DUVAL COUNTY PUBLIC SCHOOLS (DCPS) INFORMATION SECURITY PROGRAM

SUBJECT: ACCEPTABLE USE POLICY (AUP) SCHOOL BOARD POLICY NUMBER: 8.71

PURPOSE/SCOPE: This establishes the School Board Policy for Acceptable Use of Information Resources and applies to all users of DCPS information resources. Individuals using information resources belonging to DCPS must act in a legal, ethical, responsible, and secure manner, with respect for the rights of others.

The primary purpose of the DCPS network is to assist in preparing students for success in life and work in the 21st century. Computer and/or Electronic networks provide the ability to share educational and research resources from around the world. These resources include but are not limited to, access to instructional/business applications, interactive collaboration between teachers, students and other users, document sharing, and communications of all forms with people from around the world.

Access to computers, computing systems and networks owned by the School Board is a privilege which imposes certain responsibilities and obligations, and which is granted subject to DCPS policies and procedures, Code of Student Conduct, the Code of Ethics of the Education Profession in the State of Florida, and governing laws. These procedures set forth the principles that govern appropriate use of information resources, and is intended to promote the efficient, ethical and lawful use of these resources.

1. DEFINITIONS

1.1. Access: The right to enter or make use of a computer system. To approach, view, instruct, communicate with, store data in, retrieve data from, or otherwise make use of computers or information resources.
1.2. Administrative Access: Enhanced privilege level that allows the user to perform administration of the system.
1.3. Account: A set of privileges for authorization to system access, which are associated with a user id.
1.4. Information Resources: The procedures, equipment, facilities, software and data that are designed, built, operated and maintained to collect, record, process, store, retrieve, display and transmit information.
1.5. Audit Trail: In computer security systems, a chronological record of system resource usage. This includes user login, file access, other various activities, and whether any actual or attempted security violations occurred, legitimate, and unauthorized.
1.6. Information Custodians: Individuals who maintain or administer information resources on behalf of Information Owners. They are guardians or caretakers who are charged with the resource owner's requirements for processing, telecommunications, protection controls, and output distribution for the resource.
1.7. Information Owners: The individuals ultimately responsible for information resources, and are generally Directors or designated senior managers. The initial

owner is the individual who creates, or initiates the creation or storage of, information. Once information is created, stored or transmitted, the individual's respective DCPS business unit becomes the Owner, with the Director of that unit taking official responsibility.
1.8. Information Security Manager (ISM): Directs the organization's day-to-day management of its Information Systems Security Program. This individual is also responsible for coordinating all security-related interactions among organizational elements involved in the Information Systems Security Program.
1.9. Information Users: Individuals who use or have access to DCPS's information resources, including employees, vendors, and visitors.
1.10. Password: Any secret string of characters which serves as authentication of a person's identity (personal password), or which may be used to grant or deny access to private or shared data (access password).
1.11. Personal Use Activity: that is conducted for purposes other than accomplishing official or otherwise authorized activity.
1.12. System Administrator: A designated individual who has special privileges to maintain the operation of a computer application or system.

2. PROCEDURES & GUIDELINES

2.1.1. Employees shall use DCPS provided information resources primarily for DCPS related business in accordance with their job functions and responsibilities. Employees are permitted limited personal use of information resources if the use does not result in a loss of associate productivity, interfere with official duties or business, and involves minimal additional expense to the School Board. Unauthorized or improper use of information resources may result in loss of use or limitations on use of those resources or disciplinary action.

2.1.2. Employees are required to comply with the Districts Information Security Program and its procedures. Updated procedures will be sent to all employees using the District's e-mail system.

2.1.3. Pursuant to the Children's Internet Protection Act (CIPA), DCPS uses filtering software to screen Internet sites for offensive material. DCPS acknowledges the fact that inappropriate materials exist on the Internet and will do everything it can to actively avoid them. To that extent, DCPS has implemented technology protection measures that filter Internet access to block visual displays that are obscene, pornographic, or harmful to minors. The Internet is a collection of thousands of worldwide networks and organizations that contain millions of pages of information. Users are cautioned that many of these pages contain offensive, sexually explicit, and inappropriate material. In general, it is difficult to avoid at least some contact with this material while using the Internet. Even innocuous search requests may lead to sites with highly offensive content. Additionally, having an e-mail address on the Internet may lead to receipt of unsolicited e-mail containing offensive content. Users accessing the Internet do so at their own risk. No filtering software is one hundred percent effective. In the event that the filtering software is unsuccessful

and children and staff gain access to inappropriate and/or harmful material, the District will not be liable.

