ARTICLE 10. INFORMATION TECHNOLOGY

I. Education Division Information Technology Policies

A. Statement of Fundamental Policy

The purpose of these policies are to provide and maintain a foundation for Information Technology used in the Education Division, which is based on best practice standards in the application, development, design and adoption of Technologies. This includes but is not limited to an approach to be fair and reasonable in the methodologies utilized to provide a reliable, secure and purposeful implementation of the Education Division's Information Technology resources.

B. Scope of Education Division Information Technology Policies

These policies apply to all SRPMIC Education Division students, employees (full-time, part-time, term-limited and temporary), elected and appointed SRPMIC Education Division Officials and business affiliates performing work on behalf of the SRPMIC Education Division (e.g., contractors. Volunteers, interns, vendors and consultants). Equipment within the scope of this policy includes but may not be limited to the following: SRPMIC Education Division issued devices and/or devices utilizing any of the SRPMIC Education Division's technology infrastructure.

II. Virtual Private Network (VPN)

A. Policy

1. End User Responsible Items
    a. The Division VPN does not provide end point Internet service; it provides secure access into the Division's resources. Individual users are solely responsible for selecting and purchasing an Internet Service Provider (ISP) internet connection, coordinating installation, and installing any required software necessary for Internet service. It is recommended that end users acquire at a minimum a broadband internet connection. It is the responsibility of users with VPN privileges to ensure that unauthorized persons are not allowed access to Division's resources via their Education VPN access.

2. Access Restrictions

a. VPN access is only provided to Division employees and students that have been issued a Division approved devices; access to the Education's resources via VPN by third parties including contracted vendors is strictly prohibited. Only VPN client software that is distributed by the Division's Information Technology (EIT) department may be used to connect to the Division's resources. VPN users will be automatically disconnected from the Division's VPN after a period of inactivity. User must then logon again to reconnect the VPN session. The Division's VPN does not allow dual (split) tunneling; only one network connection is allowed.

3. Access Issue Resolution
    a. EIT will install and maintain all related VPN client software and hardware. EIT will correct issues related only to the following for VPN access; end user account issues, issues related to EIT delivered VPN software, Division hardware and Division network issues. All connectivity issues beyond the physical bounds of the Education perimeter equipment will not be investigated nor will any attempts be conducted to make repairs beyond Education perimeter equipment; connectivity issues beyond the Education perimeter equipment are beyond the internal control of the EIT Department.

III. Employees and Contractor Resource Account Control

A. Policy

1. Resource Account Creation
    a. Human Resources Verification of Employment
    The Education Division Information Technology (EIT) Department will not create any user resource access accounts without an electronic or written request from Education Division Human Resources (HR) Department.

    b. Account Creation

    EIT staff members will create a work order to track account creation request. Information provided by HR will be attached to the work order ticket that is created. Only member of the EIT staff may create Directory enabled accounts.

    c. Initial Setup
    EIT will create a resource access user accounts in the Education Active Directory for newly hired employees. New accounts will have an associated e-mail account created for business correspondence purposes, will have their employee ID associated with their account in the Directory, will be granted access to a common e-mail distribution group and will be granted access to common staff shared data.

d. Activation

New accounts will be activated for usage once EIT has been notified by HR that the new employee is scheduled for Education Division New Employee Orientation (NEO). The employee must complete the Education Division NEO with HR and EIT within one week of HR notification or the newly created network access account will be subject to deletion. Users attending the NEO must sign the "*Employee Information Use Agreement*" and the "*Software Policy Use Agreement*". Both agreements shall be retained in the employee's personnel file in HR and as EIT documentation.

2. Resources Account Deletion
    a. Human Resources Verification of Separation

    The EIT Department will not delete any user resource access account without an electronic or written request from Education Division HR.

