ANCHORAGE SCHOOL DISTRICT

Internet & Electronic Communication Guidelines

September 2015

INTRODUCTION: The Anchorage School District promotes an open, cooperative exchange of ideas; however, ASD must also educate its students, faculty, and staff about how technology abuse can interfere with the exchange of ideas integral to learning. All system users are all responsible for the well-being of the computing, network and information resources that are used in the district.

The primary purpose of the district's network is to support and enhance learning and teaching that prepares students for success. Major technology strands are embedded into the Common Core State Standards and intrinsically linked to the school board's goals for Destination 2020, as well as the goals of the Elementary and Secondary Education Act (ESEA). ASD believes that responsible use of its network will provide students and staff with the access to information they need in order to expand their knowledge and use information resources.

In accordance with the mission of the Anchorage School District, students and staff must use the district's network and communications resources, along with any associated equipment, in a responsible, ethical, respectful and legal manner. Users of these ASD resources assume responsibility for understanding the procedures and guidelines associated with their use. Staff are required to sign *a Staff and Community Internet Agreement* and students must sign a *Student Internet Agreement* before access to said resources may be provided. Staff are also expected to familiarize themselves with the state's *Code of Ethics* and Teaching Standards (AS 14.20.480), since the foundational expectations for teacher conduct should also guide and determine responsible use of technology in an educational setting.

The purpose of this document is to provide schools and departments with a set of guidelines for using the district's Internet and network services and to be in compliance with the Children's Internet Protection Act (CIPA). Deviations from these guidelines, and any associated agreement forms, may result in loss of access in addition to other disciplinary or legal action.

The ASD Internet Policy Committee was established in April 1998. Since then, the committee has held the responsibility to recommend procedures and guidelines for Internet use by students, staff and community members in the district. Committee membership includes representation from principals, librarians and secondary technology staff, as well as staff from the Communications, Information Technology and Educational Technology departments.

NOTE: Staff may also be required to sign a *Mobile Device Staff User Agreement* if they are issued mobile technology. This agreement is accompanied by the *Mobile Device Staff User Guidelines*. Students may also be required to sign a *Mobile Device Student Check-out Agreement* if they are issued district-owned mobile technology. This agreement is accompanied by the *Mobile Device Student Check-out Guidelines*.

1. DISCIPLINE

The *Internet and Electronic Communication Guidelines* are applicable to all users of the district's computer resources and refer to all information resources whether individually controlled, shared, stand alone or networked. Disciplinary action in response to violation of these guidelines by students, faculty, staff and other users shall be consistent with the district's policies and

procedures. Violations may result in revoking access privileges to district computers, other school disciplinary action and/or appropriate legal action. Specific disciplinary measures will be determined on a case-by-case basis.

2. WEB SERVICES

The content on ASD websites will provide information regarding curriculum, instruction, school activities, governance and other general information relating to individual classes, the school or district. Any links to external websites must also remain within these parameters. Web pages for individuals or organizations not directly affiliated with the district are not permitted.

The district reserves the right to remove any Web pages or links to websites deemed inappropriate or contrary to district policies. If the author's contact information is available and current, the author will be contacted and informed that their Web content has been removed.

ASD's district website, ASD Online, includes information about the district and functions as a communication tool.

Staff members are expected to adhere to the *Staff and Community Internet Agreement* and copyright laws. Staff members, schools and departments are encouraged to publish and maintain a Web presence for their classroom, school and/or department using the SiteManager Web content management system.

A district-related website is established in one of the following ways:

- by school district employees or students with employee supervision on behalf of the district;

- by any school within the district; or

- by any school-sponsored club or organization, or authorized volunteer, within the district.

ASD does not endorse and is not responsible for websites created by employees, students or others outside the standards and guidelines of this policy. Students or employees who publish personal websites that create a substantial and material disruption to the school environment may be subject to disciplinary action.

2.1. INTERNET AND INTRANET SERVERS

(Definitions: An "intranet server" is one that is **not** accessible outside the district firewall. An "Internet server" is accessible outside the district firewall.)

2.1.1. Intranet servers are allowed at ASD schools and departments.

2.1.2. Information Technology is responsible for all domain name servers in the district. Schools may request that Information Technology assign a domain

name for ease of access to their intranet server. However, if approved, this domain name will be available only on ASD domain name s e r v e r s .

2.1.3. Maintenance and support for intranet servers is a site responsibility.

2.1.4. ASD Internet servers, once approved by the Executive Director of Information Technology, will be housed at Information Technology.

2.2. MANAGEMENT OF INTERNET WEB PAGES

2.2.1. School and department Web pages should be maintained on the ASD Web server using the SiteManager Web content management system.

2.2.2. Schools and departments are responsible for the content and maintenance of their Web pages and are enjoined to perform initial and periodic checks of their websites.

2.2.3. An evaluation checklist is available on the district website and may be used for self-evaluation of school and teacher websites: www.asdk12.org/internet/webguide

2.2.4. Schools and departments will provide Information Technology and the Communications department with the name of the individual(s) responsible for their Web presence.

2.2.5. The importance of content accuracy and appropriateness, as well as the need to be reasonable in terms of file size and redundancy, should be considered when adding files to a website.

2.2.6. Information Technology will monitor and manage disk space usage on the Web server.

2.3. STAFF WEB PUBLISHING ACCESS AND PRIVILEGES

2.3.1. Any staff member may publish a page or pages on the district Web server using SiteManager in order to provide information relating to ASD curriculum or business.

