible for his/her actions involving information technology and his/her computer files, passwords and accounts. Examples of prohibited use of the MPS Network Systems include, but are not limited to, the following:

1. Any use that violates any federal, state or local law or regulation, or violates a School Committee policy;
2. Any use to harass, discriminate, threaten, defame, demean or intimidate another person(s);
3. Any use that involves material or language that is profane, obscene, fraudulent, offensive, sexually explicit or sexually suggestive, or vulgar;
4. Any commercial use, use for private financial gain, advertising, or solicitation purposes;
5. Obtaining or sharing confidential information for non-school related purposes;
6. Revealing your password to anyone else or failing to take reasonable precautions to properly safeguard your password, using another's password without administrative approval, allowing another person to use your account or using another person's account, or gaining or attempting to gain unauthorized access to any computer or network;

7. Any misuse, disruption, or degradation of the MPS Network Systems, including intentional physical misuse or damage to equipment, materials, data, or programs, or any breach or attempt to breach the security features of school IT;
8. Any use which fails to comply with or violates software license agreement terms, copyright, or other intellectual property rights of other persons.

Privacy

Users do not have any expectation of privacy or confidentiality in the content of electronic communications or of other files sent and received or stored in the user's directory or on a disk drive or any other storage type device or print-out. The use of a password is solely to protect the user's information from access by fellow users, but creates no expectation of privacy with regard to access to that information by authorized MPS employees. MPS reserves the right to review and/or monitor all electronic records and communications, at any time, with or without notice, including individual user folders and other information, whether such records, communications, folders, and information are password-protected or not. All communications including text and images may be disclosed to law enforcement or other appropriate third parties without the prior consent or knowledge of the sender or the receiver.

Violations

The district reserves the right to deny, revoke or suspend specific user privileges and/or to take other disciplinary action, including suspension or dismissal from one's position, for violations of this policy. The district will advise appropriate law enforcement agencies of illegal activities.

Complaints or Problems of Misuse

Any individual who is aware of any violation of this policy must report such violations to the Building Principal or IT Department.