3. Account Deletion
    a. Internal Controls

    EIT staff will create a work order to track the account deletion request. Information from HR will be attached to the work order ticket that is created. This work order ticket will be completed once the account has been disabled at which time both HR and the account holder's supervisor will be notified.

    b. Recovery of Equipment

    EIT staff members will recover any Education Division issued electronic devices; however, exceptions can be arranged if a new employee will be filling the vacant position and will required the use of the same said devices. Upon determination that equipment needs to be recovered; EIT will report the findings directly to HR. EIT will then begin asset recovery.

    c. E-mail Account Inactivation

    E-mail accounts are disabled and removed from public address lists for 60 days. Once 60 days from the deletion request has lapsed the e-mail account will be purged.

d. Home Directory Inactivation
Employee's "Home" directory data is moved to a holding location on the EIT staff server where it is retained for 60 days. All user rights to the data are removed with the exception of EIT administrative rights. Once 60 days from the deletion request has lapsed the data is purged from the system.

e. Resource Account Inactivation
Resource Accounts are disabled and moved to the retired objects container in the Directory where they are retained for 60 days. Once 60 days from the deletion request has lapsed the account will be purged from the system.

IV. Student Account Creation, Archival & Deletion

A. Policy

1. STUDENT ACCOUNT CREATION
    a. Teaching and Learning Verification
    The Education Division Information Technology (EIT) Department will not create any student resource access accounts without an electronic or written request from Education Division Teaching and Learning Department.

    b. Internal Controls
    EIT staff members will create a work order to track account creation request. Information provided by Teaching and Learning (TL) will be attached to the work order ticket that is created. This work order ticket will be completed once the account has been activated and at this point both TL and the designated school staff members will be notified that the account is ready for use.

c. Initial Setup

EIT will create a resource access user accounts in the Education Active Directory for students. New accounts will have an associated storage folder for storage of school work, will be placed into a student web filtering group, and granted access to common shared data if applicable.

2. STUDENT DATA ARCHIVING

a. Prior Year Student Data Preservation

A onetime backup of all student home directory data residing on the Education network will be migrated to backup media.

b. Preservation of Data is of limited scope

Only data that resides in the designated student home directories is migrated to tape and that data is maintained for a minimum of three years.

c. Archive process

Making use of the current enterprise backup system, the Education Information Technology (EIT) Department will run a onetime full backup (archival) of student data using new archive media. This archival media will not contain any other data than the student home directory data. This media is labeled indicating the school year being archived.

d. Documentation

A record of the completed process will be logged by EIT staff.

e. Responsible Staff

This process will be carried out by a senior member of the EIT staff.

3. REMOVAL OF STUDENT DATA

a. Internal Control Standard

All student “Home” directory data will be purged from the Education Division’s designated student “Home” directory server no later than July 31st of each year.

b. Procedure

Once student data archival has been completed logged, an EIT senior engineer staff member will select all student home directories on the designated student server and purge all student data from the designated server.

c. Scope

Data to be deleted will include data for individual ALA students, SRES students, and SRHS students.

4. REMOVAL OF STUDENT ACCOUNTS
    a. Internal Control Standard
    All student "User" accounts will be purged from the Education Division's Directory no later than July 31st of each year.

    b. Procedure
    An EIT staff member will select all student accounts from the Education Division's Directory student's organizational unit and purge all student accounts from the system.

    c. Scope
    Accounts to be deleted will include individual ALA students, SRES students, and SRHS students.

V. User Access Rights Modifications

A. Policy

1. Requesting Access Rights Modifications
    a. Default Level of Access Granted
    All access rights and/or modifications will provide the minimum rights required to reasonably access a given resource or perform a given task.

2. Internal Control - Approval
    a. Any user rights modification action will require two factor authentications for the account requesting rights modification. This two factor authentication will require, at a minimum, electronic or written communication from:

        1. The account holder or a third party, on the account holder's behalf, stating explicitly what rights changes is being requested.

2. Electronic or written communication from the account holders direct supervisor or owner of the resource where rights are to be granted must be delivered to Education Information Technology (EIT) department stating explicit approval of such request.

