Diocese of San Jose - Drexel School System

Technology Use & Internet Policy

FOR THE 2018/2019 SCHOOL YEAR

Overview

Technology and the Internet are important resources for the Drexel School System, a K-8 network of schools in the Diocese of San Jose henceforth referred to in this document as DSS. DSS will use technology and the Internet to improve services and contribute broadly to its mission.

All DSS policies and procedures apply to student's conduct on the Internet and with technology, especially, but not exclusively, relating to: intellectual property, confidentiality, information dissemination, standards of conduct, misuse of DSS resources, anti-harassment, and information and data security.

Purpose

This policy is intended to identify the principles of acceptable use and unacceptable use of the Internet and technology; define DSS specifically reserved rights; address enforcement and violations; define and accept associated fee schedule. The parent/guardian of each student granted access privileges will be required to acknowledge and sign this document.

Principles of Acceptable Use

Students may use DSS's technology and Internet/Intranet access only for authorized purposes. DSS students are required:

- To respect the work product of others. Students shall not intentionally seek information on, obtain copies of, or modify files or data maintained by other students, unless explicit permission to do so has been obtained.
- To respect copyright and license agreements for software, digital artwork, and other forms of electronic data.
- To protect DSS data from unauthorized use or disclosure in accordance with state and federal laws and DSS regulations.
- To respect the integrity of computing systems: for example, students shall not use or develop programs that harass other students or infiltrate a computer or computing system and/or damage or alter the hardware or software components of a computer or computing system.
- To safeguard their accounts and passwords. Accounts and passwords are assigned to a single student and are not to be shared with any other person without authorization. Students are expected to report any observations of attempted security violations. Passwords must be provided to the School Information Services Department upon request.

Unacceptable Use

Unless specifically granted in this policy under Principles of Acceptable Use, any non-schoolwork use of the DSS's systems is expressly forbidden. It is not acceptable to use DSS technology resources, including Internet access, for activities unrelated to the mission of the DSS. Some examples of Unacceptable Uses include:

- Activities unrelated to DSS assignments and/or responsibilities.
- Any illegal purpose.
- Transmitting threatening or harassing materials or correspondence.
- Unauthorized distribution of DSS data and information.
- Interfering with or disrupting network users, services or equipment.
- Use for private purposes, whether for-profit or non-profit, such as marketing or business transactions unrelated to DSS duties.
- Any activity related to political causes.
- Advocating religious beliefs or practices contrary to Roman Catholic teaching.
- Private advertising of products or services.
- Any activity meant to foster personal gain.
- Revealing or publicizing proprietary or confidential information.
- Representing personal opinions as those of DSS.
- Uploading or downloading commercial software without prior authorization of the School and/or in violation of its copyright.
- Intentionally interfering with the normal operation of any DSS Internet gateway or access point.
- Sending chain letters or participating in any way in the creation or transmission of unsolicited commercial e-mail ("spam").
- Violating the laws and regulations of the United States or any other nation or any state, city, or other local jurisdiction in any way.
- Deliberately propagating any virus, worm, Trojan horse, trap-door program code, or other code or file designed to disrupt, disable, impair, or otherwise harm either DSS's networks or systems or those of any other individual or entity.
- Using abusive, profane, threatening, racist, sexist, or otherwise objectionable language in either public or private messages.
- Sending, receiving, possessing, or accessing indecent, obscene, or pornographic materials, including child pornography.
- Maintaining, organizing, or participating in non-school-related Web logs ("blogs"), Web journals, "chat rooms", social networking sites (e.g. Facebook, My Space. etc.), or private/personal/ instant messaging.
- Failing to log off any secure, controlled-access computer or other form of electronic data system to which you are assigned; negligently exposing your computer or system to inappropriate access or use.
- Defeating or attempting to defeat security restrictions on DSS systems and applications.

It is never acceptable for students to use DSS technology resources, including Internet access, to transmit threatening, obscene or harassing materials or correspondence, but especially in a shared youth environment or to send, receive, possess, or access indecent, obscene, or pornographic materials, including child pornography. Such uses of DSS technology resources will never be tolerated. When warranted, law enforcement authorities will be notified.

