

Douglas Public School District Internet Safety & Acceptable Use Policy

Revised by Director of Technology/Technology Vertical Curriculum Team: April 2008

Introduction

The purpose of the Douglas Public School's Internet Safety & Acceptable Use Policy is to provide guidelines for using computer technology while complying with the Children's Internet Protection Act and the Neighborhood Children's Internet Protection Act. Throughout the course of this document, both of the protection acts will be referred to jointly as CIPA. The Internet Safety & Acceptable Use Policy will be referred to as the AUP.

The Douglas Public School District offers access to computer technologies, the Internet, and electronic communication to students, employees, and patrons, provided that these resources are used in a responsible, legal and ethical manner to enhance educational learning.

The term "user" includes - but is not limited to - students, teachers, staff members, administrators, and members of the community who use the District's computer resources.

It is the policy of the Douglas Public School District 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 (CIPA) [Pub. L. No. 106-554 and 47 USC 254(h)].

"Inappropriate Material", materials "harmful to minors" and the technology protection measure will be further defined within this AUP in section *B - Access to Inappropriate Material*. Prevention of unauthorized access and other unlawful online activity will be further defined within this AUP in section *C - Network Usage - Part 4 - Illegal Activities*. Prevention of unauthorized online disclosure, use, or dissemination of personal identification information of minors will be further defined within this AUP in section *C - Network Usage - Part 1 - Personal Safety, Security and Privacy*.

Computer Technologies and Internet Access

Access to computer technology resources and the Internet are **privileges, not rights** offered to users at the discretion of the school and District administrators. Only authorized users may log on using the District's computer technologies and/or Internet access connections.

Any technology connection physically on district premises, remote connections (RAS,

VPN, etc.) or wireless technologies which utilize district resources and/or an Internet connection are subject to the policies stated within this AUP and CIPA.

A. Educational Purpose

1. Computer technology resources and Internet access have been implemented for the purpose of educational enhancement. The term "educational enhancement" includes support of classroom activities, assignments, curriculum development, enrichment, and career development, as determined by the classroom teacher or administration.
2. The computer technology resources and Internet access have not been established as a public access service or a public forum. The District has the right to place reasonable regulations on the material accessed or posted through these resources.
3. The Internet may not be used for non-authorized commercial purposes; therefore, non-authorized products or services must not be offered, provided, or purchased through the Internet.
4. Computer technology and/or the Internet may not be used for political lobbying. However, resources to communicate with elected representatives and to express opinions on political issues may be utilized.
5. Computer technology and/or the Internet may not be used for any unlawful or criminal activities, including violation of any criminal or civil laws or regulations.

B. Access to Inappropriate Material

1. Technology Protection Measures

- a. To the extent practical, technology protection measures shall be used to block or filter the Internet, other forms of electronic communications, and access to inappropriate information. Specifically, as required by the Children's Internet Protection Act (CIPA), blocking shall be applied to:
 - i. visual depictions of material deemed obscene as the term is defined in section 1460 of title 18, US Code
 - ii. child pornography, as the term is defined in section 2256 of title 18, US Code
 - iii. Material deemed "harmful to minors"
 1. Taken as a whole and with respect to minors, appeals to a prurient interest in nudity, sex, or excretion;
 2. 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 (refer to section 2246 of title 18 US code), or a lewd exhibition of the genitals; and

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

- b. In addition to blocking of materials that are “harmful to minors” as described above and within CIPA, the District will enable blocking protection measures for additional web sites and materials that are not within the District’s educational curriculum. Blocking protection shall be applied to materials that are illegal, promote violence, profanity, intolerance or violates District/school policies. This may include any site that does not contribute to educational pursuits.
- c. Blocking of additional websites will be maintained by the Technology Director.
- d. The technology protection measures may be temporarily bypassed when requested by staff only for bona fide research or other lawful purposes. Only the District technology administrators will have the authority to disable filters for adult bona fide research.
- e. District administrators may request proof of age identification for users before disabling filters for “adult bona fide research.”
- f. Inadvertently blocked web sites that conform to the policies stated in this AUP and CIPA may be unblocked by the technology administrators after a thorough review by school and District administration for educationally suitable, age appropriate content.

2. **User Policies Concerning Access to Inappropriate Material**

- a. Computer technologies and/or the Internet may not be used to access material that is profane, obscene, pornographic, advocates illegal acts, advocates violence or discrimination towards other people.
- b. If a user mistakenly accesses inappropriate information, he/she should immediately notify the technology administrators and appropriate faculty members in order to be protected against a claim of intentional policy violation.
- c. Parent(s) or guardian(s) of students should provide guidance and instruction to their children regarding material that would be considered inappropriate and inconsistent with family, religious or ethnic values. Any web site or e-mail message that is inappropriate or inconsistent with these values should be promptly disclosed to faculty or school administration.

C. Network Usage

To the extent practical, steps shall be taken to promote the safety and security of users of the Douglas Public School District's computer technologies and Internet access when using electronic mail, chat rooms, instant messaging, and other forms of direct electronic communications. Internet safety is taught in all technology classes and safe use of technology is reinforced by all teachers when using technology in the classroom.

