Durant Independent School District
Mobile Computing Handbook

Acceptable use for Personal and District Owned Computers and Devices, Mobile Devices, Internet Access, Google Apps for Education Suite, and Internet Applications

Student Guidelines and Policies for Acceptable Use of Technology Resources for Mobile Computing at DISD

These guidelines and policies are provided so that students and parents are aware of the responsibilities students accept when they use Personal or District-owned computer hardware, operating system software, application software, stored text, data files, electronic mail, local databases, CDROMs, digitized information, communication technologies, and Internet access. In general, this requires efficient, ethical, and legal utilization of all technology resources.

1. Expectations are as follows:

a. Student use of Personal or district-owned computers or devices, other technology hardware, software, and computer networks, including the Internet, is only allowed when supervised or granted permission by a staff member, during passing periods or at lunch.
b. All users are expected to follow existing copyright laws.
c. Although the District has an Internet safety plan in place, students are expected to notify a staff member whenever they come across information or messages that are inappropriate, dangerous, threatening, or make them feel uncomfortable.
d. Students who identify or know about a security problem are expected to convey the details to their teacher without discussing it with other students.
e. Students are expected to follow Digital Citizenship guidelines as established by the ISTE National Education Technology Standards (NETS □S), v
topics below.

2. Unacceptable conduct includes, but is not limited to the following:

a. Using the network for illegal activities, including copyright, license, or contract violations or downloading inappropriate materials, viruses, and/or software, such as but not limited to hacking and host file-sharing software.
b. Using the network for financial or commercial gain, advertising, or political lobbying.
c. Accessing or exploring online locations or materials that do not support the curriculum and/or are inappropriate for school assignments, such as but not limited to pornographic sites.
d. Vandalizing and/or tampering with equipment, programs, files, software, system performance, or other components of the network. Use or possession of hacking software is strictly prohibited.
e. Causing congestion on the network or interfering with the work of others, e.g., chain letters or broadcast messages to lists or individuals.
f. Intentionally wasting finite resources, i.e., online time, real-time music.
g. Gaining unauthorized access anywhere on the network.
h. Revealing the home address or phone number of one's self or another person.
i. Invading the privacy of other individuals.
j. Using another user's account, password, or ID card or allowing another user to access your account, password, or ID.
k. Coaching, helping, observing, or joining any unauthorized activity on the network.
l. Posting anonymous messages or unlawful information on the system.
m. Engaging in sexual harassment or using objectionable language in public or private messages, e.g., racist, terroristic, abusive, sexually explicit, threatening, demeaning, stalking, or slanderous.
n. Falsifying permission, authorization, or identification documents.
o. Obtaining copies of or modifying files, data, or passwords belonging to other users on the network.
p. Knowingly placing a computer virus on a computer or network.

3. Acceptable use guidelines for the District's network computer online services are as follows:

a. General Guidelines:

i. Students will have access to all available forms of electronic media and communication that is in support of education and research, and in support of the educational goals and objectives of the District. Personal devices will be filtered by the District in the same manner as District-owned equipment.

ii. Students are responsible for their ethical and educational use of the computer online services in the District.

iii. All policies and restrictions of the District's computer online services must be followed.

iv. Access to the District's computer online services is a privilege and not a right. Each employee, student, and/or parent will be required to sign the Acceptable Use Policy Agreement Sheet and adhere to the Acceptable Use Guidelines in order to be granted access to District computer online services.

v. The use of any District computer online services in the District must be in support of education and research and in support of the educational goals and objectives of the District.

vi. When placing, removing, or restricting access to specific databases or other District computer online services, school officials will apply the same criteria of educational suitability used for other education resources.

vii. Transmission of any material that is in violation of any federal or state law is prohibited. This includes, but is not limited to confidential information, copyrighted material, threatening or obscene material, and computer viruses.

viii. Any attempt to alter data, the configuration of a computer, or the files of another user without the consent of the individual, campus administrator, or technology administrator, will be considered an act of vandalism and subject to disciplinary action in accordance with the District's Student Code of Conduct booklet.