Diocese of San Jose - Drexel School System Schools Reserved Rights

DSS owns the rights to all data and files in any computer, network, or other information system used in the DSS system. System administrators have access to all mail and user access requests and will monitor messages as necessary to assure efficient performance and appropriate use. Messages or information relating to or in support of illegal activities will be reported to the appropriate authorities.

All information stored on, entered into, or transmitted in any way through the School computers, network or information systems, including but not limited to electronic mail messages sent and received using DSS equipment are not private and are subject to viewing, downloading, inspection, release, and archiving by DSS officials at all times. DSS and authorized Information Systems Department personnel have the right, without notice, to inspect any and all files stored in private areas of the network or on individual computers or storage media in order to ensure compliance with policy and state and federal laws. No student may access another student's computer, computer files, or electronic mail messages without prior authorization from either the student or an appropriate DSS official.

- DSS reserves the right to log network use and monitor file server space utilization by students and assumes no responsibility or liability for files deleted due to violation of file server space allotments.
- DSS reserves the right to remove a user account from the network.
- DSS will not be responsible for any damages resulting from the use of its computers, network or information systems. This includes the loss of data resulting from delays, non-deliveries, or service interruptions caused by negligence, errors or omissions. Use of any information obtained is at the user's risk. The School makes no warranties, either express or implied, with regard to software obtained from the Internet.
- DSS reserves the right to change its policies and rules at any time.
- DSS makes no warranties (expressed or implied) with respect to Internet service, and it specifically assumes no responsibilities for:
    - The content of any advice or information received by a student through Internet facilities or any costs or charges incurred as a result of seeking or accepting such advice.
    - Any costs, liabilities or damages caused by the way the student chooses to use the Internet facilities.
    - Any consequence of service interruptions or changes, even if these disruptions arise from circumstances under the control of the School.
- DSS technology resources, including Internet access, are provided on an as is, as available basis.
- Students are individually liable for any and all damages incurred as a result of violating the DSS security policy, copyright, and licensing agreements.

The DSS has licensed the use of certain commercial software application programs for its purposes. Third parties retain the ownership and distribution rights to such software. No user may create, use, or distribute copies of such software that are not in compliance with the license agreements for the software and without express authorization from the DSS.

Enforcement and Violations

This policy is intended to be illustrative of the range of acceptable and unacceptable uses of Internet facilities and is not intended to be exhaustive. Questions about specific uses related to security issues not enumerated in this policy statement and reports of specific unacceptable uses should be directed to the school administrator. Other questions about appropriate use should be directed to the school administrator. DSS will review alleged violations of the Technology Use and Internet Policy on a case-by-case basis.

Violations of the policy will result in disciplinary actions as appropriate, up to and including expulsion from school. Use of DSS resources for illegal activity will lead to disciplinary action, up to and including expulsion and criminal

prosecution. DSS will comply with reasonable requests from law enforcement and regulatory agencies for logs, diaries, archives, or files on individual Internet activities, e-mail use, and/or computer use. Notifications of appropriate agencies, including the Office for the Protection of Children & Vulnerable Adults, Child Protective Services and local law enforcement will take place in all cases where the perceived safety/welfare of children is at risk and as mandated by law.

Breakage and Replacement

Techology provided to students by DSS for educational use remains the property of DSS. Students, and by extension their parent(s)/guardian(s), are directly responsible for the care and treatment of school technology. DSS expects students to protect and care for the iPads and other technology provided to them. Parent(s)/guardian(s) will be invoiced by the Drexel School Site for all incurred damage to issued technology per the fee schedule.

iPad Fee Schedule for the 2018/2019 School Year

Description	Cost
Full Replacement (iPad, Case, Cable, Charger) (Based on DSS's bulk educational rate)	$375
Cracked Screen Repair	$249
Damaged Corners Repair	$225
Lost/Damaged Case Replacement	$35
Lost/Damaged Charger Replacement	$15
Lost Damaged Charge Cable Replacement	$10
Total cost not to exceed full replacement cost above.	

Signature and Consent

By signing below, I acknowledge that I have read and agree to this policy and the associated fee schedule. Please note that both parents/guardians (where applicable) are required to sign this agreement in order for the student to receive issued technology.

Student Name	Student Signature	Date
Parent/Guardian Name	Parent/Guardian Signature	Date
Parent/Guardian Name	Parent/Guardian Signature	Date