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.

1. Personal Safety, Security and Privacy

- a. Users will not disclose, use and disseminate personal identification information regarding minors. Personal identification information includes: address, telephone, {photograph, and school records.}
- b. Users will not post personal information about another person. This includes physical or sexual harassment or cyber-bullying.
- c. Users will not agree to meet with someone met via the Internet.
- d. Users will promptly disclose to faculty or school administration any Web site or E-mail message that is inappropriate or makes them feel uncomfortable.
- e. Passwords are not transferable. A user account is limited to use by the person to whom it is issued. Use of another person's account or providing unauthorized access to one's account constitutes grounds for termination or restriction of access privileges. Users should take precautions to keep their passwords confidential.

2. E-mail & Electronic Communications

When using E-mail, chat rooms or other forms of electronic communication; users should be aware that their messages are the property of the Douglas Public School District. All messages are archived. They may also be copied, printed or forwarded by recipients. E-mail users should use professionalism and maturity in composing or distributing messages. Under Massachusetts law, all electronic messages received or sent by school employees are considered public records and are subject to the requirements of the Public Records Law. M.G.L. Chapter 66.

The technology administrators will assign E-mail accounts to employees at the request of school administration. Student E-mail accounts will be allowed only if an account is needed to perform communications for a

currently enrolled course. Faculty members offering courses that require student E-mail addresses must provide the technology administrators with a formal request for an account.

Students must request consent from faculty before each usage of E-mail, chat rooms, blogs, instant messengers, or other forms of electronic communications. **Students are not to use electronic communications unsupervised.**

Any user who observes another user abusing, inappropriately using, or failing to follow any of these guidelines shall report this to a teacher or an administrator.

3. **Use of Personal Computer Technology**

- a. Students may not use any personal accounts to communicate on the Internet unless the accounts have been assigned by District faculty or the technology administrators.
- b. Students may only use District-approved computer resources to access the District's network or Internet connection(s). Students must request approval for each connection time when the computer equipment being connected to the District's resources is not owned or leased by the District. Approval will be determined by the Technology Director. This equipment must be used in accordance with network security policies established by the District technology administrators.
- c. Employees, students, and visitors who wish to use personal equipment or accounts to communicate through the district's Internet access must also comply with the policies stated within this AUP, CIPA and any other network security policies established by the District technology administrators. This includes - but is not limited to - cell phones, personal music devices, handheld computing devices, and other evolving technologies.
- d. The use of any recording devices to record or broadcast the activities of any person on school property without the express knowledge and consent of the subject is strictly prohibited. This prohibition does not apply to performances, sporting events, and other publicly attended events.

4. **Illegal Activities**

- a. **Hacking** - Users will not attempt to gain unauthorized access or go beyond their authorized access when connecting to technology resources available in the Douglas Public School District or to any other computer system through the use of the Internet so called "hacking".
- b. **Eavesdropping / Wiretapping "sniffing"** - Users will not listen to or

decrypt any electronic communication that is not meant for their attention.

- c. **Spoofing** – Users will not attempt to use the computer technologies to illicitly impersonate or assume the name of another computer system.
 - d. **Port Scanning** – Users will not generate an attack on any host for the purpose of finding vulnerabilities in active ports.
 - e. **Viruses** - Users will not make deliberate attempts to disrupt the computer system or destroy data by uploading, downloading or spreading computer viruses by any other means. The District has implemented virus protection software; users must not uninstall or disable this software. District virus protection procedures must be followed in order to prevent the inadvertent spread of computer viruses.
 - f. **Denial of Service (DOS)** – Users will not generate an attack by monopolizing system resources so that other users can not gain access to technology resources and the Internet.
 - g. **Other Illegal/Non-authorized Activities** - Users will not use the District's computer resources to engage in any other illegal/non-authorized acts such as - but not limited to - arranging for a drug sale or the purchase of alcohol, entering into criminal gang activity, threatening the safety of a person, and gambling.
5. **System Security**
- a. Users must immediately notify a technology or school administrator if they have identified a possible security problem. **USERS MUST NOT** intentionally search for a security problem because this activity may be construed as an illegal attempt to gain access.
6. **Dial-In Access**
- a. VPN, RAS or any other dial-in means is restricted to Douglas Public School District employees and authorized students for the purpose of distance learning.

D. Inappropriate Language

1. Restrictions against inappropriate language apply to public messages, private messages, and material posted on Web pages.
2. Users must not use obscene, profane, lewd, vulgar, rude, inflammatory, threatening, or disrespectful language.
3. Users must not post information that could cause damage or a danger of disruption.
4. Users must not engage in personal attacks, including prejudicial or discriminatory attacks.

5. Users must not harass others. Harassment is persistently acting in a manner that distresses or annoys another person. **If a user is told by another person to stop sending him/her messages, the user must stop!**
6. Users will not knowingly or recklessly post false or defamatory information about a person or organization.