ix. Parents concerned with the District's computer online services at their child's school should refer to EFA(LOCAL): Instructional Resources: Instructional Material Selection and Adoption policy and follow the stated procedure.

x. Any parent wishing to restrict their children's access to any District computer online services will provide this restriction request in writing. Parents will assume responsibility for imposing restrictions only on their own children.

b. Network Etiquette:

i. Be polite.

ii. Use appropriate language.

iii. Do not reveal personal data (home address, phone number, phone numbers of other people).

iv. Remember that the other users of the District's computer online services and other networks are human beings whose culture, language, and humor have different points of reference from your own.

v. Users should be polite when forwarding e-mail. The intent of forwarding email should be on a need-to-know basis.

c. E-Mail:

i. All secondary students will be provided with a school affiliated email address which is filtered to meet CIPA requirements.

ii. E-mail should be used for educational or administrative purposes only.

iii. E-mail transmissions, stored data, transmitted data, or any other use of the District's computer online services by students, employees, or any other user shall not be considered confidential and may be monitored at any time by designated staff to ensure appropriate use.

iv. All e-mail and all e-mail contents are property of the District.

d. BYOD (bring your own device) [At this time, Durant Middle School will not be participating in the BYOD Initiative]

i. Personal device types allowed, for the use of BYOD at the District, include but are not limited to most laptops, tablets, netbooks, etc. Devices must support wireless WPA2 Enterprise using certificate-based authentication and be capable of using Google Applications. Smartphones are not acceptable devices for the BYOD initiative without permission by the teacher or administration under extenuating circumstances.

ii. Students using personal devices must attend BYOD orientation to insure the proper connectivity and use of their device on the District network.

iii. Students may not use personal devices to record audio, video, or take still photos during school unless they have permission from both a staff member and those whom they are recording.

iv. Personal devices must be in silent mode while on school campuses and while riding school buses.

v. Personal devices must be connected to the District Wireless network to access the Internet and may not be used with cellular provider service while on campus.

vi. Personal devices are the sole responsibility of the student owner. The school or District assumes no responsibility for personal devices if they are lost, loaned, damaged or stolen. The District will handle disciplinary issues concerning personal devices in the same manner as with any other personal property.

vii. Campus administrators and teachers have the right to prohibit use of devices at certain times or during designated activities (i.e. campus presentation, theatrical performance, or guest speaker) that occur during the school day.

viii. Each student is responsible for his/her own personal device: set-up, maintenance, and charging. Teachers will not store student devices at any time, nor will any District employee diagnose, repair, or work on a student's personal device. Minimal tech support may be provided for student's personal devices.

ix. Personal devices are only to be used in the classroom for educational purposes at the discretion of a teacher.

x. An appropriately-trained administrator may examine a student's personal device and search its contents, in accordance with the law, if there is a reason to believe that the Responsible Use Guidelines has been violated.

4. Consequences for breach of Acceptable Use Policy

a. The student in whose name a system account and/or computer hardware is issued will be responsible at all times for its appropriate use.

b. Noncompliance with the guidelines published here, in the Student Code of Conduct, may result in suspension or termination of technology privileges and disciplinary actions. Use or possession of hacking software is strictly prohibited and violators will be subject to consequences of the Student Code of Conduct. Violations of applicable state and federal law, including the Oklahoma Penal Code, Computer Crimes, will result in criminal prosecution, as well as disciplinary actions by the District.

c. Electronic mail, network usage, and all stored files will not be considered confidential and may be monitored at any time by designated District staff to ensure appropriate use.

d. The District will cooperate fully with local, state, or federal officials in any investigation concerning or relating to violations of computer crime laws. Contents of e-mail and network communications will be turned over to the proper authorities and proper authorities will be given access to their content.

Terms of the Netbook Loan

Terms: You will comply at all times with the Durant School District's Parent/Student Netbook Handbook and Acceptable Use Policy, incorporated herein by reference and made a part hereof for all purposes. Any failure to comply may terminate your rights of possession effective immediately and the District may repossess the property. Students shall have no reasonable expectation of privacy in the Netbook and the District, in its sole discretion, can review the contents of the Netbook at any time.