3. Modification of Account Rights
    a. Granting Account Access Rights
    Rights granted to Education Division resources will be assigned at the minimum level required to perform tasks or work for the Education Division. Rights modifications will be performed by members of EIT exclusively.
    b. Authorization for Inactivation
    The Education Human Resources Department shall have the authority to authorize immediate inactivation of an employee's access if the employee is terminated, on long term leave, on suspension, or is under investigation. Such requests may be submitted by email. Any other exception will require electronic or written approval from the Superintendent/Director or by those granted authority via devolution of said party's authority.

4. Logging and Review
    a. Logging
    All account rights modifications will be logged. These logs, where applicable, will also have the corresponding work order, if any, recorded in the work order Tracking field, contain relevant e-mail and documents attachments as necessary. The logs may consist of nothing further than the actual work order(s).
    b. Review of Account Changes
    The EIT Manager will review all user access modifications and select the appropriate approval status. In the interest of Education Division Security the EIT Manager reserves the right to deny any account request that will subvert established Education Division resource security.

c. Considerations

When the EIT Manager is the source of the rights modification, a senior level engineer will select the appropriate approval status and if denied, will report these modifications to the EIT Managers' senior level management for review.

VI. Information Access Misrepresentation and Disclosure

A. Policy

1. Misrepresentation

a. It is the policy of the SRP-MIC Education Division to maintain access for its staff, students and contractors (user, users) to sources of information and to provide an atmosphere that encourages access to knowledge and sharing of information while utilizing Education Division networks.

b. It is the policy of the SRP-MIC Education Division that information resources will be used by these users with respect for the public trust through which they have been provided and in accordance with policy and regulations established from time to time by the SRP-MIC Education Division and its operating units. As a user of the SRP-MIC Education Division resources, you may not assume another person's identity or role through deception or without proper authorization. You may not communicate or act under the guise, name, identification, email address, signature, or indicia of another person without proper authorization, nor may you communicate under the rubric of an organization, entity, or unit that you do not have the authority to represent.

c. In accordance with the above policies, the SRP-MIC Education Division works to create an intellectual environment in which all assigned users may feel free to create and to collaborate without fear that the products of their intellectual efforts will be violated by misrepresentation, tampering, destruction and/or theft.

2. Disclosure
    a. Access to the information resource infrastructure both within the SRP-MIC Education Division and beyond the campus, sharing of information, and security of Education Division data, all require that each and every user accept responsibility to protect the rights of the Community. Any user of the SRP-MIC Education Division who, without authorization, accesses, discloses, uses, destroys, alters, dismantles or disfigures SRP-MIC Education Division resources, properties or facilities thereby threatens the atmosphere of increased access and sharing of information, threatens established security within which users access various data and maintain records, and in light of the SRP-MIC Education Division's policy in this area, has engaged in unethical and unacceptable conduct. Access to the resources and to the information technology environment at the SRP-MIC Education Division is a privilege and must be treated as such by all users of these systems.

VII. Technology Security Incident Reporting

A. Policy

1. GUIDELINES
    a. Users of Education Division Information Technology resources must promptly report all information security incidents to the EIT Manager. The EIT Manager must promptly report all serious incidents (which are reported to them or identified by them) to the Chief Academic Officer and the Superintendent/Director. Incidents must be reported by users or by the EIT Manager as soon as possible, but no later than within 24 hours from the time an incident is identified or initially reported. Privacy and confidentiality of sensitive information as staff report, track, and respond to information security incidents, must protect and keep confidential any sensitive information. Tracked incident data will exclude any sensitive information that is not required for incident response, analysis, or by law, regulation, or other SRPMIC Education policy.

VIII. Third Party Access to Education Division Resources

A. Policy

1. Requirements for Access

   Outside agencies conducting business with the Education Division requiring access to Education Division resources must be a vendor of record for the Community, have a justifiable Education Division business related purpose for making said connection and be preapproved by the Education Information Technology Department in writing. Vendors must supply their own internet connection, software and equipment in order to successfully reach the Education Division resources. All connections by third parties must be shadowed (observed) by a qualified member of the EIT staff for the duration of said access.