E. Supervision and Monitoring

1. It shall be the responsibility of all members of the Douglas Public School District to supervise and monitor usage by a minor of District computer technologies and the access to the Internet through District resources in accordance with this policy and CIPA.
2. In addition to supervising and monitoring usage by a minor, the District will continue to monitor District computer and Internet usage of students until the student is no longer enrolled in the District.
3. The technology administrators may install and enable devices for the purpose of routinely monitoring network resources and activities.

F. Data and System Resource Limitations

1. Users must not change copy, delete, read or otherwise access data or software programs without the permission of the owner or the technology administrators.
2. Users must not download or save files that will consume large amounts of data resources.
3. Users must not post chain letters or engage in "spamming". Spamming is sending or replying to irrelevant or inappropriate messages to a large number of people which may lead to the disruption of services.
4. Users must not modify or change computer settings which may affect the functionality or navigation of software when accessed by other users.
5. Users must not install software on any computer system without permission of the technology administrators. Software installations must conform to the said vendor's copyright agreement. Software licensing agreements must be provided to the technology administrators.
6. Users may neither install nor have access to any unauthorized executable files.
7. Users must not vandalize or intentionally damage any computer technology.
8. Users must not remove computer technologies without the consent of the technology director and school or District administration. This includes hardware, software and data.

G. Plagiarism and Copyright Infringement

1. The user must not plagiarize works found on the Internet. Plagiarism is taking the ideas or writings of others and presenting them without giving proper credit.
2. The user must respect the rights of copyright owners. Copyright infringement occurs when a user inappropriately reproduces a work that is protected by a copyright. For example, copyrights may apply to software, documentation, music, video, and graphics. If a work contains language that specifies appropriate use of that work, the user must follow the expressed requirements. If a user is unsure about whether or not he/she may use a particular work, permission must be requested from the copyright owner.
3. Any and all sources used, including multimedia, must be cited in the proper format.

H. User Rights

1. Free Speech

A user's right to free speech applies to his/her Internet communications. Use of technology resources and the Internet from the Douglas Public School District is considered a limited forum, similar to any school publication, and therefore the District may restrict a user's free speech for valid educational purposes.

2. Intentional Violations

The Douglas Public School District is aware that policy violations may occur when a user is involuntarily routed to sites that contain inappropriate material. Therefore, disciplinary action shall only result when the policy is willfully and intentionally violated. The Douglas Public School District reserves the right to discipline any user for violations of this policy when it is apparent that the user knew, or should have known, that a policy violation was likely to occur as a result of the actions or inactions of the user in question.

3. Privacy, Search and Seizure

- a. The District retains ownership and control of its technology resources. Accordingly, all users possess no rights to privacy in regard to their use of District technology resources, including – but not limited to – District computers, the computer network, the electronic mail system (e-mail), the Douglas website, and Internet access. The District does not guarantee - and users should not expect - confidentiality, privacy, security, or ownership of the content of any information accessed, sent, received,

created or stored, using technology resources, with the exception of databases storing confidential information. All users should be aware that electronic communications and other information sent via the Internet are accessible by third parties, specifically the Internet Service Provider.

- b. An individual search will be conducted if there is reasonable suspicion that a user has violated this policy, the disciplinary code, or the law. The investigation will be reasonable and related to the suspected violation.

4. **Due Process**

- a. The District will cooperate fully with local, state, or federal officials in any investigation related to any illegal activities conducted through the District's technology resources and the Internet.
- b. In the event there is a claim that a user has violated this policy and/or the disciplinary code in using the technology resources and/or Internet, he/she will be provided with a written notice of the suspected violation and an opportunity to present an explanation before an administrator.
- c. If the violation also involves other violations of the disciplinary code, it will be handled in a manner described in the student or faculty handbooks. Additional restrictions may be placed on a user's use of the technology resources and/or Internet, which may include cancellation of privileges.

5. **Disciplinary Action**

Student violation of this policy and/or other Douglas Public School District policies shall result in one or more of the following consequences:

- a. Restriction, suspension or revocation of access privileges;
- b. Removal from a class activity;
- c. Removal from a course;
- d. Removal from an extracurricular activity;
- e. Detention, suspension or expulsion;
- f. Referral to the appropriate legal authorities for possible criminal prosecution;
- g. Civil liability

Staff violations of this policy shall be addressed by the District Administration.

I. **Limitation of Liability**

The District makes no guarantee that the functions or the services provided by or through the computer technology resources and/or Internet will be error-free or

without defect. The District will not be responsible for any damage a user may suffer - including but not limited to - loss of data or interruptions of service. The District is not responsible for the accuracy or quality of the information obtained through or stored on the system. The District will not be responsible for financial obligations arising through the unauthorized use of the system.

J. Adoption

This Internet Safety Policy was adopted by the Douglas School Committee on: 06/26/2002. In compliance with CIPA, a public meeting was held on 05/22/2002, following normal public notice. The policy was revised by the Director of Technology/Technology Vertical Curriculum Team in April 2008, and brought before the Douglas School Committee on May 7, 2008, and again on May 21, 2008. This updated policy was approved by School Committee on June 18, 2008.

