Information Systems Rules of Behavior

Effective Date:	Changes:	Approved by:	Version:
February 17, 2020	Initial Implementation	MACS Management	1.0
February 17, 2021	Personal Devices & Remote Access	MACS Management	1.1

1. Overview

The **MicroSociety Academy Charter School (MACS)** Information Systems Rules of Behavior defines the scope and responsibilities of each employee that has any level of access to the MACS Information System. This policy also provides an overall description of the data protection approach at MACS.

MACS Information System is defined as, but not limited to anything that includes data that resides on, is transferred to or is created by a MACS system. This includes, but is not limited to: laptops, desktops, tablets, mobile devices including smart phones, servers, network equipment, telecommunication systems, local wired, wireless and wide area networks, cloud and hosted systems, paper and electronic communications.

Proper usage of MACS Information Systems is critical to the success of the school. It is every employee's responsibility to fully understand and follow the rules set forth in this "Rules of Behavior" policy. All employees must acknowledge their understanding and sign off on receipt of this required policy before being granted access to MACS Information Systems.

Inability or negligence in following these rules may result in removal of access and or disciplinary action by MACS. Certain violations may also result in prosecution under local, State and or Federal laws.

2. Definitions

For the purpose of this policy, "protected information" will refer to all personal and confidential information, defined below.

Personal Information entrusted to MACS includes personal data that is protected under state data privacy regulations (such as NH RSA 359-C:20 and MA 201 CMR 17), the Family Educational Rights and Privacy Act Regulations (FERPA) 34 CFR §99.3, and NH's Student and Teacher Information Protection and Privacy RSA 189:66

Personally Identifiable Information (PII) refers to any information about an individual that could be used to *distinguish or trace* an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, or biometric records.

As MACS is a K-8 educational institution in the state of New Hampshire, the personal information of students and teachers are protected by state and federal regulations. These regulations expound upon the broader definition of PII to require the protection of Student and Teacher Personally-Identifiable Data and Education Records:

Student Personally-Identifiable Data under RSA 189:65 includes PII identifiers related to a student as well as the student's name, the name of the student's parent or other family member's, the address of the student or student's family, email, social media address, or other electronic address, telephone number, credit card account number, insurance account number, and financial services account number.

Teacher Personally-Identifiable Data under RSA 189:65 includes PII identifiers related to teachers, paraprofessionals, principals, school employees, contractors, and other administrators. It also includes personal street address, personal email address, personal telephone number, and performance evaluations.

Education Records protected under the Family Educational Rights and Privacy Act Regulations (FERPA) 34 CFR §99.3 are records that are directly related to a student and that are maintained by an educational agency or institution or a party acting for or on behalf of the agency or institution. These records include but are not limited to grades, transcripts, class lists, student course schedules, health records (at the K-12 level), student financial information (at the postsecondary level), and student discipline files.

Directory Information means information contained in an education record of a student that would not generally be considered harmful or an invasion of privacy if disclosed. Directory information includes, but is not limited to, the student's name; address; telephone listing; electronic mail address; photograph; date and place of birth; major field of study; grade level; enrollment status (e.g., undergraduate or graduate, full-time or part-time); dates of attendance; participation in officially recognized activities and sports; weight and height of members of athletic teams; degrees, honors, and awards received; and the most recent educational agency or institution attended.

Directory information can be released without a parent or eligible student's explicit consent if MACS has provided eligible students and parents with the option to opt-out of having directory information disclosed.

For the purpose of Directory Information, "release" refers to providing information to a third party. Common situations in which directory information is released (provided a parent or eligible student has not opted out of disclosure) include, but are not limited to:

- Publications including newsletters, social media, and/or yearbooks;
- Honor roll or attendance award recipients made available in newspapers;
- Manufacturers of school uniforms, rings, or yearbooks; and
- Third-party educational resources/applications used in the classroom that collect student email addresses and/or name.

Confidential Information means all sensitive, private information disclosed by one party to the other such as financial and personal information including without limitation. This information includes but is not limited to Personal Financial Information (PFI), Federal Tax Information (FTI), Payment Card Information (PCI) and or other sensitive and confidential information. Confidential information may include data protected by state and/or federal regulations or contractual obligations.

3. Employee Account Access Control

User Accounts and Passwords: Access to the organization's network will require employees to successfully log in with usernames and passwords. These accounts will provide system access based on job responsibilities tied to role-based access, least privilege principles and separation of duties.