2.3.2. In order to have a website, a district employee must have a signed *Staff and Community Internet Agreement* on file.

2.3.3. Each school and department may assign one or more people to maintain a website. Principals may approve and grant access to school-based staff by modifying the user's role in SiteManager. Following approval by their department head, Communications may create an account for staff not a s s i g n e d to a school and/or modify the user's role to allow access to sections of ASD Online.

2.3.4.   Each individual with a SiteManager account is responsible for maintaining the security of his or her password. Passwords are not to be share with **anyone**.

2.3.5.   Technology self-help guides are available via District Connection.

2.4.   PUBLISHING STUDENT INFORMATION ON THE WEB

In order to ensure the safety of our students, it is important that we follow guidelines concerning the publication of student information on student, staff, department and school web pages.

2.4.1.   All Schools, Departments and Students

2.4.1.1.   No home phone numbers or addresses of students may be published. Students will not publish personal information that would permit o t h e r s to determine the location of the student at any given time. This includes places of employment, class schedules and other information that may pose a safety concern for the student.

2.4.1.2.   Content of Web pages(s) must comply with the staff and community or student Internet user agreement.

2.4.1.3.   Links to student Web pages not located on district Web servers may n o t be made from schools' Web pages.

2.4.1.4.   Should any student or staff member fail to abide by the *Internet and Electronic Communication Guidelines* of the Anchorage School District or their Internet user agreement, he/she may face disciplinary action.

2.4.2.   Use of Student Images and information

Email address	Video/ photographs of anonymous students engaged in normal classroom/school activity	Video/ photographs or interviews of students at events that are open to the public	Students are interviewed or will be identified by name in a photograph or news article	An individual student is the focus of the story	Video/ photographs or interviews of students who are in special education classes or specialized programs (drug/alcohol, detention/work detail, etc.)
Never permitted for elementary students, permitted for secondary students	No media release needed	No media release needed	Media release required	Media release required	Media release required

2.4.2.1.   Individual photos, group photos and group video shots of elementary, middle or high school students may be published without a media release if student names are omitted. Individual and group photos and video that identify a student require a media release form. Exceptions to these guidelines will be made for parents who do not want their student's image to be used under any circumstances.

2.4.3. Use of Student Email Addresses

2.4.3.1.   Email addresses of elementary students may not be published online.

2.4.3.2.   Middle and high school students may publish their email address, but are required to notify a teacher or other school official immediately if they receive inappropriate email. The district takes no responsibility for any inappropriate email they may receive.

2.5. COMMERCIAL PRODUCT ADVERTISEMENT

2.5.1. It is the policy of ASD not to permit any advertising, function, or activity, which has a motive of profit to a private individual, firm or corporation. Any material bearing commercial advertising must have the written approval of the superintendent (Anchorage School Board Policy 832).

2.5.2. A school may acknowledge school business partners on the website by creating a page for those acknowledgements.

2.5.3. The acknowledgement page may contain names and logos of any school business partners, as well as a short description of the partner's contribution(s). The logos should be no larger than 200 x 200 pixels and should be static images. Animated logos are not to be used.

Descriptions of partners should be restricted to their involvement with the school, and should not promote the use of a partner's product or service.

Examples:

Appropriate: [School Name] would   like to thank [Business Name] (link)   for assistance in creating our new computer lab. The employees of [Business Name] (link) helped us buy the materials and build the tables that were needed for the new computers.

Inappropriate: [School Name] would like to thank [Business Name] for   assistance in creating our new computer lab. The employees of [Business Name] helped us buy the materials and build the tables that were needed for the new computers. Visit [Business Name] for all your [business] needs! (link).

3. EMAIL ACCOUNTS

Email creates a permanent record that may be archived and retrievable at a later date, even though the user has deleted it. Email is subject to the district document retention policy. **Be cautious about what you send and to whom. Emails are a public record that may be examined by any individual at any time.**

Email users must follow the same code of conduct expected in any other form of written communication or face-to-face business/school communication.

Email attachments may contain viruses. Be cautious if you are unsure of the origin of an email; if the email includes an attachment, do NOT open it – delete it immediately. **Never give out your password via email.**

3.1. SCHOOL AND DEPARTMENT ACCOUNTS

3.1.1. Only ASD staff members will be granted accounts on district email servers unless otherwise approved by the Executive Director of Information Technology.

3.2. ELECTRONIC COMMUNICATION

3.2.1. ASD employees are limited to one email account.

3.2.2. Users are allowed to post announcements and general information regarding retirements, surplus, want ads, etc. in the Outlook public folders. Users will not use email groups to send emails on these subjects.

3.2.3. When sending email to a long list of recipients, outside of the district, it is recommended that the BCC field be used. This practice reduces the chances of having addresses used in a spam attack. If BCC is used to distribute messages to group(s), please state in the first line of the message that BCC has been used to reduce the duplication of messages being forwarded between members of the group(s). NOTE: "Reply All" does not go to the entire BCC group.

3.2.4. Email groups are allowed. The principal/supervisor or their designees are responsible for providing current staffing information to the Help Desk.

3.2.5. Email operations are explained in the ASD Style Guide.

3.2.6. Email enclosure size should be limited to 10 MB.

3.2.7. Email items older than 90 days may be purged from the servers. Retention guidelines can be found on the Records Management's Web page.