K. Signed Agreement

All employees and students must return a signed agreement page. Students must return the signed agreement page to their homeroom teacher within three days of the school year's start date or time of enrollment.

L. Glossary

Cite – To attribute the source of information

Copyright infringement – Use of copyrighted work without permission or in violation of copyright law.

Cyberbullying – Use of technology such as e-mail, chat rooms, blogs, etc., to harass someone.

Executable file – File that runs or starts a program

Plagiarism – Presenting the work or ideas of others as one's own.

RAS – Remote Access Server

VPN – Virtual Private Network

First Reading: February 1, 2012

Second Reading: February 15, 2012

Third Reading: March 7, 2012

Adopted March 7, 2012

Douglas Public Schools Chromebook Use Agreement

1.0 General Information

The policies, procedures and information within this document apply to all student Chromebooks used in the Douglas Public Schools, including any other device considered by the Administration to come under this policy. Teachers may set additional requirements for use in their classroom.

1.1 Receiving the Chromebook

The Chromebooks will be distributed during class. Students will be allowed to take the Chromebooks home, once both the parent and the student have signed and returned the Chromebook Use Agreement.

1.2 Returning the Chromebook

Chromebooks, with accessories, will be returned to the Douglas Public Schools during the final week of school. If a student transfers out of the Douglas School District during the school year, the Chromebook will be returned at that time. Students who withdraw, are suspended or expelled, or terminate enrollment at Douglas Public Schools for any other reason must return their individual school Chromebook with accessories on the date of termination.

2.0 CARE OF THE CHROMEBOOK

The Chromebook is school property and all users will follow the Douglas Public Schools Acceptable Use Policy in utilizing this technology resource. Students are responsible for the general care of the Chromebook they have been issued by the school. Chromebooks that are broken or that fail to work properly must be taken as soon as possible to the Douglas Technology Department for evaluation.

2.1 General Precautions

- Only a clean, soft cloth must be used to clean the screen; no cleansers of any type should be used.
- Cords and cables must be inserted carefully into the Chromebook to prevent damage.
- Chromebooks must remain free of any writing, drawing, stickers, or labels that are not the property of the Douglas Public School District.
- Chromebooks must never be left in an unlocked locker or any unsupervised area.
- Food and drinks must be kept away from the Chromebook.

2.2 Carrying Chromebooks

- Care should be exercised when carrying the Chromebook in backpacks that hold other objects (such as folders and textbooks), to avoid placing too much pressure and weight on the Chromebook screen.
- Books should not be placed on top of the Chromebook when being carried.

2.3 Screen Care

The Chromebook screen can be damaged if subjected to rough treatment. The screen is particularly susceptible to damage from excessive pressure.

- Do not lean on the top of the Chromebook.
- Do not place anything near the Chromebook that could put pressure on the screen.
- Clean the screen with a soft, dry cloth or anti-static cloth.
- Do not “bump” the Chromebook against lockers, walls, car doors, floors, etc., as doing so will eventually break the screen.

3.0 USING THE CHROMEBOOK AT SCHOOL

Chromebooks are intended for use at school each day. In addition to teacher expectations for Chromebook use, school messages, announcements, calendars and schedules may be accessed using the Chromebook. Students must be responsible to bring their Chromebook to all classes, unless specifically instructed not to do so by their teacher.

3.1 Chromebook Undergoing Repair

Loaner Chromebooks may be issued to students when they leave their Chromebooks for repair in the Technology Department. Requests for loaner Chromebooks will be filled, based on availability.

3.2 Screen Savers/Background photos

Inappropriate media may not be used as a screensaver or background photo. Inappropriate media includes but is not limited to the presence of guns, weapons, pornographic materials, inappropriate language, alcohol, drug, gang related symbols or pictures and will result in disciplinary actions. Passwords are not to be used.

3.3 Sound, Music, Games, or Programs

Sound must be muted at all times unless permission is obtained from the teacher for instructional purposes. Internet Games are not allowed on the Chromebooks. Game apps may only be installed for educational purposes. All software/Apps must be district provided or approved.

3.4 Printing

Printing will be available with the Chromebook on a limited basis. Students should talk to their teachers about which printer to use. Students will be given information and instruction on printing when using the Chromebook at school.

4. MANAGING YOUR FILES & SAVING YOUR WORK

4.1 Saving to the Chromebook/Home Directory

Students may save work directly on the Chromebook. Storage of files will be available online using Google Drive through the school's Google Drive domain. Students may also e-mail documents to themselves and/or their teacher for storage on a District server. Limited storage space will be available on the Chromebook—but it will not be backed up in case of re-imaging. It is the student's responsibility to ensure that work is not lost, due to mechanical failure or accidental deletion.

4.2 Network Connectivity

The Douglas School District makes no guarantee that their network will be up and running 100% of the time. In the rare case that the network is down, the District will not be responsible for lost or missing data.

5. SOFTWARE ON CHROMEBOOKS

5.1 Originally Installed Software

Software is not installed directly on Chromebooks. The Chromebook runs mostly web based software.