The utmost care must be taken to safeguard your account credentials and MACS' Information Systems. It is each employee's responsibility to safeguard passwords. Unless otherwise specified for specific access and roles, MACS' general password policy is as follows:

a) Accounts are created only at request of the Director or the Curriculum Coordinator.
b) Accounts are reviewed every 12 months at minimum, reviewing for both active/inactive accounts and appropriate permissions levels.
c) All permissions are assigned on a least-privilege basis.
d) All permissions are assigned per role-based access.
e) All permissions are assigned per separation of duties.
f) Passwords should never be written down or left in an openly accessible place.
g) Employees must report any compromise of password immediately to the Director and the Curriculum Coordinator.
h) All users have unique usernames.
i) All passwords (memorized secrets) used to access MACS data and systems must follow these requirements wherever technically feasible:
    i. Be a minimum of 12 characters in length although more characters (up to 64) will make your password more secure. Spaces and special characters may be used and are encouraged.
    ii. Avoid the use of dictionary words to create your password.
    iii. Avoid common variations that could easily be guessed (e.g. family member names, local sports teams and obvious milestone dates)
    iv. Avoid easy character mapping. a = @, S = $, B = 8 etc. These characters are easily mapped in automated password cracking programs.

v. Do not use repetitive or sequential characters (e.g. aaaaaa, or 1234abcd).
vi. All passwords are unique to their usage. Employees should never use the same password for different systems or applications.
vii. Passwords should be changed if they are forgotten or if you believe your password may have been compromised.
viii. Passwords that were previously breached should be replaced and never used again.

j) Technical support assistance may be required but you should never offer up your password or share any account information with a source that has not been fully vetted and validated.
k) Default passwords are changed on all devices.
l) All computers should always be locked when unattended.
m) System administrative accounts are used for administrative use only, and not general use.
n) Accessing a system via another employee's login, snooping, or trying to ascertain another employee's password is strictly prohibited.

System Access: All system and data access is granted by MACS Director and Curriculum Coordinator (MACS Management) based on employee job function. Any changes to system and data access must be documented, coordinated and approved by the MACS Director or Curriculum Coordinator. MACS follows a Change Management process to ensure we maintain stable, available and highly efficient environment.

Remote Access, Work from home & Telecommuting: MACS may authorize specific roles and or employees to have remote access to the Information System. Employees must receive written approval to work remotely from MACS' Director or Curriculum Coordinator. This includes accessing any MACS resources or information (in either digital or paper format) outside of the school location. Accessing emails, grading exams, etc. offsite would be considered working remotely.

Remote access may introduce additional security risk to the Information System. To address this risk, all job functions that allow remote access must adhere to the following security requirements:

a) Follow password and account control guidelines.
b) Documented approval from MACS Management for role and or employee remote access.
c) Limit log on times where appropriate.
d) Access is only allowed via MACS owned or approved equipment.
e) Multi-Factor authentication is enabled where technically feasible.
f) Exercise appropriate environmental, operational, technical and management controls and best practices in the remote environment necessary to protect MACS data at ALL times.
g) Escalate any incidents immediately to MACS Director and Curriculum Coordinator based on reliability, security and or access to the Information System.
h) All sensitive data protections, policies and procedures must be adhered to for alternate work sites.
i) It is understood that this access may be considered a privilege that is outside of required job functions. This privilege may be revoked at any time without notice if violations of security requirements, best practices or the perception of misuse occurs.

4. Asset Management

Third-Party Tools: MACS recognizes the benefit of technology within our students' education and is mindful of the importance of providing a wide range of technologies to promote our educational objectives. However, MACS is required to ensure that any third-party systems or applications that necessitate the input of data protected under RSA 189:66 meet or exceed standards for data protection and privacy outlined in the Minimum Standards for Privacy and Security of Student and Employee Data.

To provide a variety of educational tools within our classrooms, MACS has identified a listing of applications that are approved for use. As many of these applications require a student's name and/or e-mail address for registration, tracking, or grading purposes, these applications have been verified as meeting or exceeding the required data protected standards.

- Alma
- Boom Learning
- BrainPop
- Brainscape
- Code.org
- CommonLit.org
- CommonSense
- Desmos
- Dreambox
- EdPuzzle.com
- Everfi
- GetEpic
- Gsuite/Google Classroom
- Happy Numbers
- icivics.org
- Kahoot
- Khan Academy
- Learning A-Z
- Lexia
- MathGames
- MobyMax
- Newsela
- NoRedInk
- PBS NOVA Labs
- Prodigy
- Pixton
- Quill.org

- Quizizz
- QuizLit
- ReadWorks
- SplashMath
- Tynker
- Typing Club
- Vocab.com
- Vocabulary Spelling City
- Xtra Math
- Zearn
- Zoom

Any other paid or free applications, tools, or systems not listed above are expressly prohibited from being used to receive, store, process, transmit, or dispose of any protected information. This includes, but is not limited to, third-party productivity or project planning applications, lesson planning applications, grading systems or applications, etc. that would require the input of any protected information.

