

**Da Vinci Academy of Science and The Arts**

**Policy Number: 701**

**Policy Section: 700 - Information Technology (IT)**

**POLICY TITLE: IT General Acceptable Use Policy**

**Revision History**

<b>Effective Date</b>	<b>Action Date</b>	<b>Revised</b>
<b>8 October 2008</b>	<b>New Policy</b>	<b>New Policy</b>
August 17, 2023	Renewed with Internet Safety Policy	Revised

General Acceptable Use Policy  
Effective Date: 1 October 2008  
Revision Date:

## I. OVERVIEW

The Information Technology and Acceptable Use Policy is based on Federal and State laws and policies and local DaVinci concerns about the design and use of the DaVinci computer network to protect it and information encoded therein. We are committed to protecting DaVinci Academy from illegal or damaging actions by individuals that are performed either knowingly or unknowingly.

This policy includes but is not limited to, Internet/Intranet/Extranet-related systems and property belonging to DaVinci Academy which includes but is not limited to all computer equipment, all software, all DASA technology items, all operating systems, remote connections/connections of any kind, storage media, networks, all accounts, electronic mail, WWW browsing and FTP.

Effective security is a team effort involving the participation and support of every DaVinci Academy employee and affiliate who deals with information and/or information systems. It is the responsibility of every computer user to know the federal, state, and DaVinci policies and to conduct their activities accordingly.

## 2. PURPOSE

The purpose of this policy is to outline an acceptable use of DaVinci Academy computer equipment, network systems, software, websites, user accounts, state and federal systems as DaVinci uses them and all technology items at DaVinci Academy. The design of the system's and acceptable use rules are in place to protect the employee and DaVinci Academy. Inappropriate system design or use exposes DaVinci Academy to risks including virus attacks, compromise of network systems and services, and legal issues. A central goal of the policy is for all members of the DaVinci community to understand that the design, procurement and use of DaVinci Academy IT resources, state and federal resources, vendor specific resources and technology is regulated by policy and under the direct supervision and the responsibility of the DaVinci IT Director. Individual DaVinci Academy community users must understand that their use of the hardware, software, web services, and networks is a public not a private activity which must be regulated by policy. This policy was created to retain the DaVinci Academy's established culture of openness, trust and integrity.

## 3. SCOPE

This policy applies to all members of the DaVinci Academy (DASA) community including those person(s) or groups who are permanent such as students, parents, faculty, staff, employees and partners, those who are temporary such as contractors, consultants, temporary employees, volunteers, all various DaVinci Academy organizations such as but not limited to DaVinci PTO, committees, DaVinci clubs, groups and DaVinci alumni, as well as all personnel who are affiliated with third parties or those person(s) or groups who make up third parties, vendors,

contractors, suppliers and other various workers and non workers affiliated with DaVinci. This policy applies to all equipment, networks, wireless devices, web technologies and services, remote connections of any kind, user accounts, state and federal applications and confidential data, all software and in general any technology based product that is owned, donated to the school or leased by DaVinci Academy. This policy applies to all DASA community members, anyone who has access to system(s) inside or outside of the school and who uses these items or anyone who represents as an affiliate of the school inside or outside of the school. *(This policy is in compliance with Utah State Code Part 2 Section 9-7-215)*

#### **4. POLICY INHERITANCE**

The Acceptable Use Policy adheres to all Federal, State, Local and USOE laws as shown below in 4.1. References. Should any of these policies change or new policies be created, the new federal or state policy will take precedence over and update the present policy.

##### **4.1. REFERENCES**

- 4.1a Federal Communications Commission order 03-188 Childs Internet Protection Act (CIPA) {see attachment "A" for a brief overview of the CIPA Act}
- 4.1b Federal Law 20 U.S.C. § 1232g; 34 CFR Part 99: Family Educational Rights and Privacy Act (FERPA) (see attachment "B" for a brief overview of the FERPA Act)
- 4.1c 18 U.S.C. § 2510: Electronic Communications Privacy Act
- 4.1d Utah Code Ann § 76-6-703: Utah Computer Crimes Act
- 4.1e Utah Code Ann § 76-10-1801: Communications Fraud
- 4.1f Utah Code Ann § 63-2-101 et seq: Government Records Access and Management Act (GRAMA)