5.2 Software Upgrades

The Chromebook updates its operating system and software automatically. It is not necessary for the user to run updates.

6. ACCEPTABLE USE

6.1 Statement of Responsibility

The use of the network is a privilege. Users are responsible for what they say and do on the network. Communication with thousands of others is quick and easy. Therefore, it is crucial for the user to stop and think before communicating, and to show respect for other people and for their ideas.

Keeping the network running efficiently is beneficial for all users. Each user must take responsibility for keeping down costs and avoiding system disruption. Excessive streaming of videos or music should be avoided unless directed to do so by a teacher for educational purposes.

Network administrators will make reasonable efforts to maintain reliable service. They cannot, however, absolutely guarantee that the system will always be available or operating correctly. Student users should assume that none of their data is private or confidential. Any communication or data may be subject to review by network or school administration.

Internet access is available on every computer with network access in the Douglas Public Schools. Users must adhere to the Douglas Public Schools' network rules, guidelines, and procedures when connected to other networks.

6.2 Parent/Guardian Responsibilities

Parents are encouraged to speak with their children about safe usage of the Internet, including guidelines to follow in order to ensure proper usage. As with any use of media, the potential exists for misuse. It is important that students, educators, and parents all work together to ensure that students practice good digital citizenship.

6.3 School Responsibilities

- Provide Internet and Email access.
- Provide Internet Blocking of inappropriate materials to the greatest extent possible.
- Provide network data storage areas. These will be treated similar to school lockers. The District reserves the right to review, monitor, and restrict information stored on or transmitted via district-owned equipment, and to investigate the inappropriate use of resources.
- Provide staff guidance to aid students in proper technology usage.

6.4 Students Responsibilities:

- Use computers/devices in a responsible and ethical manner.
- Obey school rules concerning behavior and communication that apply to network use, in accordance with the **Douglas Public Schools Acceptable Use Policy**. This policy is available online and in the student handbooks and must be signed by students and their parents each year as part of the student handbook.
- Use all technology resources in an appropriate manner so as to not damage school equipment through negligence, errors or omissions - potentially causing loss of data resulting from delays, non-deliveries, mis-deliveries, or service interruptions.
- Use of any information obtained via the Douglas School District's designated Internet System is at the user's own risk. The District is not responsible for the accuracy or quality of information obtained on the Internet through utilizing the District's services.
- Cooperate with the Douglas Public Schools in protecting the computer system and devices by promptly notifying an adult about any security problems encountered.
- Monitor account activity.
- Turn off and secure the Chromebook when finished working to protect one's work and information.
- Notify an adult immediately of any inappropriate or abusive messages received.
- Return the Chromebook to the Douglas Public Schools at the end of each school year. Students who graduate early, withdraw, are suspended or expelled, or terminate enrollment in the District must return their individual school Chromebook computer prior to leaving.

6.5 Chromebook Care

- **The Chromebook must be charged and ready for school each day.**
- Students will be held responsible for maintaining their individual Chromebooks and keeping them in good working order.
- Only labels or stickers approved by the Douglas School District may be applied to the Chromebook.

- Chromebooks that malfunction or are damaged must be reported to an adult at school, and the Technology Department will be contacted. The District will be responsible for repairing Chromebooks that malfunction. The cost to repair Chromebooks damaged through misuse or neglect will be borne by the student and/or parent.
- Chromebooks that are stolen must be reported immediately to the school's main office, and the theft will also be reported to the Douglas Police Department.

6.6 Student Discipline

Students who intentionally misuse the Chromebook are subject to a range of disciplinary consequences in accordance with the school disciplinary code, including the loss of Chromebook usage and/or network privileges, detention, suspension – or, in extreme cases – expulsion.

7. PROTECTING & STORING YOUR CHROMEBOOK

7.1 Chromebook Identification

Student Chromebooks will be labeled in the manner specified by the school.

7.2 Storing the Chromebook

When students are not using their Chromebooks, they should be stored in their locked lockers. Nothing should be placed on top of the Chromebook when it is stored. If a student needs a secure place to store their Chromebook, they may check it in for storage with their homeroom teacher.

7.3 Chromebooks Left in Unsupervised Areas

Under no circumstances should Chromebooks be left in unsupervised areas. Unsupervised areas include the school grounds and campus, the lunchroom, computer lab, locker rooms, library, unlocked classrooms, dressing rooms, hallways, and other unsupervised areas. Any Chromebook left in these areas is in danger of being stolen. If a Chromebook is found in an unsupervised area, it will be taken to the Technology Department or the Principal's Office.

8. LOSS OR DAMAGE

In cases of theft, vandalism and other criminal acts, a police report - or in the case of a fire, a fire report – must be filed by the student or parent . A copy of the police/fire report must be provided to the Principal's Office.

If it has been determined in the sole judgment of the school district that intentional damage was done to an Chromebook, or the Chromebook is lost, the students' parents will be responsible for the repair or replacement cost. Students/parents are not responsible for routine "wear and tear."