Employees wishing to utilize a new application or system at MACS must submit a written request to the Director and the Curriculum Coordinator. The application or system will be evaluated for general security and compliance with all applicable requirements, and if accepted for use, will be added to the list of approved applications.

Software Licensing: Employees under no circumstances will copy or transmit MACS owned software to devices not owned by the MACS, unless approved by the manufacturer. The use of non-MACS owned software and or unlicensed software on MACS devices is strictly forbidden. Unauthorized use or copying of copyrighted or licensed information is also strictly forbidden.

Procurement: All MACS equipment and resources must be approved by the MACS Director before purchase.

Hardware, Software use & Configuration: Equipment will be procured and assigned based on the employee's job function and role. Equipment belonging to MACS is not allowed to be altered or modified in any way without the written approval of MACS Management. Any defective or damaged equipment or software must be reported immediately. All software installations and configurations must be implemented by a member of the Mainstay Technologies' Response Services Team based on an open ticket within the ConnectWise Ticketing System.

Employees may not connect non-MACS (personally owned) devices to the Information System nor store any sensitive data non-MACS devices. Employees with a passcode on their personally owned cellphones **and** authorization from the MACS Director may access MACS email on their personally owned cellphones.

Data Storage and Management: MACS employees should never store sensitive data on any device, local or remote if it is not an approved and fully protected storage system. Encryption, redundancy and fault tolerance methods should be in place to eliminate the loss or corruption of sensitive data. Local systems may not be part of the overall backup strategy and may not have proper encryption and safeguards to house sensitive data.

Employees should never attempt to access data that they do not have proper authorization for. Role based access, least privilege and separation of duties should always be considered when accessing data. Employees should never alter or delete another employee's information or data without documented permission even if the system allows you to do so. Employees should never bypass or attempt to bypass existing security measures and controls for the Information System.

5. Vendor & Public Communications Management

Vendor Management:

a) All computer equipment, portable media and software must be approved by MACS Management before it is connected to the Information System or used to work remotely.
b) All on-site vendors must be properly signed in and signed out at the front office.
c) All vendors must sign confidentiality agreements before accessing the Information System locally or remotely.
d) All employees and vendors must adhere to the MACS Vendor Management Policies and Procedures.

Communications Management:

a) All public information postings that represent MACS must be approved by a member of the MACS Director ***or*** specifically be part of an employee's role and job function. Communication forums are not limited to but may include:
    i. Websites
    ii. Social Media
    iii. Email
    iv. Blogs
    v. Press/Media Outlets
    vi. Mailers
    vii. MACS Sponsored/Non-MACS Sponsored events

b) Protected information entrusted to MACS should never be exposed or transmitted in any way to unauthorized internal or external sources. MACS Incident Response procedures should be followed immediately in the event of unauthorized data exposure. Sensitive and Confidential Information must be transmitted and stored in an encrypted fashion.

6. Information System Use

MACS Information Systems are intended for professional business use. Employees must rely on training and good common sense to avoid accessing content that could be unlawful, harmful to the information system or might violate information protection best practices.

E-mail: Employees represent MACS when they send e-mails and must take full responsibility for their content. Policies against harassment, fraud, obscenities and anything that may violate local, state or federal laws must be followed.

E-mails containing MACS information may not be forwarded to external parties unless it is an authorized communication with the best interest of the organization in mind. E-mails should adhere to the same level of etiquette and professionalism as would be expected in a in person meeting. Employees should avoid receipt of and should not open information from untrusted 3rd parties or personal associations that could put the organizations Information System or reputation at risk. Unsolicited bulk email must not be sent via MACS resources or on behalf of the MACS.

MACS employees should be wary of Phishing and social engineering attempts as instructed during Information Security training. Phishing is a criminal technique that could be used to: obtain information that is confidential, grant unauthorized network and system access or transfer funds to an untrusted entity. Phishing e-mails could appear to be from a trusted source, but they are designed to fool the e-mail recipient. MACS employees should look for signs of phishing attempts. Suspicious signs can include: spelling errors, web links that aren't legitimate, e-mail communications that you weren't expecting and anyone asking for information from you directly without validating who they are first. If you receive a suspicious e-mail, do not open it, click on links, reply to or forward the information. You should delete the information and notify the Director and the Curriculum Coordinator to raise awareness for others. *Note: Do **not** forward the email in your report.*

Web Access & Malware: The internet should be used for school purposes. Information online may be subject to copyright laws. It is critical that employees have proper authorization and permission from the provider before copying anything from the internet for school use.