2. Access Request and Restrictions

   EIT is responsible for managing all connections to the Education Division's internal resources. Education departments that require assistance via connections from third parties must submit a request to the EIT helpdesk at ithelpdesk@srpmic-ed.org to obtain permission for such connections. Request shall explain the business justification for the desired connection and the benefit(s) for the Education Division. Departments may not make request for third parties that will, in any way, provide the opportunity or the means to extract Education Division data without express written agreements on record that have been approved Education Division Administration, Education Information Technology and the Office of General Counsel .

IX. Request for Software and Electronic Devices

A. Policy

1. Requirements for Request
    a. All requests must meet a minimum set of approval requirements prior to purchasing.
        1. All requests must have approval from site administration, the Chief Academic Officer, Teaching and Learning and Education Information Technology (EIT). Failure to obtain these approvals will result in a delay and possible denial of purchase.
        2. Any request to that will disclose information to a third party must also have approval from the Community's Office of General Counsel. All hosted software solutions, software installed and maintained by a third party, must have approval listed in 1b.1 and approval from the Community's Office of General Counsel. Failure to obtain these approvals will result in a delay or denial of purchase.
        3. All requests must have a valid funding source and shall disclose upon request the initial and ongoing cost for said purchases, ongoing maintenance and/or warranties.

2. Approval for Request
    a. Once requirements for request have been met EIT will complete the purchases with the provided funding source.

3. Delivery and Install of Approved Items
    a. EIT will begin testing and verification of software and hardware upon arrival in the EIT storage facilities. Once all internal EIT deployment requirements have been met, EIT will schedule and deploy approved items.

X. Division Resource Access Rights

A. Policy

1. Administrative Privilege Restriction (Standard Level of Access Granted)
   Administrative privileges will not be granted to any user account outside of the Education Information Technology (EIT) department under any circumstances. All accounts used to access Division resources shall operate with the minimum access rights level of "Domain User" except as described in ARTICLE 10. INFORMATION TECHNOLOGY section IV. User Access Rights Modifications.

2. Request for Administrative Rights

   User rights modification(s) that request administrative level access will be denied; however, on a case by case basis, EIT may provide technical resources for software/hardware installations that require administrative rights to accomplish such tasks. EIT, at its discretion, may create and own service accounts to run services intended to allow normal business functionality for the Education Division.

3. LOGGING & REVIEW

   a. Logging Account Modifications

      All user account security rights modifications will be logged. These logs, where applicable, will have the corresponding work order, if any, recorded in the Work Order Tracking field, contain relevant e-mail and documents attachments as necessary.

   b. Review of Account Changes

      The EIT Manager will review all user security access modifications and select the appropriate approval status. The EIT Manager reserves the right to deny any account request that will subvert Education Division's resource security.

   c. Considerations

      When the EIT Manager is the source of the rights modification, a senior level engineer will select the appropriate approval status and if denied will report these modifications to the EIT Manager's senior level management for review.

XI. Server Room Access Policy

A. Policy

1. Restrictions

   Access to EIT server rooms is restricted to EIT staff that requires regular access to the server rooms to perform their job. EIT staff members accessing to the server rooms are responsible for ensuring the area remains secure upon entering or exiting. This includes securing internal locking mechanisms, activating server room alarms and securing entrance doors while accessing or exiting the server rooms.

2. Escort Conditions and Requirements

   EIT will provide escort to non-EIT parties requiring access to EIT server rooms except in cases declared as an emergency. In cases determined to be an emergency situation this policy may be superseded by authority granted to the SRPMIC Fire department, SRPMIC Police department, the EIT Manager, the

Assistant Director of Business Services, Chief Academic Officer or the Superintendent/Director. For non-emergency access all non-EIT staff access must be escorted by EIT staff while permitted in the server room area. Non-Emergency request must be submitted in writing 48 hours in advance of requiring access to the EIT server rooms. Written request must be submitted to the EIT helpdesk and will require EIT Manager approval for access authorization every time non-EIT party access is required. If the EIT Manager is unavailable, EIT helpdesk staff members will contact the Assistant Director of Business Services, the Chief Academic Officer or the Superintendent/Director to obtain access authorization. Every occurrence where access is granted or denied to non-EIT personnel for access to the EIT server room areas shall be logged.