3.2.8.   Staff members may not use their district-provided email account for monetary gain, political/religious advocacy, union activities not approved by negotiated agreement, or private business enterprise.

3.2.9.   The sharing of ASD email account credentials is prohibited.

3.2.10. Correspondence from a union to the employee concerning union issues is governed by negotiated agreement.

3.2.11. Unacceptable use is defined to include, but is not limited to, the following:

- Any unauthorized attempts to read, copy, modify or delete email messages of other users.

- Use of email to upload, download or resend copyrighted or pornographic material.

- Use of email to harass or discriminate against someone.

- Use of email to post chain letters or engage in "spamming" (sending annoying or unnecessary messages to a large number of people).

- Copy messages or attachments identified as confidential without first acquiring permission from the originator.

- Forge or attempt to forge email messages, or disguise or attempt to disguise your identity when using email.

3.2.12. ASD allows personal email use if it is reasonable, appropriate and does not interfere with work. Keep in mind that all ASD emails are public record.

3.2.13. All email accounts maintained on ASD servers are the property of ASD. Users do not have a right of privacy to anything they create, store, send or receive while using ASD email or computers. Any email, including private email accounts, related to ASD students, employees or business is considered ASD property and may be subject to public disclosure unless deemed confidential through a review process and/or consultation with ASD legal counsel.

All email accounts maintained on in-house or outsourced email systems, are the sole property of ASD. ASD has the right to monitor any user email account at any time for legitimate business reasons, including compliance with this procedure without prior notification.

Violations of this email procedure may result in disciplinary actions, leading up to and including termination, for ASD employees, or loss of use privileges for non-employees. Violation of this email procedure may also result in referral to law enforcement agencies if any violation of law in email use is suspected.

3.2.14. ASD has an anti-spam appliance in place. Spam is unsolicited email sent in large quantities, not just unwanted email. Unwanted email sent directly to users and not in a mass mailing may still appear in mailboxes. True spam emails will be quarantined in a location outside of mailboxes where users can view it if they wish. Instructions for viewing and managing spam can be found on the District Connection.

3.3. STUDENT EMAIL GUIDELINES

3.3.1. The district does not provide student email accounts on ASD servers.

3.3.2. ASD reserves the right to limit student access to personal email accounts on school premises.

3.3.3. Students are responsible for the content, operation and use of personal email accounts. The district may monitor student email account content and activity accessed by any district resource.

3.3.4. Students' use of email accounts continues to be governed by the Student *Internet Agreement* signed by both the students and their parents or guardians.

3.3.5. Noncompliance with the *Internet and Electronic Communication Guidelines* or the *Student Internet Agreement* may result in the termination of computer access privileges, disciplinary and/or legal action.

3.4. NON-ANCHORAGE SCHOOL DISTRICT EMPLOYEE EMAIL GUIDELINES

3.4.1. The district does not provide non-employees ASD domain email accounts (lastname_firstname@asdk12.org). An approved personal email account may be added to the district's global email directory to be used for ASD business.

3.4.2. The district reserves the right to limit non-employee access to personal email accounts.

3.4.3. Non-employees are responsible for the content, operation and use of their personal email accounts. The district may monitor the content and activity of any email accounts accessed by district network resources.

3.4.4. Non-employees' use of email accounts continues to be governed by the guidelines set forth in the signed *Staff and Community Internet Agreement* form.

3.4.5. Noncompliance with the *Internet and Electronic Communication Guidelines* or the *Staff and Community Internet Agreement* may result in the termination of computer access privileges, disciplinary and/or legal action.

3.5. DELETING EMAIL/USER ACCOUNTS AT THE END OF THEIR SERVICE

3.5.1. Email accounts will be disabled for 30 days prior to permanent deletion. Disabled accounts will not appear in the district's global address book. The following procedures will be used to disable and then permanently delete mail accounts.

    a. An automated process will run nightly to disable all accounts of employees with an inactive status in both HR and Payroll records on IFAS.

    b. It will be verified that an employee has terminated, not taken another ASD position.

    c. If a terminated employee has taken a temporary/substitute position, the email password will be set to expire at the end of the temporary job, if known, or at the end of the school year.

    d. If the employee has any active record in IFAS, the account will not be disabled.

    e. Terminated employees will not be granted access to their ASD email once the account has been disabled.

3.5.2. Email accounts will be disabled upon request by an appropriate supervisor. Requests will be submitted to the Help Desk.

3.5.3. Accounts that have been disabled for 30 days will follow these procedures:

    a. Upon request, supervisors will be given access to a file containing emails from the terminated employee's account.

    b. If there is no response within 30 days, the account will be permanently deleted.

    c. All email account deletions will be suspended between June 1 and September 30, unless specifically requested by the appropriate supervisor.

4. STUDENT INTERNET PROJECTS

In order to safely and appropriately use online collaboration and communication tools, teacher guidelines have been established. These guidelines can be found in the *Online Collaboration Tools Teacher Checklist*. Teachers and students participating in these projects are also required to complete the *Online Collaboration Tools Classroom User Agreement* which details the purpose of the project, the configuration of the safety restrictions and the consequences of violations of the agreement.