#### **5. USE POLICY**

**5.1 The following are DaVinci Academy specific restrictions and acceptable usage of DaVinci Academy owned resources.**

##### **5.2 General Use and Ownership**

- 5.2a Users should be aware that the data they create on the DaVinci Academy systems or through the DaVinci Academy resources remains the property of DaVinci Academy. Because of the need to protect tjaVinci Academy's network, computers, software and owned resources IDaVinci cannot guarantee the confidentiality of information stored on any network device belonging to DaVinci Academy.
- 5.2b Employees will be held responsible for knowing the policy and relevant statutes *(Refer to section 4.1)* and exercising good judgment regarding the use of DaVinci Academy owned resources. In the absence of IT policies, employees should be

- guided by DASA IT best practices, standards and processes, and if there is any uncertainty, employees should consult the IT Director or Executive Director.
- 5.2c The IT Director recommends that any information that users consider personally sensitive or vulnerable not be placed on the computer network or be encrypted. Please note that encryption will not prevent inspection of the digital information encoded by designates of the school (see 5.2a).
- 5.2d For security and maintenance purposes, the IT Director has authority and is empowered to perform regular and detailed monitoring of equipment, systems, E-Mail accounts, user accounts, personally owned laptops and devices and network traffic at any time due to the fact that the worse threats of viruses come through e-mail, spy ware and ad ware through unauthorized web site traffic. Targeted monitoring of specific Email accounts may be performed by the IT Director on a case-by-case basis. The IT Director will notify the Executive Director, and the DASA board in a timely manner on all monitoring, with a monitoring log, when a situation arises that is deemed inappropriate, and any action taken will be a collaborative effort in the best interests of the students and the school.
- 5.2e There is an active content filter device to filter out web sites that are not DaVinci approved and may contain harmful viruses or spyware. If any DASA community member needs a web site unblocked, they need to submit the web site url/web address/ftp address in an e-mail to the DaVinci Academy IT Director at least one day in advance before its intended use. The IT Director will be responsible for deciding whether or not to allow the requested site to be made available.
- 5.2f. The IT Director's decision to unblock or not unblock web site for a DASA community member should be based on whether the site is needed for professional use during the school-time and appropriate personal use (for the convenience of the DASA community member) for other times. No private business correspondence will be permitted to ensure compliance to policy.

### 5.3 Security and Proprietary Information

- 5.3a The user interfaces and applications for information contained, used or maintained on Internet/Intranet/Extranet-related systems should be classified as either confidential or not confidential. Examples of confidential information include but are not limited to: DaVinci propriety information, State or Federal systems and applications, connections, internal systems, research data, and student information of any kind (*see the referenced FERPA Act for more information*). Employees should take all necessary steps to prevent unauthorized access to this information. *Da Vinci Academy's Confidential Information policy* also applies to sections 5.3a - 5.3f.
- 5.3b Keep passwords secure and do not share accounts, passwords or any kind of school data. Authorized users are responsible for the security of their passwords, accounts and school data that they are stewards over. System level passwords will be changed quarterly; user level passwords will be changed every six months.

- 5.3c All PCs, laptops and workstations will be secured with a password-protected screen saver with the automatic activation feature set at 7 minutes or more, or by logging-off (control-alt-delete for Win2K users) when the host is unattended. DASA community member personal laptops are permitted only on the approval of the IT Director and under the requirements set forth by IT Director and all other it polides, best practices and processes.
- 5.3d Because information contained on portable computers is especially vulnerable in public spaces, special care should be exercised. Protect laptops and devices in accordance. DaVinci Academy Student Directory Information, State and Federal confidential school data will not be allowed on any personal owned laptops or device unless the IT Director has approved of it and your job/duties qualifies it. *(See the referenced FERPA Act for more information.)*
- 5.3e Employee's as well as DASA community members are prohibited from accessing or changing State and Federal applications, remote applications, access controls, user rights, permissions, accounts, confidential data therein and connections of any kind, unless this activity is a part of the [employee's normal job/duty and the IT Director has given approval. The IT Director will manage, delegate and setup any of the above mentioned State and Federal items based on the employee's normal job/duty and being in conjunction with State regulations and the Executive Director. It is prohibited for a DASA community member to give, impart, or let others see any State or Federal confidential data, user names, passwords or IP Addresses unless it is part of the employee's normal job/duty.
- 5.3f Postings by employees from a DaVinci Academy e-mail address to newsgroups should contain a disclaimer stating that the pinions expressed are strictly their own and not necessarily those of DaVinci Academy, unless posting is in the course of business duties. Indeed no reference to your DaVinci position should be made in the body of the text, subject lines or in the signature. Postings which refer to an individual's employment at DaVinci needs to be approved by the DaVinci Executive Director.
- 5.3g All hosts, hosting providers or other services used by the employee that are connected to the DaVinci Academy Intranet/Extranet, whether owned by the employee or DaVinci Academy, shall b' continually executing approved virus-scanning software and content filtering with a current virus database *(see the referenced CIPA Act for more information).*
- 5.3h Employees must use extreme caution when, opening e-mail attachments received from unknown senders, which may contain viruses, e-mail bombs, or Trojan horse code. It is expected that cases of email atct:chments from an unknown sender will be referred to the IT Director prior to it beig opened.

