EGAEA-R1 – Regulation of Use of Electronic Mail and Internet Systems

The following regulation is developed for the implementation of School Board Policy EGAEA – Electronic Mail and Internet. This regulation is designed to be consistent with the general purpose and principles outlined in Policy EGAEA, as well as consistent with federal and state statutes, and local ordinances.

Purpose

The District's Regulation for Acceptable Use of Electronic Mail and Internet Systems is to prevent unauthorized use, access and other unlawful activities by users online and offline, prevent unauthorized disclosure of or access to District information, and to comply with the Children's Internet Protection Act ("CIPA") including without limitation, all applicable state and federal laws concerning electronic communications, privacy, copyrights, personally identifiable, confidential, and legally protected information. As used in this policy, "user" includes anyone using the District internet and or intranet which includes any device that connects to the District System or holds District information regardless of the physical location of the user. This regulation applies even when District provided equipment (laptops, tablets, etc.) is used off of District property.

Regulation

Access is provided primarily for education and District business. By using the District System, users have agreed to adhere to terms and conditions of this policy. If a user is uncertain about whether a particular use is acceptable or appropriate, he or she should call the DoTS Hotline at 720-423-3888 or consult their supervisor or other appropriate District personnel.

The District reserves the right to take immediate action regarding any activity that may create security and/or safety issues for the District and its students, employees, schools, or District System; or device as defined in this policy, or expend District resources on content the District, in its sole and absolute discretion, determines to lack legitimate educational content/purpose, or other activities deemed inappropriate. Examples include, but are not limited to the type of prohibited activities and uses the District may act upon at any time, with or without providing notice to any user are below.

1 Violating any state or federal law municipal ordinance or applicable District policy or regulation;

2 Accessing or transmitting pornography of any kind, obscene depictions, harmful materials, materials that encourage others to violate the law, confidential information or copyrighted materials;

3 Criminal activities that can be punished under law;

4 Selling or purchasing illegal items or substances;

5 The unauthorized collection of email addresses (“harvesting”) of e-mail addresses from the Global Address List and other District directories;

6 Obtaining and/or using anonymous email sites; spamming; spreading viruses;

7 Causing harm to others or damage to their property such as using profane, abusive, or impolite language; threatening, harassing, or making damaging or false statements about others or accessing, transmitting, or downloading offensive, harassing, or disparaging materials;

8 Deleting, copying, modifying, or forging other users' names, emails, files, or data; disguising one's identity, impersonating other users, or sending anonymous email;

9 Damaging computer equipment, files, data or the District System in any way, including intentionally accessing, transmitting or downloading computer viruses or other harmful files or programs, or disrupting any computer system performance;

10 Using any District computer to pursue “hacking,” internal or external to the District, or attempting to access information protected by privacy laws;

11 Accessing, transmitting or downloading large files, including "chain letters" or any type of "pyramid schemes";

12 Engaging in uses that jeopardize access or lead to unauthorized access into others’ accounts or other computer networks by using another’s account password(s) or identifier(s); interfering with other users' ability to access their account(s); or disclosing your own or anyone’s password to others or allowing them to use your or another’s account(s).

13 Using the District System for:

13.1 Unauthorized commercial purposes personal financial gain

13.2 Personal advertising, promotion, or financial gain

13.3 Conducting for-profit business activities and/or engaging in non-government related fundraising or public relations activities such as solicitation for religious purposes, lobbying for personal political purposes

Definitions

DPS User
The user is every person given access to a DPS network and or use of personal and or confidential student or employee identifiable information in any form.

Device
A device is a machine such a laptop, desktop, and mobile devices including tablets, smart phones, thumb drives, backup drives, compact discs, DVDs, and any electronic portable storage devices.

Personal, Confidential and Student and Employee Identifiable Information
This includes but is not limited to any information about an individual student and employee that may be used to distinguish or trace his or her identity, a name, social security number, date and place of birth, mother‘s maiden name, or biometric records and other information such as medical, educational, financial, and employment information that could be linked or linkable to an individual, that DPS has an obligation to maintain and safeguard as a matter of state and federal laws.

District System
The District System is defined as any computer system, electronic devices or network provided by Denver Public Schools that supports information technology or technology services.

Expectations

District employees as managers of many types of data, physical or electronic, should exercise good stewardship to protect information belonging to the district especially information considered to be personally identifiable information of its students, employees and members of the DPS community. This includes any information that is used through cloud applications or web based tools. Users should exercise discretion and understand the terms, conditions and agreements of external websites and third party applications where data may be stored before using any website, application, technology and service, free or paid, to store, manage, distribute and access any student and/or employee information in the care, control and possession of the District.