4.1. SITE-BASED MANAGEMENT OF LARGER STUDENT INTERNET PROJECTS

4.1.1. A school or group of teachers may decide to administer Internet-based collaborative tools to a group larger than a particular class or set of classes. In

such a case, a plan must be in place in writing that defines the scope of that administration, including how students will be enrolled into the system, what methods will be used to monitor proper student use and behavior, who is responsible for that monitoring, and the range of student activities that are covered. That plan must be presented to and accepted by the building p r i n c i p a l .

4.1.2. Teachers that are making use of the Internet-based collaborative tools, contained entirely within the scope of that administration, do not need to seek additional student agreements or parent permissions for the use of those tools, or individually define monitoring policy and protective oversight for those covered items as part of the planning of their activity.

5. REMOTE ACCESS FROM A NON-ASD LOCATION

To obtain remote access to the ASD network, the user must have an Active Directory account, which is created with an ASD email address, connection to the Internet and VPN software.

5.1.   REMOTE ACCESS GUIDELINES

5.1.1. Acquisition, installation and configuration of all necessary hardware and software for remote access are the responsibility of the user.

5.1.2. The sharing of ASD remote access accounts with non-ASD personnel is prohibited.

6. PRIVATELY-OWNED DEVICES

Anyone who brings a privately-owned device to ASD facilities is personally responsible for the equipment. Responsibility for the maintenance and repair of the equipment rests solely with that individual, including installation of software and configuration of peripherals. Any damage to the equipment, including results from viruses, is the responsibility of the individual.

Software residing on privately-owned devices must be personally owned unless authorized by the district and within the licensing constraints of the software company. The district retains the right to determine where and when privately-owned equipment may be attached to the network. The individual is responsible for the security of the equipment at all times.

A privately-owned device may be allowed connection to the district's network, including access to the Internet, under the following conditions:

- Use of the device must adhere to ASD policies and procedures.

- File storage on the network from privately-owned devices is limited to official business only.

- The individual must supply all necessary hardware/software and cabling to connect to the network.

- Prior to connecting to the district network or Internet the user of a privately-owned device must take appropriate action to prevent malware on the device. This may include running anti-virus software and/or keeping security software up to date.

- The individual has a signed *Staff and Community Internet User Agreement* form on file.

- The individual may be required to have a signed *Privately-Owned Device Use* form for the site where the device will be used.

6.1. DISTRICT RIGHTS

There can be no expectation of privacy on any device used in the district, including privately-owned devices.

As it relates to privately-owned devices being used in district facilities, the district reserves the right to:

- Monitor and log all activity,

- Make determinations on whether specific uses of the device are consistent with the district's policies and procedure,

- Deem what is appropriate and inappropriate,

- Restrict access to district resources, such as printers and servers,

- Remove the user's access to the network and suspend the right to use the privately-owned device in district facilities at any time if it is determined that the users are engaged in unauthorized activity or are violating district policies and procedures.

Disciplinary action for misuse of privately-owned devices at district facilities shall be consistent with the district's policies and procedures. Violations may be cause for removing the individual's access privileges, suspension of use of the privately-owned device in district facilities and other disciplinary actions and/or appropriate legal action.

7. COPYRIGHT

It is the intent of ASD to adhere to the provisions of copyright laws in all areas including the Internet. Illegal copies of copyrighted material may not be made or used on district equipment.

As stated in section 532.37 of the Administrative Procedures, "The legal or insurance protection of the district will not be extended to employees who violate copyright laws." Every district

employee should be aware that the penalty for the first offense of copyright violation is $10,000 and one year in prison. If the violation involves sound or media, the penalty starts at $25,000.

For further information on copyright and Fair Use, visit the U.S. Copyright Office: www.copyright.gov/fls/fl102.html.

Some material on the Web is published under the Creative Commons license. For information regarding Creative Commons licenses visit http://creativecommons.org.

7.1. COPYRIGHT VIOLATION GUIDELINES

The following guidelines give general information about what is a copyright violation.

7.1.1. Under current U.S. law, all creative efforts are copyrighted the moment they are first put on paper, input into a computer or recorded in any tangible f o r m . While registration or stating that an item is copyrighted could increase the penalties to an infringer and the monetary return to the copyright holder in a civil suit, a copyright notice is not required.

7.1.2. Copyright is violated whether a fee is charged or not.

7.1.3. Postings to the Internet are not automatically in the public domain and do not grant permission to do further copying.

7.1.4. Copyright is not lost simply because it is not defended.

7.1.5. Copyright exists in civil law and criminal law. Criminal fines start at $10,000 per violation.

7.1.6. Every attempt should be made to get permission from the copyright h o l d e r prior to republishing any material.

8. INTERNET SAFETY

8.1. CIPA–COMPLIANT INTERNET SAFETY POLICY FOR ANCHORAGE SCHOOL DISTRICT

8.1.1. It is the policy of ASD to prevent user access to or transmission of inappropriate material over its computer network.

8.1.2. It is the policy of ASD to prevent unauthorized access to online information.

8.1.3. It is the policy of ASD to prevent unauthorized online disclosure, use or dissemination of personal identification information.

8.1.4. It is the policy ASD to comply with the Children's Internet Protection Act [Pub. L. No. 106-554 and 47 USC 254(h)].