XII. Social Media

A. Policy

1. For the purposes of this section (XII) the terms listed below shall have the following meaning(s):

    a. "Authorized Social Networking" means Social Networking conducted on behalf of SRP-MIC Education with prior authorization as described within this policy outlined in section XII.A.4.

    b. "Confidential and Proprietary Information" means confidential information regarding SRP-MIC Education business, business or governmental operations, including, but not limited to, financial information, employee information, student information, contract information, trade secrets, copyrighted information, proprietary information and other information protected from disclosure.

    c. "Social Networking" means web-based interaction through online multi-media and social networking websites (e.g., MySpace, Facebook, Yahoo! Groups, and YouTube), blogs and microblogs (e.g. Twitter), wikis (e.g., Wikipedia) and gaming sites (e.g., World of Warcraft).

    d. "Personal Social Networking" means Social Networking that is neither Authorized Social Networking nor Unauthorized Work-Related Social Networking.

    e. "Unauthorized Work-Related Social Networking" means Social Networking that is not Authorized Social Networking that either: (1) discusses the Education Division, the government or business

operations of SRPMIC and / or its' Divisions or Enterprises (e.g., discusses work that the poster is performing for SRPMIC Education, discusses events happening in the workplace, discusses interactions between people in the workplace, etc.); (2) is conducted by an employee, official or business affiliate of SRPMIC Education that is identified online as such (e.g., an employee who lists his/her employment with SRPMIC in the "work info" section of his/her Facebook profile); or (3) both discusses the Education Division, the government or business operations of SRPMIC and / or its' Divisions or Enterprises and is performed by an employee, official or business affiliate of SRPMIC or SRPMIC Education that is identified online as such.

2. General Standards.
    a. Ethical Conduct.
        i. Authorized Social Networking and Unauthorized Work Related Social Networking shall be consistent with SRP-MIC and SRP-MIC Education Division laws, policies, rules, regulations, directives, agreements and standards of conduct, as well as any other applicable laws concerning matters such as defamation, pornography, harassment, protected health information, privacy, confidentiality, copyright and trademarks.

    b. Protection of Confidential and Proprietary Information.
        i. Confidential and Proprietary Information shall not be disclosed through Social Networking.

    c. Protection of Privacy.
        i. Private information obtained through SRP-MIC or the SRP-MIC Education Division about any SRP-MIC students, business affiliates, Community Members, elected or appointed officials, employees or other stakeholders shall not be disclosed through Social Networking without the express written permission of the individuals or entities involved. Applicable privacy protection laws such as HIPAA must be followed.

    d. Laws Pertaining to Publications.
        i. Authorized Social Networking and Unauthorized Work-Related Social Networking shall not violate the copyright, trademark or publication rights of others. Authorized Social Networking and Unauthorized Work-Related Social Networking must conform to all applicable laws regarding copyright, public records, retention, fair use, financial disclosure and other relevant subjects.

e. Cyber-bullying and Other Prohibited Acts.

i. Authorized Social Networking and Unauthorized Work-Related Social Networking shall not be used to attack, abuse or cyber-bully. Authorized Social Networking and Unauthorized Work-Related Social Networking shall not be used to publish discriminatory or harassing comments, profanity, personal insults, or any other type of communication that would not be acceptable in the SRP-MIC Education Division workplace.

f. Press Contacts.

i. If an individual is questioned by the press about any Social Networking activity pertaining to the SRP-MIC Education Division, the individual or entity should immediately contact Education Division Administration Leadership for coordination and guidance.

g. Photographs and Other Media Recordings.

i. Photographs and other media recordings shall not be posted online without following all applicable SRP-MIC policies.

ii. Requests received by the SRP-MIC or SRP-MIC Education Division by its students, employees, officials, or business affiliates to remove from the internet any pictures or other media recordings impacting their rights and interests shall be honored immediately.

iii. Photographs and other media recordings that portray sacred sites or rituals of SRP-MIC shall not be posted online without the express written permission of the SRP-MIC Community Relations Department and the SRP-MIC Cultural Resources Department.