## 5.4 Unacceptable Use

5.4a The following are specifically prohibited for all DaVinci community members (unless otherwise exempted by the IT Director). The prohibition applies to DASA community members using either the DaVinci network, wireless services, computers, printers, fax machines, websites, technologies of any kind or other devices (including cell phones) or off-site networks while the member is acting as an associate of the DaVinci community, whether inside the school or out.

### 5.4b Prohibitions against general IT-Related Activities

- i. Under no circumstances is a community member of DaVinci Academy authorized to engage in any information technology or information systems-related activity that is illegal under local, state, federal or international law.
- ii. Under no circumstances is a community member of DaVinci Academy authorized to engage in any information systems or information technology-related activity that is pornographic in nature or makes reference to pornographic activities, images or nuances. Such activity includes making pornography available by displaying generating, distributing, forwarding, hiding through encryption or storing the pornography using DaVinci Academy facilities such as the internet, software packages, email, storage devices, mobile telephones or computer hardware or using other facilities, media, and network(s) while involved or engaged in DaVinci Academy activities whether in school or out.

***Pornography is understood by the School to be material of any sexual nature, explicit sexual nature that is intended, implied, proposed or calculated to sexually excite, stimulate, encourage, motivate or arouse, which may be in the form of visual texts, including photographs, or moving images, such as video files including mpg, avi, recordings and ram files, or written texts of any kind, or audio files of any kind.***

- iii. Under no circumstances is a community member of DaVinci Academy authorized to engage in any related activity that involves in any way the DASA network and its resources, wireless resources, computer resources, telecommunication resources leased donated or bought equipment and/or data/voice service lines to operate or maintain a private business.
- iv. Under no circumstances is a community member of DaVinci Academy authorized to allow anyone who has not been authorized by the IT Director to use any of the DaVinci Academy-owned resources such as computers, wireless networking devices, hardware, phones, fax machines, printers, internet/intranet, telecommunication resources, software or any other devices owned, leased or maintained by DaVinci Academy.

## 5.4c. Prohibited System and Network Activities

- i. Under no circumstances is a community member of DaVinci Academy authorized to violate the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by DaVinci Academy.
- ii. Under no circumstances is a community member of DaVinci Academy authorized to copying of copyrighte material including, but not limited to, digitization and distribution of photographs from magazines, books, student pictures, and/or other copyrighted sources, copyrighted music, copyrighted videos and the installation of any copyrighted software for which DaVinci Academy or the end user does not have an active license, is strictly prohibited.
- iii. Under no circumstances is a community member of DaVinci Academy authorized to export software, technical information, encrypted software or technology without express permission. If the need arises then the appropriate management will be consulted prior to export of any material that is in question.
- iv. Under no circumstances is a community member of DaVinci Academy authorized to use programs which may be malicious or cause any kind of "lag" or "down time" to the network (e.g., introducing viruses worms, Trojan horses, e-mail bombs, etc into the network, server(s), computers and email or use port scanners and other various network tools). A community member must contact the IT Director if there is the least bit of suspicion that a program, user or users actions may have deleterious effects on the system.
- v. Under no circumstances is a community member of DaVinci Academy authorized to reveal any account(s) and/or password(s) to others or allow use of your account by others. This includes family and other household members when work is being done at home or at the school after employment hours.
- vi. Under no circumstances is a community member of DaVinci Academy authorized to use DaVinci Academy computing asset(s) to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws in the user's local jurisdiction, chain email or other various forms. The sending of such material through other networks or computers to another trtember of the community is also a violation.