(Current replacement cost for the Chromebook is \$279 subject to change)

I have read and agree to the terms of the Douglas Chromebook Use Agreement. I understand that unless I sign this agreement, my child will not be allowed to take an Chromebook home. I understand that I will be held responsible for the return of the Chromebook to the Douglas Public Schools*

Student Name (Please Print) _____

Student Signature _____ **Date** _____

Parent/Guardian Signature _____ **Date** _____

Chromebook ID # _____

***Replacement cost for Chromebook is \$279 (Subject to change)**

**Commonwealth of Massachusetts – Statewide IT Asset Lease Services Contract ITC49
IT ASSET LEASE QUOTE FORM**

IT ASSET TRANSACTION SUMMARY

Lessee: Douglas Public Schools
 Lessee Location: 21 Davis St. Douglas, Ma. 01516
 Lessee Contact Name: Donna Sousa
 Telephone: 508-476-4125
 Fax: 508-476-7431
 Email: dsousa@douglas.k12.ma.us or dsousa@douglasps.net

The Lessee hereby requests financing under the Statewide IT Asset Lease Services Contract ITC49 for the following IT Asset(s). The table will expand to accommodate additional rows. Lessee should append a row at the bottom of the list of IT Assets for de-installation, packaging, and/or return of the IT Asset(s) upon lease termination, if appropriate.

| Brief Description of Asset | Asset Cost: | Total Financing Amount Requested: | Useful Life in Years (3 or more Years) |
|--|--------------|-----------------------------------|--|
| 500 Acer C720 Chromebooks 2 GB 16 GB SSD +Chrome OS Mgt Licenses | \$129,600.00 | \$129,600.00 | 3 Years |

IT Asset Contractor Name (Entity being paid by IT Asset Lease Services Contractor): CDW Government.

Contractor Address: 230 North Milwaukee Ave.

Contractor Remittance Address if different: 75 Remittance Dr. Suite 1515 Chicago, IL 60675-1515.

Contact Name: Sarah Warkowski.

Telephone: 866-849-5197.

Fax: Click here to enter text.

Email: Click here to enter text.

Description of items being purchased from this IT Asset Contractor: Acer Chromebooks with Google Chrome OS Mgt.

Anticipated Delivery Date for Acceptance of IT Asset by Lessee after Delivery: ASAP.

Total Amount of IT Asset Cost to be paid to IT Asset Contractor: \$129,600.00.

Anticipated Date for funding to be made by Statewide IT Asset Lease Services Contractor/Lessor: within 30 days of delivery and signed acceptance.

Anticipated Lease period (which may not exceed useful life): 3 Years.

Describe the essential use of the IT Asset and whether this IT Asset is replacing a current IT Asset or is a new essential use: Student Use.

Statewide IT Asset Lease Services Contractor Name: Hewlett-Packard Financial Services Company.

Vendor Code: VC6000262752. (For state agency Lessee payments.)

Contact Name: Sean Capria.

Telephone: 315-317-0668.

Fax: 908-345-6811.

Email: sean.capria@hp.com.

QUOTE:

The Statewide IT Asset Lease Services Contractor must complete the following, execute this document and submit a proposed Payment Schedule for this Quote. If accepted, the Lessee will execute this document (below) then complete and submit the necessary IT Asset Listing, Essential Use Certification, Certificate of Appropriation, and IT Asset Acceptance Certificate to their Financial/Budget Authority for approval, and, after receipt and acceptance of the IT Asset, shall complete the IT Asset Acceptance Certificate, including the Final IT Asset Lease Payment Schedule.

Statewide IT Asset Lease Services Contractor Offer of Fixed Interest Rate Quote (Valid for 30 days): (-8.09%)

Statewide IT Asset Lease Services Contractor Payment Schedule Number of payments: 3 Annual Payments of \$40,799.38 each.

Complete and attach the IT ASSET ACCEPTANCE CERTIFICATE AND LEASE PAYMENT SCHEDULE

Lessee certifies that this document is being submitted to its funding authority to confirm availability of Lease funding. Contractor certifies that this quote will be held for 30 days and is being made in compliance with the Statewide IT Asset Lease Services Contract ITC49

AUTHORIZING SIGNATURE FOR THE IT ASSET LEASE SERVICES CONTRACTOR:

X: _____ Date: _____

(Signature and Date Must Be Handwritten At Time of Signature)

Print Name: Sean Capria.

Print Title: Financial Area Manager.

AUTHORIZING SIGNATURE FOR THE LESSEE:

X: _____ Date: _____

(Signature and Date Must Be Handwritten At Time of Signature)

Print Name: Click here to enter text.

Print Title: Click here to enter text..

Douglas Public Schools iPad Use Agreement

1.0 GENERAL INFORMATION

The policies, procedures and information within this document apply to all student iPads used in the Douglas Public Schools, including any other device considered by the Administration to come under this policy. Teachers may set additional requirements for use in their classroom.

1.1 Receiving the iPad

The iPads will be distributed during class. Students in grades 2-5 will utilize the iPads via an iPad cart assigned to each teacher. Students in grades 6-8 will be allowed to take the iPads home, once both the parent and the student have signed and returned the iPad Use Agreement.