3. Unauthorized Work-Related Social Networking.

a. Unauthorized Work-Related Social Networking is Social Networking that is not Authorized Social Networking and either:

i. Discusses the SRP-MIC Education Division or business operations of the SRP-MIC Education Division (e.g., discusses work that the poster is performing for SRP-MIC Education, discusses events happening in the workplace, discusses interactions between people in the workplace, etc.);

ii. Is conducted by a student, employee, official or business affiliate of SRP-MIC and /or SRP-MIC Education that is identified online as such (e.g., an employee who lists his/her employment with SRP-MIC or SRP-MIC Education Division, Community Schools or the like in the "work info" section of his/her Facebook profile); or Both discusses the SRP-MIC Education Division or business operations of the SRP-MIC Education Division and is performed by an employee, official or business affiliate of the SRP-MIC Education Division that is identified online as such.

b. Transparency of Origin.

i. Individuals engaging in Unauthorized Work-Related Social Networking shall make it clear that they are speaking for themselves and not on behalf of SRP-MIC or the SRP-MIC Education Division.

ii. Mandatory Disclaimers.

1. Individuals engaging in Unauthorized Work-Related Social Networking must also publish a simple and visible disclaimer explaining that their activity reflects the personal views of the author, and not those of SRP-MIC or the SRP-MIC Education Division.

iii. Seals, Logos and Trademarks.

1. Individuals engaging in Unauthorized Work-Related Social Networking shall not use the official seal of SRP-MIC, SRP-MIC Education Logo(s) or the logos or trademarks of SRP-MIC's enterprises or divisions unless express written permission has been granted by the referenced Division's Board, Community Manager and appropriate Enterprise CEO.

c. Conflicts of Interest.

i. Individuals shall not engage in Unauthorized Work-Related Social Networking that creates prohibited conflicts of interest.

1. Paid Postings.

a. Students, employees, officials and business affiliates of SRP-MIC that are offered payment to engage in Unauthorized Work-Related Social Networking for a third party must seek approval

through the appropriate chain of command prior to engaging in the Unauthorized Work-Related Social Networking to ensure that the postings do not create prohibited conflicts of interest.

d. Individuals engaging in Unauthorized Work-Related Social Networking shall be personally liable for any violations of law or policy caused by their Social Networking. The SRP-MIC Education Division shall not be liable, under any circumstances, for any errors, omissions, losses or damages claimed or incurred as a result of Unauthorized Work-Related Social Networking.

4. Authorized Social Networking on Behalf of SRP-MIC Education.
    a. Authorization.
        i. Only individuals and entities authorized by the Community Manager, SRP-MIC Education Board and SRP-MIC Education Leadership to engage in Social Networking on behalf of SRP-MIC may do so or represent that they do so.

        ii. Authorization to engage in Social Networking on behalf of SRP-MIC Education must be obtained through SRP-MIC Education Board, SRP-MIC Education Division Leadership and from the Community Manager.

        iii. Authorizations to engage in Social Networking on behalf of SRP-MIC Education shall be for a fixed period of time. Under no circumstances shall any authorization to engage in Authorized Social Networking extend beyond the date of termination of the professional relationship between SRP-MIC Education and the authorized poster.

    b. Transparency of Origin.
        i. Unless given specific authorization by the Education Board, Education Division Administration Leadership and Community Manager to do otherwise, individuals and entities engaging in Authorized Social Networking:

            1. Must disclose their affiliation with SRP-MIC and / or SRP-MIC Education;

2. May not use aliases; and may not provide information that conceals their affiliation with SRP-MIC and / or SRP-MIC Education or otherwise misleads the public.

ii. Seals, Logos and Trademarks.

3. Individuals and entities engaging in Unauthorized Work-Related Social Networking shall not use the official seal of SRP-MIC, SRP-MIC Education Logo(s) or the logos or trademarks of SRP-MIC's enterprises or divisions unless express written permission has been granted by the referenced Division's Board, Community Manager and appropriate Enterprise CEO.

c. Basic Standards.

i. Information published online can easily be republished, redistributed and retained, regardless of later attempts to restrict, recall or remove it. Therefore, Authorized Social Networking must, at a minimum, conform to the following basic standards, unless given specific authorization by the Education Board, SRP-MIC Education and Community Manager to do otherwise.