Responsibilities

Just as everyone in the District is expected to use the District’s physical resources responsibly, Users are expected to safeguard and maintain all District information resources. Protecting information includes any medium, including but not limited to digital, hard copy or verbally communicated materials that may be used to personally identify a District employee, student, and District community member. As a data manager, each User is responsible for protecting and preventing the unauthorized disclosure of information considered private and/or protected without the expressed permission of its owner or an authorized DPS representative.

Protecting DPS Information Resources from Physical Access
You are responsible for the use of the District information resources that you have been provided. You must prevent unauthorized use of District information resources by preventing others from obtaining access to your computer, or any tablet or mobile device.

Protecting DPS Information Resources from Electronic Access

Likewise, you are responsible for protecting information resources from unauthorized electronic access by using effective passwords (or other access controls) and by safeguarding those passwords. Although you may believe that the data you store on a DPS computer system needs no protection from access, remember that an insecure account may provide an access point to the entire DPS System. Persons attempting to gain unauthorized access to DPS networks do so through user accounts, and your password may be the only safeguard against such access.

Using Electronic Communications Responsibly
District users are encouraged to use electronic communications for District-related activities and to facilitate the efficient exchange of useful information. However, access to the District's electronic communications services is a privilege, and certain responsibilities accompany that privilege.

Complying with the Terms of the User Agreement
As a member of the District, you are expected to read, understand, and comply with the terms of the District's applicable policies regarding the use and operation of the District's System and information. If you have any questions, contact the DoTS Hotline at 720-423-3888.

Requirements

You are the only person allowed to use an information resource (such as an electronic identifier or an electronic mail account) that the District has provided for your exclusive use. Therefore you shall do as follows:

Passwords
NEVER GIVE YOUR PASSWORD TO ANYONE ELSE, even people you trust, such as your friends or relatives or someone who has offered to help you fix a problem. If you suspect someone may have discovered or guessed your password, change it immediately.

Charges
You are responsible for all charges accrued using the DPS resources and devices assigned to you, even if someone else uses your account without your permission.

Access
Do not give others access to District Information, its System or resources unless they are authorized and authenticated to do so.

Personal Use for Gain
You may not be paid, or otherwise profit, from the use of any District-provided information resource, device or from any output produced while using the District System.

Copyrights and Trademarks

Never agree not to infringe upon any copyrighted or trademark protected materials. It is a violation of federal law to participate in copyright and trademark infringement. The District complies with all legal requests (e.g., subpoenas) for information and will not hesitate to report your use in response to a lawful request. Copyrighted and trademark protected materials include, but are not limited to, computer software, audio and video recordings, photographs, electronic books, and written material. If you share movies or music that you did not create, you may be infringing on another's copyright. Consequences of copyright or trademark infringement can include disciplinary actions by the District. In addition, copyright and or trademark owners or their representatives may sue persons in federal courts who infringe on another's copyright.

Login Procedures

You will never try to circumvent login procedures on any system or otherwise attempt to gain access where you are not allowed. Never deliberately scan or probe any information resource without prior authorization. Such activities are not acceptable under any circumstances and can result in serious consequences, including disciplinary action.

Purchase Card Program

This expressly applies to any and all DPS Purchase Card who make purchases of software, software subscriptions, and applications must thoroughly review before downloading or purchasing the terms of use and privacy policy of the software to ensure that DPS Information, especially data that may include student or employee personally identifiable information data, is protected in accordance with federal and state laws and regulations including but not limited to privacy acts: FERPA, COPPA, and CORA. A list of approved and unapproved software is available at www.dpsk12.org/dpsapplist

Loss/Theft of Data, Device, or information

As the user, you are responsible for any loss of District Information whether stored and kept physically or on a private owned or District owned Device include but not limited to, CDs, portable storage devices, laptops, or tablets. Each incident of loss, release or breach, will be evaluated on a case by case basis and if necessary DPS may take the appropriate disciplinary action.

Penalties for Improper Use

The use of the District System and information is a privilege not a right, any misuse will result in the restriction, suspension, or cancellation of the user's rights. Any unauthorized or misuse of District information may also lead to disciplinary, legal and/or corrective action being taken against any user, up to and including termination from District employment, or referral to government authorities for possible criminal prosecution.

Reporting Improper Use

To report any violations of this policy, contact the DoTS hotline at 720-423-3888.

Questions
Questions about this policy should be directed to the DoTS hotline at 720-423-3888, or your DPS legal department at 720-423-3394.

Adopted ------, 2015

LEG. REF.:
20 U.S.C.A. § 6301 (Children's Internet Protection Act (CIPA)

CROSS REF.:
EGAEA, Electronic and Internet Mail

EGAEA-R1, Regulation of Social Media