ARTICLE 10. INFORMATION TECHNOLOGY

I. Education Division Information Technology Policies 2

A. Statement of Fundamental Policy 2

B. Scope of Education Division Information Technology Policies 2

II. Remote Access (Staff and Students) 2

A. Policy 2

III. Non-Student Resource Account Control 3

A. Policy 3

IV. Student Accounts Deactivation/Revocation 4

A. Policy 4

V. User Access 5

A. Policy 5

VI. Information Access Misrepresentation and Disclosure 6

A. Policy 6

VII. Technology Security Incident Reporting 7

A. Policy 7

VIII. Third Party Access to Education Division Resources 7

A. Policy 7

IX. Request for Software or Electronic Devices 8

A. Policy 8

X. Server Room Access Policy 8

A. Policy 8

XI. Social Media 8

A. Policy 8

XII. Information Technology Definitions 16

I. Education Division Information Technology Policies

A. Statement of Fundamental Policy

The purpose of these policies is to provide and maintain a foundation for Information Technology used in the Education Division DBA Salt River Schools (SRS), which is based on best practice standards in the application, development, design, and adoption of Technologies. The policy 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 SRS Information Technology resources.

B. Scope of Education Division Information Technology Policies

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

II. Remote Access (Staff and Students)

A. Policy

1. End User Responsible Items
    a. SRS remote access does not provide endpoint Internet service; it provides secure access to SRS 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 the responsibility of users with remote access privileges to ensure that non-SRS employees, as well as any person(s) not directly authorized, not be allowed access to SRS resources provided via remote connectivity solutions.

2. Access Restrictions
    a. Remote access is only provided to SRS employees and students that have been issued an SRS approved device; access to the SRS resources via remote access solutions by third parties including contracted vendors is strictly prohibited. Only remote access software that is distributed by the SRS Information Technology (I.T.) department may be used to connect to the SRS resources when outside the physical bounds of the SRS infrastructure. The SRS remote access shall not allow dual (split) tunneling; only one network connection is allowed.
    b. All remote access shall be subject to SRS web access filtering and rule sets in the SRS firewalls.

c. All remote access solutions shall make use of non-proprietary encryption technologies that conform to the use of encryption methods, and key length considered not yet compromised such as the paring, example as of 1st quarter 2019, of IPSEC and SHA256 or SHA512 encryption.

3. Access Issue Resolution
   a. I.T. shall install and maintain all related remote access software and hardware solutions. I.T. shall correct issues related only to the following for remote access; end-user account issues, issues related to I.T. delivered remote access software, SRS hardware and SRS network issues. All connectivity issues beyond the physical bounds of the SRS perimeter equipment shall not be investigated nor shall any attempts be conducted to make repairs beyond SRS perimeter.

III. Non-Student Resource Account Control

A. Policy

1. Resource Account Creation
   a. Service or universal access only accounts
      I.T. may create service accounts as required to run or maintain services, system or automation where necessary at the sole discretion of I.T.

   b. Human Resources Verification of Employment
      SRS I.T shall not create any user resource access accounts without an electronic or written request from SRS Human Resources (H.R.) Department.

   c. Account Creation

      Only members of the I.T. staff may create Directory enabled accounts. Only members of the I.T. staff may create resource access accounts.

   d. Initial Setup
      New accounts shall have an associated e-mail account created for business correspondence purposes as necessary, shall have their employee ID associated with their account, shall be granted access to a standard e-mail distribution group(s) and shall be granted access to typical staff shared data according to information received from H.R. These accounts shall be created and set to a status of disabled/not activated. All accounts are created with access at the minimum level required to perform a given task. No accounts shall be given Administrative access beyond members of the SRS I.T. department.

e. Activation

New accounts shall be activated for usage once I.T has been notified by H.R. that the new employee is scheduled for SRS New Employee Orientation (NEO). The employee must complete the SRS NEO with H.R. and I.T. within one week of H.R. notification or the newly created network access account shall be subject to deletion. Employees attending the NEO must sign the "*Employee Information Use Agreement*" and the "*Software Policy Use Agreement.*"

2. Resources Account Deactivation/Revocation
    a. Security Threat

    Any account found to be a threat to SRS technology security shall be immediately deactivated/revoked.

    b. Human Resources Verification of Separation

    I.T. shall not deactivate/revoke any user resource access account without an electronic or written request from SRS H.R. Except as previously mentioned in Article X Section III, A, 2, a.