1. Ethics and Professionalism.
   a. Authorized Social Networking must be ethical, professional and consistent with the values of SRP-MIC Education and SRP-MIC.

2. Accuracy.
   a. Individuals engaging in Authorized Social Networking may not knowingly communicate information that is false, inaccurate or deceptive. It is the responsibility of the individuals and entities engaging in Authorized Social Networking to verify that the information they are communicating is accurate and up-to-date.

3. Completeness.
   a. If a complete thought, along with its context, cannot be communicated through a character-restricted internet posting (such as a Twitter posting), an individual or entity engaging in

Authorized Social Networking must provide a link to an online space where the message is completely and accurately conveyed.

4. Corrections.
    a. Individuals that identify mistakes in their Authorized Social Networking activity shall promptly correct their mistakes and clearly indicate that corrections have been made. Authorized Social Networking activity may not be altered without a clear indication of the changes made.

5. Recordkeeping.
    a. Online SRP-MIC Education statements are held to the same legal standards as traditional media communications. Therefore, all individuals engaging in Authorized Social Networking must maintain records of their Authorized Social Networking activity and any related online interactions, unless given specific authorization by the Education Board, Education Division Administration Leadership and Community Manager to do otherwise.

5. Personal Social Networking.
    a. Personal Social Networking is Social Networking that is neither Authorized Social Networking on behalf of SRP-MIC Education nor Unauthorized Work-Related Social Networking.

    b. SRP-MIC Education owned computing devices shall not be used for Personal Social Networking.

    c. Personal Social Networking shall not be conducted using the SRP-MIC Education Network or any other communications services provided by the SRP-MIC Education Division.

    d. Personal Social Networking shall not be conducted during work hours.

e. Individuals engaging in Personal Social Networking shall be personally liable for any violations of law or policy caused by their Social Networking. SRP-MIC Education shall not be liable, under any circumstances, for any errors, omissions, losses or damages claimed or incurred as a result of any Personal Internet Posting.

6. ENFORCEMENT:
   a. Violations of this policy by an Education Division student, employee or SRP-MIC Education official should be reported to the appropriate SRP-MIC Education Division Superintendent or Director.

   b. A violation of this policy by a student, employee or SRP-MIC Education Division official may lead to disciplinary action, up to and including termination or removal from office, and shall be handled in accordance with the relevant disciplinary procedures.

   c. Violations of this policy by a business affiliate performing work on behalf of the SRP-MIC Education Division should be reported to the appropriate SRP-MIC Education Division Superintendent, Director, Education Board and / or Community Manager.

   d. A violation of this policy by a contractor, vendor, consultant and/or person affiliated with any of these third parties should be reported to the appropriate SRP-MIC Education Division Superintendent, Director, Education Board and / or Community Manager.
   e. A violation of this policy may also lead to reduction or elimination of SRP-MIC Education Division Communications Systems privileges.

   f. Where an alleged violation of this policy involves illegal activity, the violator may also be subject to criminal prosecution, civil liability or both.

XIII. INFORMATION TECHNOLOGY DEFINITIONS

1. **Active Directory** is a directory service created from Microsoft for Windows domain networks.
2. **Common e-mail** distribution is an e-mail enable grouping of recipients utilized for non-secure, non-private general communications.
3. **Common shared data** is a server storage location utilized for non-secure, non-private general electronic storage. *Note: Staff and Student common shared data storage reside in distinctive separate electronic areas.*
4. **Devices** refer to all electronic peripherals capable of making a network connection.
5. **Directory** is the software system that stores, organizes and provides access to information in a directory.
6. **Dual (split) tunneling** is a computer networking concept which allows a VPN user to access a public network (e.g., the Internet) and a local LAN or WAN at the same time, using the same physical network connection.
7. **Education Division resource** refers to any electronically stored information, network enabled device or other object provisioned by the Education Information Technology Department for use in conjunction with the Education Division technology infrastructure.
8. **Emergency situation** is defined as including moments where there is reason to believe an imminent threat to anyone could be avoided by superseding a defined policy.
9. **End User** refers to account created by EIT for Education Division usage, Staff, Student and Contractor
10. **Firewall** a technological barrier designed to prevent unauthorized or unwanted communications between computer networks or hosts
11. **Home Directory** is any space allocated to a resource account for personal electronic data storage.