1.2 Returning the iPad

iPads, with accessories, will be returned to the Douglas Public Schools during the final week of school. If a student transfers out of the Douglas School District during the school year, the iPad will be returned at that time. Students who withdraw, are suspended or expelled, or terminate enrollment at Douglas Public Schools for any other reason must return their individual school iPad with accessories on the date of termination.

2.0 CARE OF THE IPAD

The iPad is school property and all users will follow the Douglas Public Schools Acceptable Use Policy in utilizing this technology resource. Students are responsible for the general care of the iPad they have been issued by the school. iPads that are broken or that fail to work properly must be taken as soon as possible to the Douglas Technology Department for evaluation.

2.1 General Precautions

- Only a clean, soft cloth must be used to clean the screen; no cleansers of any type should be used.
- Cords and cables must be inserted carefully into the iPad to prevent damage.
- iPads must remain free of any writing, drawing, stickers, or labels that are not the property of the Douglas Public School District.
- iPads must never be left in an unlocked locker or any unsupervised area.
- Food and drinks must be kept away from the iPad.

2.2 Carrying iPads

The protective cases provided with iPads are sufficient to protect the iPad during normal use and provide a suitable means for carrying the device within the school. The guidelines below should be followed:

- iPads should always be within the protective case when carried.
- Backpacks that hold other objects (such as folders and textbooks), should not be used to carry iPads in order to avoid placing too much pressure and weight on the iPad screen.
- Books should not be placed on top of the iPad when being carried.

2.3 Screen Care

The iPad screen can be damaged if subjected to rough treatment. The screen is particularly susceptible to damage from excessive pressure.

- Do not lean on the top of the iPad.
- Do not place anything near the iPad that could put pressure on the screen.
- Clean the screen with a soft, dry cloth or anti-static cloth.
- Do not "bump" the iPad against lockers, walls, car doors, floors, etc., as doing so will eventually break the screen.

3.0 USING THE IPAD AT SCHOOL

August 28, 2013

iPads are intended for use at school each day. In addition to teacher expectations for iPad use, school messages, announcements, calendars and schedules may be accessed using the iPad. Students must be responsible to bring their iPad to all classes, unless specifically instructed not to do so by their teacher.

3.1 iPad Undergoing Repair

Loaner iPads may be issued to students when they leave their iPads for repair in the Technology Department. Requests for loaner iPads will be filled, based on availability.

3.2 Screen Savers/Background photos

Inappropriate media may not be used as a screensaver or background photo. Inappropriate media includes but is not limited to the presence of guns, weapons, pornographic materials, inappropriate language, alcohol, drug, gang related symbols or pictures and will result in disciplinary actions. Passwords are not to be used.

3.3 Sound, Music, Games, or Programs

Sound must be muted at all times unless permission is obtained from the teacher for instructional purposes. Internet Games are not allowed on the iPads. Game apps may only be installed for educational purposes. All software/Apps must be district provided or approved.

3.4 Printing

Printing will be available with the iPad on a limited basis. Students should talk to their teachers about which printer to use. Students will be given information and instruction on printing when using the iPad at school.

4. MANAGING YOUR FILES & SAVING YOUR WORK

4.1 Saving to the iPad/Home Directory

Students may save work directly on the iPad. Storage of files will be available online using Google Drive through the school's Google Drive domain. Students may also e-mail documents to themselves and/or their teacher for storage on a District server. Storage space will be available on the iPad—but it will not be backed up in case of re-imaging. It is the student's responsibility to ensure that work is not lost, due to mechanical failure or accidental deletion.

4.2 Network Connectivity

The Douglas School District makes no guarantee that their network will be up and running 100% of the time. In the rare case that the network is down, the District will not be responsible for lost or missing data.

5. SOFTWARE ON IPADS

5.1 Originally Installed Software

The software/Apps originally installed by the Douglas Public Schools must remain on the iPad in usable condition and be easily accessible at all times. From time to time the school may add software applications for use in a particular course. Periodic checks of iPads may be made to ensure that students have not removed required apps or added apps that are not authorized by the school.

5.2 Additional Software

Students are not allowed to load extra software apps on their iPads unless otherwise directed to do so by their teachers or school staff. The Douglas Public Schools will synchronize the iPads so that they contain the necessary apps. Students will not synchronize iPads or add apps to their assigned iPad.

5.3 Procedure for Re-loading Software

If technical difficulties occur or illegal software is discovered, including apps not installed by the Douglas Public Schools, the iPad will be re-imaged. The Douglas Public School District is not responsible for the loss of any software or documents deleted, due to a re-image.

5.4 Software Upgrades

Upgraded versions of licensed software/apps are available from time to time. Students may be required to check in their iPads for periodic updates and syncing.

6. ACCEPTABLE USE

6.1 Statement of Responsibility

The use of the network is a privilege. Users are responsible for what they say and do on the network. Communication with thousands of others is quick and easy. Therefore, it is crucial for the user to stop and think before communicating, and to show respect for other people and for their ideas.