3. Account Deactivation/Revocation Extended Actions

    a. E-mail Account Deactivation/Revocation

    When a resource account is deactivated/revoked SRS I.T. shall also deactivate the attached/associated e-mail account if any exist.

    b. Technology Access Deactivation/Revocation

    All prior access for a resources account shall be removed for deactivated/revoked accounts.

IV. Student Accounts Deactivation/Revocation

A. Policy

1. STUDENT ACCOUNT CREATION

    a. I.T. shall establish automated account creation methods for student accounts created within the current Student Information System(s) (SIS). Accounts not listed in a given SIS shall not receive an account for SRS resource access.

    b. Exceptions

    I.T. may create everday user accounts as required. All account creations must be approved by the SRS I.T. management.

c. Initial Setup

New accounts shall have an associated storage location on the network as required, shall be placed into a student web filtering group, granted access to common shared data if applicable and assigned the minimum rights required to complete required tasks.

2. Student Account Deactivation/Revocation

V. User Access

A. Policy

1. Initial User Access
   a. All access accounts shall be created using a model of lowest privileged assignment where the account shall be given the minimum level of access to perform a required task. No account shall be granted administrative access without approval from I.T. management.

2. Request for Access Modification
   a. Any user access modification action shall require two-factor approval for access modification. This two-factor approval shall require:

      1. An electronic or written request by the account holder or a third party, on the account holder's behalf, stating the access change explicitly being requested.

      2. An electronic or written communication from the account holder's direct supervisor or in the case of resource access, communication of the same from the owner of the resource where access shall be granted must be supplied to I.T. stating explicit approval of such request.

3. Modification of Account Access

   Rights modifications shall be performed by members of I.T. exclusively. Exceptions are granted to the departments who are given direct access to approved third-party systems requiring management on behalf of a given LEA (e.g. staff related to Curriculum based software as a service (SAS).

4. Unethical or Malicious Behavior(s)

    a. Any attempt by an individual, named or unnamed, in the overall scope of the I.T. policies which results in an elevated level of user access to SRS resources without prior authorization, shall result in resource access revocation. Actions of this nature may subject the user who commits such infractions to other SRS Policy actions outside of I.T. and may include separation of employment or separation in the established relationship between the individual and SRS.

VI. Information Access Misrepresentation and Disclosure

A. Policy

1. Expectations
    a. SRS expects that access to information resources shall be used with respect for the public trust through which they have been provided such access and in accordance with policy and regulations established from time to time by the SRS and its operating units.

2. Misrepresentation
    a. As a user of the SRS 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.

3. Disclosure
    a. SRS users are required to disclose all actions that might involve any of the following, including as ones on individual action(s), attempts to gain unauthorized access to technology resources, disclosure of information without proper approvals, destruction of resources without approval(s), alteration of technology resources without approval(s), or intentional damage any SRS technology resources.

VII. Technology Security Incident Reporting

A. Policy

1. GUIDELINES
    a. SRS users of Technology resources are required to report all information security incidents to the I.T. department promptly. I.T. management shall proceed to follow the chain of command to report to the leadership of SRS. Incidents must be reported by no later than within 24 hours from the time of knowledge of an incident.

VIII. Third Party Access to Education Division Resources

A. Policy

1. Requirements for Access

    Third parties conducting business with SRS requiring access to SRS resources must be a vendor of record for the Community, have a justifiable SRS business-related purpose for making the said connection and be preapproved by the I.T. Department in writing. All connections by third parties must be shadowed (observed or recorded) by a qualified member of the I.T. staff for the duration of said access.