2.1.4. DCPS makes no guarantee that the functions or the services provided by or through the District's network will be error-free or without defect. The District will not be responsible for any damage suffered, including but not limited to, loss of data or interruptions of service. Users are responsible for making a back-up copy of crucial files. The District is not responsible for the accuracy or quality of the information obtained through or stored on the network. The District will not be responsible for financial obligations arising through the unauthorized use of the network as the result of intentional misuse.

2.1.5. Software development, modifications, and documents of such become the intellectual property of the District when developed during work hours or used as part of their normal duties or instructional material in the classroom. Ownership, including all intellectual property rights, is and remains with DCPS.

2.1.6. The District is not responsible for the accuracy or quality of information obtained through the network. All users need to consider the source of any information they obtain through the network, and evaluate the accuracy of the information.

2.1.7. All software and equipment configurations installed on DCPS computers are owned by DCPS. All files and data stored on District equipment and back-up copies are considered to be the property of the District. The District retains the right to remove from its network any material it views as unnecessary, offensive or potentially illegal.

2.1.8. Use of any information obtained via the Internet is at the user's own risk. The District will not be responsible for any damages a user may incur. This includes, but is not limited to, loss of data resulting from delays, non-deliveries, missed-deliveries, or service interruptions caused by negligence, errors, or omissions.

2.1.9. Access to the Internet from the district network as a tool for learning will be automatic. Parents must notify the school in writing if they do not want their child to access the Internet. See the Code of Student Conduct for details and opt-out form.

2.1.10. Any student e-mail access must be approved by the Principal, Chief Technology Officer (CTO), and Information Security Manager (ISM).

2.1.11. Employees must maintain professional boundaries between themselves and students. Employees will not solicit or engage in inappropriate communications with students verbally, in writing, or electronically regardless of the age of that student. Employees will not engage in any direct electronic communications with students, parents, supervisors, or co-workers whether by e-mail, instant messaging, or other

digital media that will adversely affects the employee's ability to perform his or her job.

2.1.12. DCPS employees are required to use their district assigned e-mail address for all electronic communications to DCPS parents and students. Using personal e-mail to communicate with DCPS parents and students is prohibited.

2.1.13. Employees are reminded that during non-working hours they are representatives of DCPS and should behave in a manner that does not bring disrespect or discredit the education profession. Unless engaging an officially sanctioned District activity, employees should clearly specify that any opinions or statements are the employee's and do not reflect the views of the District. Employees are prohibited from using officially sanctioned school district logos, school mascots, and other official symbols unless authorized to do so in advance.

2.1.14. When using School Board information resources, users are expected to:

2.1.14.1. Act responsibly so as to ensure the ethical use of DCPS information resources.

2.1.14.2. Acknowledge the right of DCPS to restrict or rescind computing privileges at any time.

2.1.14.3. Use security measures to protect the confidentiality, integrity, availability of information, data, and systems.
2.1.14.4. Act professionally and to refrain from using School Board information resources for activities that are inappropriate.
2.1.14.5. Respect all pertinent licenses, copyrights, contracts, and other restricted or proprietary information.
2.1.14.6. Use good judgment in accessing the Internet. Each use of the Internet should be able to withstand public scrutiny without embarrassment to DCPS or the School Board.
2.1.14.7. Safeguard their user IDs and passwords, and use them only as authorized. Any actions taken under an assigned identification (e.g., user ID) are the responsibility of the user.
2.1.14.8. Respect School Board property.
2.1.14.9. Access and appropriately use and safeguard data to which access has been granted.
2.1.14.10. Exercise good judgment regarding the reasonableness of personal use.
2.1.14.11. Use information resources efficiently.
2.1.14.12. Comply with the Family Educational Rights and Privacy Act (FERPA) and state and federal laws governing the confidentiality of employee and student records. Personally identifiable student information is confidential under Florida law and similar federal laws.