- vii. Under no circumstances is a community member of DaVinci Academy authorized to use a DaVinci Academy leased, owned or donated computing asset(s), network resources, data or voice lines or web service(s) to actively engage in any personal use or other business operation not specific to DaVinci Academy unless approved by the IT Director. Permitted personnel use is defined in the Personal Use and Procedure Policy.
- viii. Under no circumstances is a community member of DaVinci Academy authorized to allow family members, friends, correspondents, vendors, students or anyone that has not been authorized by the IT Director and is not an employee of DaVinci Academy to use any of the DaVinci Academy resources, computers and internet or checked out laptops.
- ix. Under no circumstances is a community member of DaVinci Academy authorized to use IT resources to make fraudulent offers of products, items, warranties, or services originating from or arriving at any DaVinci Academy's account(s), on blogs, forums, portals or news groups.
- x. Under no circumstances is a community member of DaVinci Academy authorized to engage in any activity which affects security breaches or disruptions of network communications. Security breaches and disruptions include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server, networked appliance or account that the employee is not expressly authorized to access, unless these duties are within the scope of regular duties and done so under the direction of the IT Director. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, pinged floods, fingerprinting, packet spoofing, denial of service, distributed denial of service attacks, media streaming services, ftp services, proxy servers or services, tunneling servers or services, any instant messaging systems, wireless resources or services and forged routing information for malicious purposes, installing any servers, services or otherwise items that may disrupt network traffic or define a security breach.
- xi. Under no circumstances is a community member of DaVinci Academy authorized to engage in port scanning or security scanning unless prior notification and approval of the IT Director has been given.
- xii. Under no circumstances is a community member of DaVinci Academy authorized to execute any form of network monitoring which will intercept data not intended for the employee's host, unless this activity is a part of the employee's normal job/duty and done under the direction of the IT Director.



- xiii. Under no circumstances is a community member of DaVinci Academy authorized to circumvent user authentication or security of any host, network or account.
- xiv. Under no circumstances is a community member of DaVinci Academy authorized to interfering with or denying service to any user, (for example, denial of service attack or mass mail bombs).
- xv. Under no circumstances is a community member of DaVinci Academy authorized to operating systems, program(s)/script(s)/command(s), or to send messages of any kind with the intent to interfere with, circumventing the current system for any reasons or disable, a user's terminal session, or VPN sessions via any means, locally or via the Internet/Intranet/Extranet.
- xvi. Under no circumstances is a community member of DaVinci Academy authorized without the IT Director's permission to procure, install or set up any networked systems (routers, switches, firewalls, LAN connections, wireless devices, wireless connections, computers, software or printers or remote accesses of any kind) software systems, databases, applications, USB devices, printers, software or any other devices, information systems or information technology systems.
- xvii. Under no circumstances is a community member of DaVinci Academy authorized to provide information stored on the DaVinci network about, or lists of, DaVinci Academy community members to parties outside of DaVinci Academy.
- xviii. Under no circumstances is a community member of DaVinci Academy authorized, without the IT Director's permission and/or direction, to procure, create or setup any type of website, web server, forum(s) portal site(s), news groups, blogs, web services or procure, create or setup any hosting-third party web service providers/site(s) for DaVinci Academy use inside or outside DaVinci Academy and that represents DaVinci Academy in any way.
- xix. Under no circumstances is a community member of DaVinci Academy authorized without the IT Directors' permission to physically open up, take apart, try to fix or move a DaVinci owned computer, laptop printer or DaVinci owned resource of any kind.
- xx. Under no circumstances is a community member of DaVinci Academy authorized to connect any wired or wireless devices to the DaVinci network without the permission from the IT Director.