2. Access Request and Restrictions

    SRS departments that require assistance via connections from third parties must submit, before connections being granted, a request to the I.T. Helpdesk via e-mail to obtain permission for such connections. The request shall explain the business justification for the desired connection and the benefit(s) for SRS. Departments may request for third parties that shall, in any way, provide the opportunity or the means to extract SRS data without the express written approved agreements, following all SRS requirements for such approvals.

3. All remote access solutions shall make use of non-proprietary encryption technologies that conform to the use of encryption methods, and key length considered not yet compromised such as the paring, example as of 1st quarter 2019, of IPSEC and SHA256 or SHA512 encryption. Exceptions may be granted at the sole discretion of I.T. management.

IX. Request for Software or Electronic Devices

A. Policy

1. Requirements for Request of software or electronic devices
    b. All requests must meet a minimum set of approval requirements before purchasing.
        1. All requests must have approval from site administration, areas tasked with monitoring and approval of Curriculum related items as applicable, I.T., approval from SRS administration as applicable, and the Office of General Counsel as applicable. Failure to obtain these approvals shall result in a delay and possible denial of requests.
        2. All requests must have a valid funding source and shall be disclosed. All initial and ongoing cost for said purchases, ongoing maintenance and warranties must be included to be considered for approval.

2. Approval for Request
    c. Once requirements for the request have been met I.T. shall complete the purchases with the provided funding source.

X. Server Room Access Policy

A. Policy

1. Restrictions

    Access to SRS server rooms is restricted, with the exception of shared access locations (e.g., Common access telecom, fire, and other resources) to I.T. staff. Shared areas require SRS I.T. to provide their local infrastructure cabinets to prevent direct third party access to servers.

XI. Social Media

A. Policy

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

a. "Authorized Social Networking" means Social Networking conducted on behalf of SRS with prior authorization as described within this policy outlined in section XI.A.4.

b. "Confidential and Proprietary Information" means confidential information regarding SRS business, business or governmental operations, including, but not limited to, financial information, employee information, student information, contact 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 SRS, the government or business operations of SRPMIC and / or its' Divisions or Enterprises (e.g., discusses work that the poster is performing for SRS, 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 SRS 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 SRS 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 SRS 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 SRS about any SRS or 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 federal laws must be adhered to including but not limited to Health Insurance Portability and Accountability Act (HIPAA), Family Educational Rights and Privacy Act (FERPA) and Children's Internet Protection Act (CIPA).

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 SRS workplace.

f. Press Contacts.
    i. If the press questions an individual about any Social Networking activity pertaining to the SRS, the individual should immediately contact SRS 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 SRS policies.

ii. Requests received by the SRP-MIC or SRS by its students, employees, officials, or business affiliates or third parties 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 SRS or business operations of the SRS (e.g., discusses work that the poster is performing for SRS, discusses events happening in the workplace, discusses interactions between people in the workplace, with the exception of SRS approved and promoted events and post remains on the topic of the promotion therein.);

ii. Is conducted by a student, employee, official or business affiliate of SRP-MIC and /or SRS that is identified online as such (e.g., an employee who lists his/her employment with SRP-MIC or SRS, or the like in the "work info" section of his/her Facebook profile); or Both discusses the SRS or business operations of the SRS and is performed by an employee, official or business affiliate of the SRS that is identified online as such with the exception of SRS approved and promoted events and posts remain on topic of the promotion therein.

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 SRS.

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 SRS.

iii. Seals, Logos, and Trademarks.
    1. Individuals engaging in Unauthorized Work-Related Social Networking shall not use the official seal of SRP-MIC, SRS 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 for engaging in Unauthorized Work-Related Social Networking for a third party must seek approval through the appropriate chain of command before 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 SRS 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 SRS.
    a. Authorization.