Keeping the network running efficiently is beneficial for all users. Each user must take responsibility for keeping down costs and avoiding system disruption. Excessive streaming of videos or music should be avoided unless directed to do so by a teacher for educational purposes.

Network administrators will make reasonable efforts to maintain reliable service. They cannot, however, absolutely guarantee that the system will always be available or operating correctly. Student users should assume that none of their data is private or confidential. Any communication or data may be subject to review by network or school administration.

Internet access is available on every computer with network access in the Douglas Public Schools. Users must adhere to the Douglas Public Schools' network rules, guidelines, and procedures when connected to other networks.

6.2 Parent/Guardian Responsibilities

Parents are encouraged to speak with their children about safe usage of the Internet, including guidelines to follow in order to ensure proper usage. As with any use of media, the potential exists for misuse. It is important that students, educators, and parents all work together to ensure that students practice good digital citizenship.

6.3 School Responsibilities

- Provide Internet and Email access.
- Provide Internet Blocking of inappropriate materials to the greatest extent possible.
- Provide network data storage areas. These will be treated similar to school lockers. The District reserves the right to review, monitor, and restrict information stored on or transmitted via district-owned equipment, and to investigate the inappropriate use of resources.
- Provide staff guidance to aid students in proper technology usage.

6.4 Students Responsibilities:

- Use computers/devices in a responsible and ethical manner.
- Obey school rules concerning behavior and communication that apply to network use, in accordance with the **Douglas Public Schools Acceptable Use Policy**. This policy is available online and in the student handbooks and must be signed by students and their parents each year as part of the student handbook.
- Use all technology resources in an appropriate manner so as to not damage school equipment through negligence, errors or omissions - potentially causing loss of data resulting from delays, non-deliveries, mis-deliveries, or service interruptions.
- Use of any information obtained via the Douglas School District's designated Internet System is at the user's own risk. The District is not responsible for the accuracy or quality of information obtained on the Internet through utilizing the District's services.
- Cooperate with the Douglas Public Schools in protecting the computer system and devices by promptly notifying an adult about any security problems encountered.
- Monitor account activity.
- Turn off and secure the iPad when finished working to protect one's work and information.
- Notify an adult immediately of any inappropriate or abusive messages received.
- Return the iPad to the Douglas Public Schools at the end of each school year. Students who graduate early, withdraw, are suspended or expelled, or terminate enrollment in the District must return their individual school iPad computer prior to leaving.

6.5 iPad Care

- The iPad must be charged and ready for school each day.
- Students will be held responsible for maintaining their individual iPads and keeping them in good working order.
- Only labels or stickers approved by the Douglas School District may be applied to the iPad.
- iPad cases furnished by the school district must be returned with only normal wear and no alterations to avoid paying a replacement fee.
- iPads that malfunction or are damaged must be reported to an adult at school, and the Technology Department will be contacted. The District will be responsible for repairing iPads that malfunction. The cost to repair iPads damaged through misuse or neglect will be borne by the student and/or parent.
- iPads that are stolen must be reported immediately to the school's main office, and the theft will also be reported to the Douglas Police Department.

6.6 Student Discipline

Students who intentionally misuse the iPad are subject to a range of disciplinary consequences in accordance with the school disciplinary code, including the loss of iPad usage and/or network privileges, detention, suspension – or, in extreme cases – expulsion.

7. PROTECTING & STORING YOUR IPAD

7.1 iPad Identification

Student iPads will be labeled in the manner specified by the school.

7.2 Storing the iPad

When students are not using their iPads, they should be stored in their locked lockers or in an iPad cart. Nothing should be placed on top of the iPad when it is stored. If a student needs a secure place to store their iPad, they may check it in for storage with their homeroom teacher.

7.3 iPads Left in Unsupervised Areas

Under no circumstances should iPads be left in unsupervised areas. Unsupervised areas include the school grounds and campus, the lunchroom, computer lab, locker rooms, library, unlocked classrooms, dressing rooms, hallways, and other unsupervised areas. Any iPad left in these areas is in danger of being stolen. If an iPad is found in an unsupervised area, it will be taken to the Technology Department or the Principal's Office.

8. LOSS OR DAMAGE

In cases of theft, vandalism and other criminal acts, a police report - or in the case of a fire, a fire report – must be filed by the student or parent . A copy of the police/fire report must be provided to the Principal's Office.

If it has been determined in the sole judgment of the school district that intentional damage was done to an iPad, or the iPad is lost, the students' parents will be responsible for the repair or replacement cost. Students/parents are not responsible for routine "wear and tear."

(Current replacement cost for the iPad is \$399 subject to change)

I have read and agree to the terms of the Douglas iPad Use Agreement. If I am the parent of a sixth or seventh grader, I understand that unless I sign this agreement, my child will not be allowed to take an iPad home. (Fourth and fifth graders will use the iPad in school, but will not take them home.)

I understand that I will be held responsible for the return of the iPad to the Douglas Public Schools*

Student Name (Please Print) _____

Student Signature _____ **Date** _____

Parent/Guardian Signature _____ **Date** _____

iPad ID # _____

*Replacement cost for iPad is \$399 (Subject to change)