12. **Information security incident** is defined as an attempted or successful unauthorized access, use, disclosure, modification or destruction of information; interference with information technology operation; or violation of explicit or implied acceptable usage policy. Examples of information security incidents include but are not limited to:
    1. Computer security intrusion
    2. Unauthorized use of systems or data
    3. Unauthorized change to computer or software
    4. Loss or theft of equipment used to store private or potentially sensitive information
    5. Denial of service attack
    6. Interference with the intended use of information technology resource
    7. Compromised user account
13. **Resource Account** is an agent, either a human agent (end-user) or software agent, who uses a computer or network service.
14. **Serious incident** is an action that may pose a threat to the Education Division or the SRPMIC Community, stakeholders, and/or services. Specifically, an incident is designated as serious if it meets one or more of the following criteria:
    1. Involves potential unauthorized disclosure of sensitive information
    2. Involves serious legal issues
    3. May cause severe disruption to critical services
    4. Involves active threats
    5. Is widespread
    6. Is likely to raise public interest
    7. Discloses unauthorized material to students
15. **Service accounts** are limited resource access accounts used to control specific automated processes. These accounts are created exclusively by the Education Information Technology department.
16. **Student Accounts** refer to unique student accounts assigned to individual Community school students.
17. **Student personal data** refers to data stored by students in their respective home directories.
18. **Unauthorized persons** are defined as any person or entity that attempts or gains access to electronic information or electronic resources without authorization.
19. **Vendor of Record** refers to any third party entity conducting business for or on behalf of the Education Division who is current with all required tribal clearances

20. **Social Media** is any online tool or application that goes beyond simply providing information, instead allowing collaboration, interaction, and sharing. Examples of social media include but are not limited to: blogs; microblogs; wikis; photo and video sharing; podcasts; virtual worlds; social networking; social news and bookmarking; web conferencing and webcasting.
21. **Virtual Private Network** is a private network that interconnects remote (and often geographically separate) networks through primarily public communication infrastructures such as the Internet. VPNs provide security through tunneling protocols and security procedures such as encryption.
22. **"Authorized Social Networking"** means Social Networking conducted on behalf of SRP-MIC Education with prior authorization as described in Article 10.
23. **"Confidential and Proprietary Information"** means confidential information regarding SRP-MIC Education business, business or governmental operations, including, but not limited to, financial information, employee information, contract information, trade secrets, copyrighted information, proprietary information and other information protected from disclosure.
24. **"Social Networking"** means web-based interaction through online multi-media and social networking websites (e.g., MySpace, Facebook, Yahoo! Groups, and YouTube), blogs and microblogs (e.g. Twitter), wikis (e.g., Wikipedia) and gaming sites (e.g., World of Warcraft).
25. **"Personal Social Networking"** means Social Networking that is neither Authorized Social Networking nor Unauthorized Work-Related Social Networking.
26. **"Unauthorized Work-Related Social Networking"** means Social Networking that is not Authorized Social Networking that either: (1) discusses the Education Division, the government or business operations of SRPMIC and / or its' Divisions or Enterprises (e.g., discusses work that the poster is performing for SRPMIC Education, discusses events happening in the workplace, discusses interactions between people in the workplace, etc.); (2) is conducted by an employee, official or business affiliate of SRPMIC Education that is identified online as such (e.g., an employee who lists his/her employment with SRPMIC in the "work info" section of his/her Facebook profile); or (3) both discusses the Education Division, the government or business operations of SRPMIC and / or its' Divisions or Enterprises and is performed by an employee, official or business affiliate of SRPMIC or SRPMIC Education that is identified online as such.