8.2. CIPA DEFINITION OF TERMS

8.2.1. TECHNOLOGY PROTECTION MEASURE: The term "technology protection measure" means a specific technology that blocks or filters Internet access to visual depictions that are:

- OBSCENE, as that term is defined in Section 1460 of Title 18, United States Code;

- CHILD PORNOGRAPHY, as that term is defined in Section 2256 of Title 18, United States Code; or

- Harmful to minors.

8.2.2. HARMFUL TO MINORS: The term "harmful to minors" means any picture, image, graphic image file or other visual depiction that:

- Taken as a whole and with respect to minors, appeals to a prurient interest in nudity, sex or excretion;

- Depicts, describes or represents, in a patently offensive way with respect to what is suitable for minors, an actual or simulated sexual act or sexual contact, actual or simulated normal or perverted sexual acts, or a lewd exhibition of the genitals; and

- Taken as a whole, lacks serious literary, artistic, political or scientific value as to minors.

8.2.3. SEXUAL ACT; SEXUAL CONTACT: The terms "sexual act" and "sexual contact" have the meanings given such terms in Section 2246 of the Title 18, United States Code.

8.3. FILTERING SOFTWARE

To the extent practical, technology protection measures (or "Internet filter") shall be used to block or filter the Internet, and other forms of electronic communications to prevent access to inappropriate information. Specifically, as required by the Children's Internet Protection Act, blocking shall be applied to visual depictions of material deemed obscene or child pornography, or to any material deemed harmful to minors. For adults only, technology protection measures may be disabled or minimized for bona fide research or other lawful purposes.

In order to address the issue of inappropriate Web-based material and to comply with CIPA, the district has installed an Internet filtering system at the district's Information Technology Data Center.

8.3.1. All Web-based content accessed through computers connected to the district network is filtered through this system.

8.3.2. Installation and operation of this, or any, Internet filtering system on ASD computers by no means precludes staff, students and community members from their responsibility to use ASD network services responsibly, as outlined in the *Staff and Community Internet Agreement*.

8.3.3. Categories of Web content to be filtered are determined by the Executive Director of Information Technology with input from district staff.

8.3.4. In some cases, sites with educational value are inadvertently blocked and may be considered for review. ASD personnel are able to unblock most sites using their staff credentials. If the site cannot be unblocked, the staff member must provide a detailed explanation describing intended use in the curriculum or other job-related function. Directions are found on the blocking screen.

8.3.5. In other cases, objectionable sites may not be identified by the filter and may need to be blocked. Anyone with a concern about an objectionable site may submit a request for review to the Help Desk.

8.3.6. While every effort will be made to act on blocking and unblocking requests as quickly as possible, in some cases the review may take 5-7 days. Those submitting a request will be notified when a decision is made. User must provide the exact URL (copy and paste into the email) in order for the site to be reviewed.

8.4. SUPERVISION AND MONITORING

It shall be the responsibility of all members of ASD staff to supervise and monitor usage of the online computer network and access to the Internet in accordance with the policy and the Children's Internet Protection Act. Procedures for the disabling or modification of technology protection measures shall be the responsibility of the ASD Executive Director of Information Technology or designated representatives.

8.5. DIGITAL CITIZENSHIP AND INTERNET SAFETY FOR STUDENTS

It is the responsibility of all teaching staff to train students in the safe and ethical use of the Internet. Internet Safety Guidelines have been developed around the strands of I am Safe, I am Secure, and I am Ethical.

Digital citizenship is about being part of the community, responsibility, respect and kindness.

Internet safety is about knowing how to keep oneself and one's equipment safe and secure online.

8.5.1. It is the responsibility of all staff to integrate the teaching of digital citizenship and Internet safety in their curriculum and activities with students. Each year every student must receive at least one lesson in each of the iSafe strands: Social Networking, Appropriate Online Behavior, and Cyber Bulling

8.5.2. The district will evaluate students' skills in digital citizenship in eighth grade in accordance with federal law.

8.5.3. The district may evaluate students' digital citizenship and Internet safety skills at other grade levels.

9. POLITICAL ACTIVITY

As stated in Section 841 of Anchorage School Board policy, the personal political rights of school employees are set forth in policy sections 264.4, 539.5, and 673, as well as in the Anchorage Municipal Code, Section 1.15.

Unacceptable use is defined as, but is not limited to, the use of district email to engage in political activities such as campaigning on behalf of a candidate, campaigning on behalf of a bond issue or other matter which is coming before the public.

10. RELIGIOUS ACTIVITY

The personal religious rights of school employees are set forth in Anchorage School Board policy sections 264.4, 539.5, and 673.

Unacceptable use is defined as, but is not limited to, the use of email to promote religious beliefs or practices, or to denigrate religious beliefs or practices.

11. PRIVACY

There can be no expectations of privacy on any device used in the district, including privately-owned devices.

ASD employees must be aware that all information accessed, created, sent, received or stored on a district computer and the network is not private.

While ASD respects the privacy of users and does not have a practice of monitoring or reviewing electronic information, the district reserves the right to do so for any reason. ASD may monitor and review activity in order to analyze the use of systems, monitor compliance with policies, conduct audits or obtain information for other reasons. ASD reserves the right to disclose any electronic message to law enforcement officials, the public or other third parties.

12. COMPUTER USE

Computer resources are to be used exclusively to support the instructional and business objectives and policies of ASD. All users must sign and adhere to the staff and community or student Internet user agreement.

Unacceptable use is defined to include, but is not limited to, the following:

- Copying and/or downloading any commercial software or other material in violation of federal copyright laws.