## 5.4d Prohibited E-mail and Communications Activities

- i. Under no circumstances is a community member of DaVinci Academy authorized to send unsolicited e-mail messages, including the sending of "junk mail", "Chain letters or chain mail" or other advertising material to individuals who did not specifically request such material (e-mail spam).
- ii. Under no circumstances is a community member of DaVinci Academy authorized to use the DASA infrastructure or other networks to engage in any form of harassment via e-mail, telephone or paging, whether through language, frequency, or size of messages.
- iii. Under no circumstances is a community member of DaVinci Academy authorized to alter, or forge e-mail header information.
- iv. Under no circumstances is a community member of DaVinci Academy authorized to solicit e-mail for any other e-mail address, other than that of the poster's account, with the intent to harass or to collect replies.
- v. Under no circumstances is a community member of DaVinci Academy authorized to create or forward "Ponzi" or other "pyramid" schemes of any type.
- vi. Under no circumstances is a community member of DaVinci Academy authorized to send unsolicited e-mail originating from within DaVinci Academy's networks or other Internet/Intranet/Extranet providers on behalf of, or to advertise, any unauthorized service hosted by DaVinci Academy or connected via DaVinci Academy's network or generated at DaVinci Academy.
- vii. Under no circumstances is a community member of DaVinci Academy authorized to post the same or similar non-school related messages to large numbers of Usenet newsgroups (newsgroup spam).
- viii. All e-mails and e-mail attachments of the DASA community member(s) are subject to routine monitoring for compliance to the Acceptable Use Policy, other IT policies and best practices. E-mail is checked from time to time to insure its proper use and for auditing and data records.
- ix. All e-mail is archived and backed up then kept under retention for years according to the *DASA e-mail retention policy*.
- x. All DaVinci Academy community members must use their DaVinci Academy provided e-mail account for ALL school related items and communications with staff, student and faculty and when they are

representing Davinci in any way. Do not use your personal e-mail account for any school related items.

#### 5.4e Prohibited Blogging Activities and the Use of Portals, Forums and Newsgroups.

- i. Blogging or the use of portal sites, news groups or forums by members of the DaVinci community (whether using DaVinci Academy's property and systems or personal computer systems) is also subject to the terms and restrictions set forth in this Policy. Limited and occasional use of DaVinci Academy's systems to engage in blogging, news groups, forums or portal sites is acceptable, provided that it is done in a professional and responsible manner, does not otherwise violate DaVinci Academy's policies, is not for personal owned business use and does not interfere with an employee's regular work duties. Blogging participating in forums, news groups or portal sites from DaVinci Academy's systems is also subject to monitoring.
- ii. ***Da Vinci Academy's Confidential Information policy*** also applies to blogging the participation in forums, news groups or portal sites. This policy also applies when procuring, creating or using blogging sites, forum(s), news groups or portal sites. As such, Employees are prohibited from revealing any DaVinci Academy confidential or proprietary information, trade secrets or any other material covered by DaVinci Academy's Confidential Information policy and the FERPA law when engaged in blogging the use of portal sites, news groups or forums of any kind.
- iii. All community members of DaVinci Academy are prohibited from making any discriminatory, defamatory or harassing comments about other community members when blogging, posting to news groups or using on-line forums while representing DaVinci Academy inside or outside the school in any way. Such a policy is consistent DaVinci Academy's Non- Discrimination and Anti-Harassment policy.
- iv. If a community member is expressing his or her beliefs and/or opinions in blogs, news groups or on-line forums the member may not, expressly or implicitly, represent themselves as a representative of DaVinci Academy. DASA community members assume any and all risk associated with blogging the use of portal sites, news groups or forums of any kind.
- v. Apart from following all laws pertaining to the handling and disclosure of copyrighted or export controlled materials, DaVinci Academy's trademarks, logos, images, statements, designs, creations and any other DaVinci Academy intellectual property may also not be used by members of the DaVinci Academy community in connection with any blogging, news groups or the use of portals, forums sites or personal websites.

6. **ENFORCEMENT**

- 6.1. Any DaVinci employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.
- 6.2. Any DaVinci student found to have violated this policy may be subject to disciplinary action, up to and including expulsion.
- 6.3 Any DaVinci volunteer found to have violated this policy may be subject to disciplinary action, up to and including revoking the member's volunteer status.
- 6.4 Any DaVinci partner found to have violated this policy may be subject to disciplinary action, up to and including termination of the partnership.
- 6.5. Any subcontractor, vendor or third party providers hired by DaVinci found to have violated this policy may be subject to disciplinary action, up to and including termination of the contract with DaVinci.
- 6.6. All other internal policies, best practices, processes and procedures are applicable and do apply where necessary in accordance with this policy.