2.1.15. The following activities are strictly prohibited when using DCPS information resources:

2.1.15.1. Intentionally corrupting, misusing, or stealing software or any other computing resource.
2.1.15.2. Accessing DCPS systems that are not necessary for the performance of the associate's duties, including student and employee records.
2.1.15.3. Performing functions that are not related to the employee's job responsibilities on systems that they are otherwise authorized to access.
2.1.15.4. Making unauthorized changes to DCPS computer resources, including installation of unapproved software or interfering with security measures (such as audit trail logs and anti-virus software).
2.1.15.5. Copying DCPS proprietary software or business data for personal or other non-School Board use.
2.1.15.6. Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which DCPS or the end user does not have an active license.
2.1.15.7. Disseminating trade secrets or business confidential information, except as permitted by law or regulation.
2.1.15.8. Transmitting, storing, or processing classified data except as authorized and in accordance with the DCPS Information Systems Security Plan.
2.1.15.9. Unauthorized access to other computer systems using DCPS information resources.
2.1.15.10. Accessing information resources, data, equipment, or facilities in violation of any restriction on use, such as Peer-to-Peer.
2.1.15.11. Using School Board computing resources for personal or private financial gain.
2.1.15.12. Using another person's computer account, with or without their permission.
2.1.15.13. Implementing any computer systems without authorization from the CTO or designee.
2.1.15.14. Knowingly, without written authorization, executing a program that may hamper normal DCPS computing activities, such as Peer-to-Peer.
2.1.15.15. Adding unapproved components or devices to DCPS equipment without approval from the CTO or designee.
2.1.15.16. Attaching or assisting others in attaching non-DCPS equipment to the DCPS network without first obtaining approval from the CTO or designee.
2.1.15.17. Knowingly introducing malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).
2.1.15.18. Revealing account passwords to others or allowing the use of one's account or DCPS equipment by others, including family, friends and other household members. Users are ultimately responsible for the activity that occurs under their account and their assigned equipment.
2.1.15.19. Knowingly allowing a student to access their assigned laptop or administrative desktop. Students are only permitted to access student designated computers and should never access or logon to a teacher or administrative computer.

2.1.15.20. Revealing system passwords (e.g. DCPS system passwords, database passwords, etc.) to anyone who is not specifically authorized to use them.
2.1.15.21. Exporting software, technical information, encryption software, or technology, in violation of international or regional export control laws.
2.1.15.22. Effecting security breaches or disruptions of network communication.
2.1.15.23. Unauthorized security scanning, network monitoring, or data interception that is not part of the associate's regular job duties and approved by the ISM.
2.1.15.24. Using District equipment or personal equipment while on DCPS property to connect to any wireless network not provided by DCPS without authorization from the ISM is prohibited and may be illegal. External signals will not provide content filtering and access to private networks may be illegal.
2.1.15.25. Circumventing any DCPS information security measures.
2.1.15.26. Use of encryption software or hardware that has not been authorized by ISM.
2.1.15.27. Interfering with or denying service to other information resource users, such as using Peer-to-Peer.
2.1.15.28. Sending unsolicited e-mail messages (spam).
2.1.15.29. Any form of harassment via e-mail, telephone, pager, IRC, SMS, or other communication method, whether through language, frequency, or size of messages.
2.1.15.30. Creating or forwarding "chain-letters", "Ponzi" or other "pyramid" schemes of any type.
2.1.15.31. Engaging in any unauthorized fund-raising activity, participating in any lobbying activity, or engaging in any partisan political activity without specific permission from DCPS.
2.1.15.32. Posting agency information to external news groups, bulletin School Boards or other public forums without authority, or conducting any activity that could create the perception that communication was made in one's official capacity as a School Board associate, unless appropriate approval has been obtained.
2.1.15.33. Any personal use that could cause congestion, delay, or disruption of service to any School Board system or equipment.
2.1.15.34. Using School Board office equipment or information resources for activities that are illegal, inappropriate, or offensive to fellow employees or the public. This includes, but is not limited to, materials related to
2.1.15.34.1. Sexually explicit or sexually oriented content
2.1.15.34.2. Offensive comments related to race, color, religion, gender, age, marital status, disability, sexual orientation, political or religious beliefs, national or ethnic origin, veteran status, or any other distinguishing physical or personality characteristics.
2.1.15.34.3. Anything that is in violation of sexual harassment or hostile workplace laws
2.1.15.34.4. Making fraudulent offers of products, items, or services
2.1.15.34.5. Gambling
2.1.15.34.6. Illegal weapons or terrorist activities
2.1.15.34.7. Planning or commission of any crime

2.1.15.35. Forging or misrepresenting one's identity

2.1.16.1. Users shall have no expectation of privacy while utilizing the DCPS network, equipment or information resources. This extends to any hardware attached to the DCPS network, even if such equipment or computer is not owned by DCPS. Any equipment attached to the DCPS network or on DCPS property is subject to be scanned, monitored, captured, and physically and electronically searched. This includes the right to confiscate any equipment if required as part of an investigation even if that equipment is not owned by the District. The District may disclose any data collected to Administration, internal and external law enforcement agencies.