- Use of the ASD network for financial gain, commercial or illegal activity.

- Use of the ASD network to download, store and copy or transmit pornographic, racist, sexist or other offensive or derogatory material.

- Any form of vandalism, including but not limited to, damaging computers, computer systems or networks, other user files and/or disrupting the operation of the network.

- Use of profanity, obscenity or other language that may be offensive to another user.

- Violation of Anchorage School Board policy, district administration regulations or any provision in the student rights and responsibilities.

- Accessing another individual's account or a restricted account without prior consent is forbidden. Passwords should be frequently changed and never shared.

- Any actions that may hinder or limit the District's ability to manage ASD resources.

13. INTERNET USAGE

Every Internet site visited has the capability of identifying the user as a representative of ASD. All activity on the Internet must be governed by discretion and good judgment.

Unacceptable use is defined to include, but is not limited to, the following:

- Downloading large files during the school day from 7 a.m. until 4 p.m.

- Use of obscene, profane, lewd, vulgar, rude, inflammatory, threatening or disrespectful language. Posting of information that could cause danger of disruption or engaging in personal attacks, including prejudicial or discriminatory attacks.

14. DISCLAIMER

ASD is not responsible for loss of information from misuse, malfunction of computing hardware and software or external contamination of data or programs. The staff in IT and

all other system administrators will make every effort to ensure the integrity of ASD's computer systems and the information stored thereon. However, users must be aware that no security or back-up system is 100% reliable. **Users are responsible for back-up and recovery of their information.**

APPENDIX A – ANCHORAGE SCHOOL DISTRICT SECURITY PROCEDURES

1. FIREWALL PROCEDURE

1.1.   FIREWALL DEFINITION

For purposes of this procedure, firewalls are defined as security systems, which control and restrict both Internet connectivity and Internet services. Firewalls establish a perimeter where access controls are enforced. Connectivity reflects which systems can exchange information. A service, sometimes called an application, refers to the way for information to flow through a firewall. Examples of services include file transfer protocol (FTP) and Web browsing.

1.2.   PLAYING THE ROLE OF FIREWALLS

In some instances, systems of routers may be functioning as though they are firewalls when in fact they are not formally known as firewalls. All ASD systems playing the role of firewalls, whether or not they are formally called firewalls, must be managed according to the rules defined in this procedure. In some instances this will require that these systems be upgraded so that they support the minimum functionality defined in this procedure. Any router that connects a vendor, or any non-ASD entity, into the ASD network must pass through an agency firewall before entering the ASD network.

1.3.   PROCEDURE APPLICABILITY

All firewalls at ASD must follow this procedure. Departures from this procedure will be permitted only if approved in advance and in writing by the ASD Information Technology Department.

1.4.   DEFINED DECISION MAKER

Before being enabled, all new firewall services and new connectivity paths must be evaluated in terms of business advantages and security risks. The ASD Information Technology Department is the recognized decision maker who can either approve or deny these requests.

1.5.   DEFAULT TO DENIAL

Every Internet connectivity path and Internet service not specifically permitted by the procedure must be blocked by ASD firewalls. The list of currently approved services must be documented and distributed to district employees with a need-to-know by the ASD Information Technology Department.

Likewise, every network connectivity path not specifically permitted by the ASD Information Technology Department must be denied by firewalls. Prior to the   deployment

of every ASD firewall, a diagram of permissible paths with a justification for each must be submitted to the ASD Information Technology Change Advisory Board (CAB). Permission to enable any paths will be granted by the CAB only when (1) the paths are necessary for important business reasons, and (2) adequate security measures will be used.

1.6. LOGS

All changes to firewall parameters, enabled services and permitted connectivity must be logged. In addition, all suspicious activity, which might be an indication of unauthorized usage or an attempt to compromise security measures, must also be logged. The integrity of these logs must also be protected with checksums, digital signatures or similar measures. These logs must be promptly removed from the recording systems and stored in a physically protected container for at least three months. These logs must be reviewed periodically to ensure that the firewalls are operating in a secure manner.

1.7. INTRUSION DETECTION

All ingress points must be protected by firewalls that include intrusion detection systems approved by the ASD Information Technology Department. These intrusion detection systems must each be configured according to the specifications defined by the ASD Information Technology Department. Such intrusion detection systems must also immediately notify technical staff who are in a position to take corrective action. All technical staff working on firewalls must be provided with remote access systems and privileges so that they can immediately respond to these incidents even when they are physically removed from the firewall in question.

1.8. CONTINGENCY PLANNING

Technical staff working on firewalls must prepare a contingency plan which addresses the actions to be taken in the event of various problems including system compromise, system malfunction and power outage. These contingency plans must be kept up-to-date to reflect changes in the ASD computing environment. These plans must also be periodically tested to ensure that they will be effective in restoring a secure and reliable computing environment.

1.9. EXTERNAL CONNECTIONS

No ASD computer system may be attached to the Internet unless it is protected by a firewall. Such computer systems include Web servers, electronic commerce servers and mail servers.

1.10. VIRTUAL PRIVATE NETWORKS

To prevent unauthorized disclosure of sensitive and valuable information, all inbound traffic (with the exception of Internet mail and push broadcasts, like Point Caster or Y a h o o

News Ticker) making access to ASD networks must be encrypted with the products approved as part of the ASD Technical Architecture. The connections are often called virtual private networks, or VPNs, and include technologies such as Secure Socket Layer (SSL), Internet Security Association Key Management Protocol (ISAKMP), Point-to-Point Tunneling Protocol (PPTP) or other forms of encryption.