I have read, understand, and agree to comply with the foregoing, federal and state laws, DASA policies, rules, regulations and conditions governing the use of the DaVinci Academy's computer information systems and information technology systems and equipment and all services herein. I understand that I have no expectation of privacy when I use any of the equipment, internet services or e-mail. I am aware that violations of these guidelines on appropriate use of the e-mail and various systems may subject me to disciplinary action, including termination from employment, legal action and criminal liability. I further understand that my use of the e-mail, internet, portals, news groups, blogs and forum participations may reflect on the image of DaVinci Academy to our customers, competitors, suppliers, volunteers, parents or students and that I have responsibility to maintain a positive representation of the company. Furthermore, I understand that this policy can be amended at any time.

**Signature of User:** \_\_\_\_\_

**Dated:** -----

## 6. DEFINITIONS

Term	Definition
------	------------

*Blogging:* Writing a blog. A blog (short for weblog) is a personal online journal that is frequently updated and intended for general public consumption.

*Forums:* A bulletin board system in the form of a discussion site. From a technological standpoint, forums or boards are web applications sometimes web services managing user-generated content. Forums often contain private messaging, moderators, etc.

*Spam:* Unsolicited or undesired bulk electronic messages, posting random comments and random tips/ideas or promoting commercial services to blogs, wikis, guestbooks, advertisements and forgery on newsgroups, illegal blanket advertising in public places.

*News*

*Group:* A repository usually within the Usenet system, for messages posted from many users in different locations.

*Da Vinci Academy (DASA)*

*Community*

*Member:* Defined as: Those person(s) or groups who are permanent such as students, parents, faculty, staff, employees and partners, those who are temporary such as contractors, consultants, temporary employees, volunteers, all various DaVinci Academy organizations such as but not limited to DaVinci PTO, committees, DaVinci clubs, groups and DaVinci alumni. As well as all personnel who are affiliated with third parties or Those person(s) or groups who make up third parties, vendors, contractors, suppliers and other various workers and non workers affiliated with DaVinci.

## Attachment "A"

### **FCC order 03-188 CIPA Act (Child Internet Protection Act).**

#### **CIPA Background**

The Children's Internet Protection Act (CIPA) is a federal law enacted by Congress in December 2000 to address concerns about access to offensive content over the Internet on school and library computers. CIPA imposes certain types of requirements on any school or library that receives funding for Internet access or internal connections from the E-rate program - a program that makes certain communications technology more affordable for eligible schools and libraries. In early 2001, the FCC issued rules implementing CIPA.

#### **What CIPA Requires**

- Schools and libraries subject to CIPA may not receive the discounts offered by the E-rate program unless they certify that they have an Internet safety policy and technology protection measures in place. An Internet safety policy must include technology protection measures to block or filter Internet access to pictures that: (a) are obscene, (b) are child pornography, or (c) are harmful to minors and employees.
- Schools subject to CIPA are required to adopt and enforce a policy to monitor online activities of minors.
- Schools and libraries subject to CIPA are required to adopt and implement a policy addressing: (a) access by minors to inappropriate matter on the Internet; (b) the safety and security of minors and employees when using electronic mail, chat rooms, and other forms of direct electronic communications; (c) unauthorized access, including so-called "hacking," and other unlawful activities by minors online; (d) unauthorized disclosure, use, and dissemination of personal information regarding minors; and (e) restricting minors' and employees access to materials harmful to them.

*Schools and libraries are required to certify that they have their safety policies and technology in place before receiving E-rate funding.*

- CIPA does not affect E-rate funding for schools and libraries receiving discounts only for telecommunications, such as telephone service.
- An authorized person may disable the blocking or filtering measure during any use by an adult to enable access for bona fide research or other lawful purposes.
- CIPA does not require the tracking of Internet use by minors or adults

Federal Communications Commission  
Consumer & Governmental Affairs Bureau, FCC order 03-188

## Attachment "B"

### **20 U.S.C. § 1232g; 34 CFR**

### **FERPA Act (Family Educational Rights and Privacy Act)**

Part 99) is a Federal law that protects the privacy of student education records. The law applies to all schools that receive funds under an applicable program of the U.S. Department of Education.

FERPA gives parents certain rights with respect to their children's education records. These rights transfer to the student when he or she reaches the age of 18 or attends a school beyond the high school level. Students to whom the rights have transferred are "eligible students."