Employees may not use the internet for anything that could be an untrusted site, deemed unlawful, offensive in any way or might potentially violate any of MACS policies or procedures.

All employees must practice safe browsing and media habits to avoid the introduction of malware. Malware must never be introduced intentionally. You must not disable or work around antimalware systems.

Media Handling & Paper records: Employees may not connect non-MACS (personally owned) media to the Information System. Portable media is a very common way to introduce risk such as malware and viruses into the Information System. MACS approved, and managed encrypted portable media may be used to transport business data.

MACS requires that all paper records containing protected information is shredded when no longer in use. MACS fully expects that employees will safeguard and properly dispose of personal and confidential information always.

7. Privacy, Training, Physical Security & Reporting

Privacy: MACS Information System activity such as online work, e-mail, and other business system connections may be reviewed at any time. There should be no expectation of privacy pertaining to MACS owned equipment, common workspace or sensitive data facilities.

Training: Information Security training is an important part of protecting the MACS Information System. Information Security Training is provided. The training principles and best practices communicated must be followed at all times. All staff will receive Information Security training at the time of hire and at least on an annual basis thereafter. Training results will be measured and tracked. Additional Information Security training may be required if the Information System experiences a major change or if there are Information Security violations.

Physical Security:

a) Employees must keep all MACS issued equipment under their supervision and protection at all times.
b) Employees should follow all visitor escort and vendor security policies and procedures.
c) Physical access logs will be maintained and reviewed as needed.
d) Employees should observe clean desk policy (store and lock all protected information if you are leaving your work area for more than 5 minutes or for the school day) and protect all information during normal school hours
e) Employees should never leave protected information in common areas and should fully understand when they are leaving secure areas and entering common areas with sensitive information
f) Employees should always lock their workstations when leaving their desk or office
g) All hard copy or mobile media containing protected information should be properly labeled, protected and secured in transport and only be given to authorized individuals
h) All printed material that contain protected information must be destroyed after usage and shredded. If protected information must be retained, it must be stored in a locked cabinet and a clean desk best practices followed
i) Any physical or data security concerns should be immediately reported to the Director, and the Curriculum Coordinator.
j) Any personal physical safety concerns should be immediately reported to the Director and Law Enforcement (if applicable). **In the event this policy directly conflicts with actions needed to address the immediate safety of employees or students, MACS expects that the safety needs will supersede this policy.**

Reporting Security Incidents: Potential Information Security Incidents must be reported to the Director and the Curriculum Coordinator immediately.

Incidents include, but are not limited to:

- Loss of an unencrypted laptop or phone with confidential MACS information stored on it
- Accidental disclosure of confidential information to an unauthorized individual or business
- Suspected compromise of credentials, or system accounts
- Unexpected new icons on a computer, erratic device behavior, including pop-ups, alerts, etc.
- Physical security incidents include loss of physical confidential information, unauthorized access to physical files, or portions of the business, etc.

8. Information Systems Code of Ethics and Conduct

Organization resources, including MACS equipment, facilities and time are provided for school purposes. We recognize that infrequent personal use of MACS resources may occur. If this use negatively impacts job performance, increases organizational risk in any way or causes workplace disruption, the activities should cease immediately.

Employees should avoid using Information Systems for outside business that could be a conflict of interest. All use of Information Systems to support outside organizations or initiatives should be approved by the Director prior to use.

9. Nondisclosure and Confidentiality

Confidential information means all information and data pertaining to the operation of MACS, including protected information defined in Section 2 above.

Information such as patents, formulas, devices, software, code, designs, projects, testing output, research information, information security plans, financial information, marketing information, customer lists, customer information, personally identifiable information including information provided by customers, affiliates, other employees and all MACS policies and procedures are strictly confidential and should never be disclosed without express written Management approval.

The destruction, theft, or any form of sabotage of MACS technology or resources is prohibited and may be prosecuted to the fullest extent of the law.

10. Nonobservance

All information systems and data are the sole property of MACS. Inspection of systems, employee activity and data can happen at any time based on suspected violations of this policy. Employees that

violate the Information Systems Rules of Behavior may be subject to disciplinary action up to and including termination of employment. Employee offenders may also be subject to pay financial damages, legal fees and any costs incurred based on the violation.

11. Sign off and Receipt

I certify that I have read and fully understand all aspects of the MACS Information Systems Rules of Behavior. I understand that this document does not constitute a contract for employment and that anything within this document may be revised and re-distributed for acknowledgement at any time without notice.

I hereby acknowledge receipt of the MACS Information System Rules of Behavior and agree to fully abide by all statements, policies and procedures contained herein.

Employee Signature Date

Printed Employee Name