1.11. FIREWALL ACCESS PRIVILEGES

Privileges to modify the functionality, connectivity and services supported by firewalls must be restricted to a few individuals with a business need for these privileges, such as the ASD Information Technology Department personnel. Unless permission from the CAB has been obtained, these privileges will usually be granted only to individuals who are full-time permanent employees of the ASD (no temporaries, contractors, consultants or outsourcing personnel). Vendor access for troubleshooting and technical support may be granted on an as-needed basis. All firewalls must have at least two staff members who are adequately trained to make changes; as circumstances require, they will be retrained to make changes.

1.12. NETWORK MANAGEMENT SYSTEMS

Firewalls must be configured so that they are visible to internal network management systems.

1.13. DISCLOSURE OF INTERNAL NETWORK INFORMATION

The internal system addresses, configurations and related system design information for ASD networked computer systems must be restricted such that neither systems nor users outside the ASD's internal network can access this information. Firewalls must be configured so they will not broadcast route or Simple Network Management Protocol (SNMP) information on an outbound basis.

1.14. SECURE BACK-UP

Current off-line back-up copies of firewall configuration files, connectivity permission files, firewall systems administration procedural documentation files and related files must be kept close to the firewall at all times. A permissible alternative to off-line copies involves online encrypted versions of these files. Either of these options will help to keep trusted copies away from intruders, but at the same time immediately available to reestablish a secure and reliable computing environment. The ASD Information Technology Department will be responsible for maintaining back-up information on all router and firewall configurations.

1.15. FIREWALL CHANGE CONTROL

Because they support critical ASD information systems activities, firewalls are considered to be production systems. This means that all changes to the software provided be vendors (excluding vendor-provided upgrades and patches) must be approved in advance by the ASD Information Technology Department, and then tested and approved before being used in a production environment.

1.16. POSTING UPDATES

Because hackers and other intruders use the latest attack techniques, ASD firewalls must be running the latest software to repel these attacks. Where available from the vendor, all ASD firewalls must subscribe to software maintenance and software update services. Unless approved in advance by the CAB, staff members responsible for managing firewalls must install and run these updates within a week of receipt. This update provision must be met by the ASD Information Technology Department.

1.17. MONITORING VULNERABILITIES

ASD staff members responsible for managing firewalls should subscribe to advisories and other relevant sources providing current information about firewall vulnerabilities. Any vulnerability, which appears to affect ASD networks and systems, must be promptly brought to the attention of the CAB.

1.18. FIREWALL PHYSICAL SECURITY

All ASD firewalls must be situated in locked rooms accessible only to those who must have physical access to such firewalls. The placement of firewalls in the open area is prohibited; although placement within separately locked rooms or areas which are within a general data processing center is acceptable.

2. VPN PROCEDURE

2.1. PURPOSE

The purpose of this procedure is to provide guidelines for Remote Access Virtual Private Network (VPN) connections to the ASD network.

2.2. SCOPE

The procedure applies to all ASD employees, contractors, consultants, temporaries and other workers including all personnel affiliated with third parties utilizing VPNs to access the ASD network. This procedure applies to implementations of VPN that are directed through an IPSec Concentrator or SSL VPN.

2.3. PROCEDURE

Approved ASD employees and authorized third parties (customers, vendors, etc.) may utilize the benefits of VPNs, which are a "user managed" service. This means that the user is responsible for selecting an Internet Service Provider (ISP), coordinating installation, installing any required software and paying associated fees.

Additionally:

2.3.1. It is the responsibility of employees with VPN privileges to ensure that unauthorized users are not allowed access to ASD internal networks.

2.3.2. VPN use is to be controlled through the use of a directory service for individual user authentication.

2.3.3. When actively connected to the ASD network, VPNs will force all traffic to and from the PC over the VPN tunnel; all other traffic will be dropped.

2.3.4. Dual (split) tunneling is NOT permitted; only one network connection is allowed.

2.3.5. VPN gateways will be set up and managed by the ASD Information Technology Department.

2.3.6. All computers connected to ASD internal networks via VPN or any other technology must pass posture assessment performed by an NAC appliance; this includes personal computers.

2.3.7. VPN users will be automatically disconnected from the ASD's network after four hours or thirty minutes of idle time. The user must then log on again to reconnect to the network. Pings or other artificial network processes are not to be used to keep the connection open.

2.3.8. User's computers that are not ASD-owned equipment must configure the equipment to comply with the ASD's VPN and network policies.

2.3.9. Only ASD-approved VPN clients may be used.

2.3.10. By using VPN technology with personal equipment, users must understand that their machines are a de facto extension of the ASD's network, and as such are subject to the same rules and regulations that apply to ASD-owned equipment, i.e. their machines must be configured to comply with the ASD's network policies.

2.4. ENFORCEMENT

Any employee found to have violated this procedure may be subject to disciplinary action, up to and including termination of employment.

3. DMZ PROCEDURE

3.1. PURPOSE

This procedure establishes information security requirements for all networks and equipment deployed in the ASD "De-Militarized Zone" (DMZ). Adherence to these requirements will minimize the potential risk to ASD from the damage to public image caused by unauthorized use of ASD resources, and the loss of sensitive or confidential data.