- Parents or eligible students have the right to inspect and review the student's education records maintained by the school. Schools are not required to provide copies of records unless, for reasons such as great distance, it is impossible for parents or eligible students to review the records. Schools may charge a fee for copies.
- Parents or eligible students have the right to request that a school correct records which they believe to be inaccurate or misleading. If the school decides not to amend the record, the parent or eligible student then has the right to a formal hearing. After the hearing, if the school still decides not to amend the record, the parent or eligible student has the right to place a statement with the record setting forth his or her view about the contested information.
- Generally, schools must have written permission from the parent or eligible student in order to release any information from a student's education record. However, FERPA allows schools to disclose those records, without consent, to the following parties or under the following conditions (34 CFR § 99.31):
  - School officials with legitimate educational interest;
  - Other schools to which a student is transferring;
  - Specified officials for audit or evaluation purposes;
  - Appropriate parties in connection with financial aid to a student;
  - Organizations conducting certain studies for or on behalf of the school;
  - Accrediting organizations;
  - To comply with a judicial order or lawfully issued subpoena;
  - Appropriate officials in cases of health and safety emergencies; and
  - State and local authorities, within a juvenile justice system, pursuant to specific State law.

Schools may disclose, without consent, "directory" information such as a student's name, address, telephone number, date and place of birth, honors and awards, and dates of attendance. However, schools must tell parents and eligible students about directory information and allow parents and eligible students a reasonable amount of time to request that the school not disclose directory information about them. Schools must notify parents and eligible students annually of

their rights under FERPA. The actual means of notification (special letter, inclusion in a PTA bulletin, student handbook, or newspaper article) is left to the discretion of each school.



**Internet Safety Policy  
For DaVinci Academy  
of Science and the Arts  
(DASA)**

**Introduction**

It is the policy of DaVinci Academy of Science and the Arts (DASA) to: (a) prevent user access over its computer network to, or transmission of, inappropriate material via Internet, electronic mail, or other forms of direct electronic communications; (b) prevent unauthorized access and other unlawful online activity; (c) prevent unauthorized online disclosure, use, or dissemination of personal identification information of minors; and (d) comply with the Children's Internet Protection Act [Pub. L. No. 106-554 and 47 USC 254(h)].

**Definitions**

Key terms are as defined in the Children's Internet Protection Act.\*

**References**

**Utah Annotated Code 53G-7-10**

**Children's Internet Protection Act [Pub. L. No. 106-554 and 47 USC 254(h)]**

**DASA Acceptable Use Policy**

**Access to Inappropriate Material**

To the extent practical, technology protection measures (or "Internet filters") shall be used to block or filter Internet, or other forms of electronic communications, 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.

Subject to staff supervision, technology protection measures may be disabled for adults or, in the case of minors, minimized only for bona fide research or other lawful purposes.

**Inappropriate Network Usage**

To the extent practical, steps shall be taken to promote the safety and security of users of the DASA online computer network when using electronic mail, chat rooms, instant messaging, and other forms of direct electronic communications.

Specifically, as required by the Children’s Internet Protection Act, prevention of inappropriate network usage includes: (a) unauthorized access, including so-called ‘hacking,’ and other unlawful activities; and (b) unauthorized disclosure, use, and dissemination of personal identification information regarding minors.

### **Education, Supervision and Monitoring**

It shall be the responsibility of all members of the DASA staff to educate, supervise and monitor appropriate usage of the online computer network and access to the Internet in accordance with this policy, the Children’s Internet Protection Act, the Neighborhood Children’s Internet Protection Act, and the Protecting Children in the 21<sup>st</sup> Century Act.

Procedures for the disabling or otherwise modifying any technology protection measures shall be the responsibility of IT Manger or designated representatives.

The IT Director along with the School Principals or designated representatives will provide age- appropriate training for students who use the DASA’s Internet facilities. The training provided will be designed to promote the DASA’s commitment to:

- a. The standards and acceptable use of Internet services as set forth in the DASA’s Internet Safety Policy;
- b. Student safety with regard to:
  - i. safety on the Internet;
  - ii. appropriate behavior while on online, on social networking Web sites, and in chat rooms; and
  - iii. cyberbullying awareness and response.
- c. Compliance with the E-rate requirements of the Children’s Internet Protection Act (“CIPA”).

Following receipt of this training, the student will acknowledge that he/she received the training, understood it, and will follow the provisions of DASA’s acceptable use policies.

### **Adoption**

This Internet Safety Policy was adopted and added to the General Acceptable Use Policy by the Board of DASA at a public meeting, following normal public notice, on August 16, 2023. And amended every three years