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

ii. Authorization to engage in Social Networking on behalf of SRS 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 SRS shall be for a fixed period and shall require reauthorization yearly. Under no circumstances shall any authorization to engage in Authorized Social Networking extend beyond the date of termination of the professional relationship between SRS and the authorized poster.

b. Revocation

i. The SRS Board or SRS Board Chair reserve the right to revoke the authorization of any previously granted authorizations at any time, without notice and at their sole discretion. Notifications of such revocations shall be made public at the next scheduled SRS Board meeting to allow inclusion in public record and service as a public notice.

c. 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 or SRS;

2. May not use aliases, and; may not provide information that conceals their affiliation with SRP-MIC or SRS 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, SRS 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.

d. Basic Standards.

i. Information published online can quickly 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 SRS Board, SRS and Community Manager to do otherwise.

1. Ethics and Professionalism.
    a. Authorized Social Networking must be ethical, professional and consistent with the values of SRS 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 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 SRS 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 SRS Board, SRS 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 SRS nor Unauthorized Work-Related Social Networking.

    b. SRS owned computing devices shall not be used for Personal Social Networking.

    c. Personal Social Networking shall not be conducted using the SRS Network or any other communications services provided by the SRS 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. SRS 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 SRS student, employee or SRS official should be reported to the appropriate SRS Superintendent or Director.

    b. A violation of this policy by a student, employee or SRS official may lead to disciplinary action, up to and including expulsion, termination or removal from office, and shall be handled by following the relevant disciplinary procedures.

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

    d. A violation of this policy by a contractor, vendor, consultant or person affiliated with any of these third parties should be reported to the appropriate SRS Superintendent, Director, Education Board and Community Manager.

    e. A violation of this policy may also lead to a reduction or elimination of SRS 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.

XII. 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 golbal communications.
3. **Common shared data** is a server storage location utilized for non-secure, non-private ample electronic storage.
4. **Devices** refer to all electronic peripherals capable of making a network connection.
5. **The 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. **An eAn emergency** is defined as including moments where there is a reason to believe an imminent threat to anyone could be avoided by superseding a defined policy.
8. **End User** refers to an account created by I.T. for SRSfor use by, Staff, Student(s) or Contractor(s)
9. **Firewall** a technological barrier designed to prevent unauthorized or unwanted communications between computer networks or hosts
10. **Home Directory** is any space allocated to a resource account for personal electronic data storage.
11. **An information security incident** is 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
12. **IPSEC** is a suite of protocols that interact with one another to provide secure private communications across IP networks. These protocols allow the system to establish and maintain secure tunnels with peer security gateways.
13. **Remote Access is** any access to private SRS resources utilizing, as the connection ingress, any configured external interface of any SRS firewall.
14. **A Resource** shall be defined for this policy as any technology related to data, infrastructure, electronic device, electronic device peripheral, electronic access medium, electronic-based storage, or items made available or accessed electronically by an end user.
15. **Resource Account** is an agent, either a human agent (end-user) or software agent, who uses a computer or network service.
16. **A serious incident** is an action that may pose a threat to the Education Division or the SRPMIC Community, stakeholders, 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

17. **Service accounts** are limited resource access accounts used to control specific automated processes. These accounts are created exclusively by the Education Information Technology department.
18. **SHA 256 and SHA 512** are novel hash functions computed with 32-bit and 64-bit words, respectively. They use different shift amounts and additive constants, but their structures are otherwise virtually identical, differing only in the number of rounds.
19. **Student Account(s)** refer to individual student accounts assigned to individual Community school students.
20. **Student personal data** refers to data stored by students in their respective home directories.
21. **Unauthorized persons** are defined as any person or entity that attempts or gains access to electronic information or electronic resources without authorization.
22. **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
23. **Social Media** is an online tool or application that goes beyond simply providing information, instead of 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.
24. **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.
25. "**Authorized Social Networking**" means Social Networking conducted on behalf of SRP-MIC Education with prior authorization as described in Article 10.
26. "**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, contact information, trade secrets, copyrighted information, proprietary information and other information protected from disclosure.
27. "**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).

28. "**Personal Social Networking**" means Social Networking that is neither Authorized Social Networking nor Unauthorized Work-Related Social Networking.
29. **"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.