3.2. SCOPE

ASD networks and devices (including but not limited to routers, switches, hosts, etc.) that are Internet facing and located outside ASD Internet firewalls are considered part of the DMZ and are subject to this procedure. All existing and future equipment, which falls under the scope of this procedure, must be configured according to the referenced documents. This procedure does not apply to networks and devices residing inside ASD's Internet firewalls or trusted networks.

3.3. PROCEDURE

3.3.1. Ownership and Responsibilities

3.3.1.1.   All new DMZ devices must present a business justification with sign-off to the CAB. The ASD Information Technology Department must keep the business justifications on file.

3.3.1.2.   Third-party-owned devices and applications are required to have a point of contact (POC), and back-up POC, for each piece of equipment or application. The device owners must maintain up-to-date POC information with the ASD Information Technology Department (and the enterprise management system, if one exists). Third-party device and application owners or their back-up must be available around-the-clock for emergencies.

3.3.1.3.   Changes to the connectivity and/or purpose of existing DMZ devices and establishment of new DMZ networks and devices must be requested through the ASD Information Technology Department.

3.3.1.4.   All ISP connections must be maintained by the ASD Information Technology Department.

3.3.1.5.   The ASD Information Technology Department must maintain a firewall device between the DMZ and the Internet.

3.3.1.6.   The ASD Information Technology Department reserves the right to interrupt any DMZ-based connections if a security concern exists.

3.3.1.7.   The ASD Information Technology Department must record all DMZ address spaces and current contact information.

3.3.1.8.   The ASD Information Technology Department must have immediate access to equipment and system logs.

3.3.1.9.   With third party DMZ deployments the ASD Information Technology Department will address non-compliance waiver requests on a case-by-case basis.

3.3.2.   General Configuration Requirements

3.3.2.1.   DMZ networks and devices must not be connected to ASD's internal networks, either directly or via a wireless connection.

3.3.2.2.   DMZ networks and devices should be in a locked rack with limited access. In addition, the ASD Information Technology Department must maintain a list of who has access to the equipment.

3.3.2.3.   The ASD maintained firewall devices must be configured in accordance with least-access principles and the DMZ business needs. All firewall filters will be maintained by the ASD Information Technology Department.

3.3.2.4.   The firewall device must be the only access point between the DMZ and the rest of ASD's networks and/or the Internet. Any form of cross-connection which bypasses the firewall device is strictly prohibited.

3.3.2.5.   Original firewall configuration and any changes thereto must be reviewed and approved by the ASD Information Technology Department (including both general configurations and rule sets).

3.3.2.6.   Traffic from the DMZ to the ASD internal network must be configured in accordance with least-access principles. Remote access from the DMZ to the ASD internal network must follow the above stated VPN procedure.

3.3.2.7.   Current applicable security patches/hot-fixes for any applications that are Internet services must be applied.

3.3.2.8.   All applicable security patches/hot-fixes recommended by the vendor must be installed.

3.3.2.9.   Services and applications not serving business requirements must be disabled.

   3.3.2.10. Remote administration must be performed over secure channels (e.g., encrypted network connections using SSH or IPSEC) or console access independent from the DMZ networks.

3.4. ENFORCEMENT

Any employee found to have violated this procedure may be subject to disciplinary action, up to and including termination of employment.

4. TRAFFIC SHAPING PROCEDURE

4.1. PURPOSE

The purpose of this procedure is to provide a methodology for creating traffic shaping rules.

4.2. SCOPE

This procedure applies to all traffic leaving the egress point of the ASD network.

4.3. PROCEDURE

A business analysis needs to be done to classify all traffic in one of three areas: Sensitive, Best-Effort and Undesired. Based upon these three areas shaping of outbound and inbound traffic will occur.

4.3.1. Sensitive Traffic

Sensitive traffic is traffic whose Quality of Service is critical to ASD business functions. This usually includes VoIP, video streaming, financial transactions, business partner virtual connections and other forms of critical data. Shaping schemes are generally tailored in such a way that the Quality of Service of these selected uses is guaranteed, or at least prioritized over other classes of traffic. This can be accomplished by the absence of shaping schemes on these, or by positive shaping (prioritization over others).

4.3.2. Best-Effort Traffic

Best-effort traffic is all other kinds of non-detrimental traffic. This is traffic that ASD is not concerned about and does not consider a priority. Shaping schemes are generally tailored in such a way that this traffic gets "what is left" of the bandwidth after sensitive traffic has "taken its share".

4.3.3. Undesired Traffic

This category is generally referred to as the "bit bucket". Meaning all other traffic not categorized by the above two classes. Shaping schemes usually involve identifying and blocking this traffic entirely, or just by severely hampering its operation.

5. URL FILTERING PROCEDURE

5.1. PURPOSE

The purpose of this procedure is to provide guidelines for filtering Web traffic.

5.2. SCOPE

This procedure applies to all Web traffic leaving the egress point of the ASD network. This procedure will affect all users within the ASD network.

5.3. PROCEDURE

All Web-based traffic will be filtered for inappropriate content as determined by the Web Filter Committee.

5.4. EXCEPTIONS

Requests for exceptions to this procedure can be made by generating a request in writing to the Web Filter Committee. This request will include the name of the school or department, requesting person name and contact information, and an educational justification for the exception.