2.1.16.2. Users agree to be governed by acceptable usage policies and to have their usage audited. By using School Board office equipment, employees imply their consent to disclosing the contents of any files or information maintained or passed-through School Board office equipment.

2.1.16.3. To the extent that employees wish that their private activities remain private, they should avoid using agency office equipment such as their computer, the Internet, or e-mail, for those activities.

2.1.16.4. Auditing procedures will be implemented to ensure compliance with DCPS security policies.

2.1.16.5. System administrators have the ability to audit network logs, employ monitoring tools, and perform periodic checks for misuse.

2.1.16.6. Accessing the Internet through District equipment is a privilege, not a right, and inappropriate use, including violation of this policy may result in limited, restricted or complete loss of the privilege.

2.1.16.7. Any user account may be closed, suspended or revoked at any time it is determined an account user or holder has used the network in an inappropriate or unacceptable manner in violation of this or any other applicable District policy.

2.1.16.8. Files and e-mail are protected by security permissions and only approved administrators can access or change permissions. Requests from supervisors to access subordinates' files and e-mail must be approved by the CTO or their designee. Unless otherwise stated, submission of a trouble call or ticket will authorize technicians to access individuals' permissions (e-mail or hard drive) as it may be necessary for technical support personnel to review the content of an individual employee's communications during the course of problem resolution. Technical support personnel are not authorized to review the content of an individual employee's communications out of personal curiosity or at the behest of individuals who have not gone through proper approval channels.

2.1.16.9. Employees and contractors will electronically or physically sign an agreement to comply with the DCPS AUP.

2.1.16.10. Usage of DCPS IT resources for illegal purposes may be reported to appropriate authorities.

2.2. ROLES & RESPONSIBILITIES

2.2.1. Information Users are responsible for:

2.2.1.1. Using information resources responsibly and in compliance with all DCPS information security policies and guidelines.
2.2.1.2. Reporting any suspected inappropriate use of information resources to their Principal, supervisor, or the ISM.
2.2.2. Supervisors are responsible for:
2.2.2.1. Ensuring that their personnel understand DCPS protocol regarding acceptable usage of information resources.
2.2.2.2. Monitor their employees' use of information resources. (Report any suspicious activity to the ISM)
2.2.3. Information Owners are responsible for implementing measures to protect their resources against inappropriate use.
2.2.4. Information Custodians are responsible for assisting information owners with implementing measures to protect their resources against inappropriate use.
2.2.5. Information Security Manager (ISM) is responsible for auditing usage of the DCPS information resources to ensure compliance with policies and guidelines.

2.3. ENFORCEMENT

Unauthorized or improper use of School Board information resources could result in loss or limitations of use of these resources, as well as disciplinary and/or legal action, including termination of employment, termination of contract, or referral for criminal prosecution.

The Duval County Public Schools Acceptable Use Policy Agreement Form:

The following form must be read and signed physically or electronically by anyone using district computers or network resources. By signing (or electronically accepting) this form, agreement is made to the terms in the Duval County Public Schools Acceptable Use Policy. In accordance with the Electronic and Communications Privacy Act of 1986, (18 US Section 2510), users are hereby notified that there are no facilities provided by Duval County Public Schools for sending or receiving private or confidential electronic communications. All messages will be determined to be readily accessible to the general public. Duval County Public Schools shall be held harmless against any and all claims arising from said use.

I have read, understand, and agree to the Duval County Public Schools (DCPS) Acceptable Use Policy. I agree to follow the rules contained in these documents. I

understand that if I violate the rules my account can be restricted or terminated, my access to computers revoked, and I may face other disciplinary measures. I hereby release the Duval County Public Schools (DCPS), its personnel and any institutions with which it is affiliated, from any and all claims and damages of any nature arising from my use of, or inability to use, the district's network and computer systems, including, but not limited to claims that may arise from the unauthorized use of the system. If I work with students, I have read the Code of Student Conduct and agree to enforce them with students.