Title: Legal title to the property is in the District and shall at all times remain in the District. Your right of possession and use is limited to and conditioned upon your full and complete compliance with this Agreement and the Parent/Student Netbook Handbook.

Loss or Damage: If the property is intentionally damaged, you are responsible for the reasonable cost of repair or its fair market value on the date of damage. Loss or theft of the property must be reported to the District by the next school day after the occurrence, or you will be responsible for the fair market value replacement. A table of estimated pricing for a variety of repairs is included in the Parent/Student Netbook handbook to which reference is hereby made. Seniors must clear all records and pay all fees before participating in graduation ceremonies.

Repossession: If you do not timely and fully comply with all terms of this Agreement and the Parent/Student Netbook Handbook, including the timely return of the property, the District shall be entitled to declare you in default and come to your place of residence, or other location of the property, to take possession of the property. The District, in its sole discretion, shall determine if a violation of this Agreement and the Mobile Computing Handbook has occurred. The District's determination shall be conclusive.

Term of Agreement: Your right to use and possession of the property terminates not later than the last day of the school year unless earlier terminated by the District or upon withdrawal from the District.

Appropriation: Your failure to timely return the property and the continued use of it for non-school purposes without the District's consent may be considered unlawful appropriation of the District's property.

Use & Maintenance Costs

- In case of theft, vandalism, and other criminal acts, a **police report MUST be filed by the student or parent within 48 hours of the occurrence. Incidents happening off campus must be reported to the police by the parent and a copy of the report must be brought to the school.**
- If netbook is stolen and student reports the theft (by the next school day) and police filed a report, then the student will not be charged.
- **Student will be charged the Fair Market Value of the netbook if lost, deliberately damaged or vandalized.** (see Fair Market Value chart below)
- Seniors must clear all records and pay all fees before participating in graduation.
- Students/Parents are responsible for reasonable cost of repair for deliberately damaged netbooks (see Repair Pricing chart below).

Fair Market Value

Original cost of a netbook to the District is currently $625.00

The costs of any other parts needed for repairs or any damage after 3rd offense will be based on manufacturer's current price list.

Age of Netbook	Value
1 year or less	$ 500
2 years	$ 400
3 years	$ 300
4 years	$ 200

Table of Estimated Repair Pricing

Loss, Deliberate Damage, or Neglect	Actual Repair Costs	Repair Costs to Students
Broken Screen	$ 200	$0 (1st offense), $50 (2nd), $75 (3rd)
Keyboard	$ 25	Up to $25
Power Adapter + Cord (damage or loss)	$ 50	$35
Battery	$ 80	$40
Re-image of Hard Drive due to violation of Acceptable Use Policy or other damages (graffiti, illegal software)	$ 15	$15
Abandonment Fee (if eventually found)	$ 15	$15
Access Panel, Display assembly, Heat/sink fan assembly, Palm Rest	$30-$50	$15-$25

Netbook Usage Guidelines and Procedures

Durant ISD is committed to provide the necessary tools to effectively utilize netbooks. To accommodate this process, the District is providing the following:

Check-Out Check-In Procedures

The netbook check-out/check-in process will mirror textbook management practices established at each individual campus.

Sophos Enterprise Anti-virus Protection

Netbooks will utilize Sophos Endpoint security solution providing real-time scanning capabilities for complete protection from viruses, spyware, malware, etc., both inside and outside the Durant ISD network.

Web Filtering and Security

Websense Remote Filtering extends the Websense industry-leading Web filtering and Web security technology to protect netbook users outside of your organization's network. Remote Filtering protects remote users and frequent travelers from external security threats and prevents access to inappropriate and malicious sites, phishing sites, spyware, and malicious mobile code. A critical component of any organization's endpoint protection strategy, remote filtering ensures secure internet use anytime and anywhere. Durant ISD has utilized the Websense Enterprise filtering solution for the past 8 years to meet federal CIPA requirements. For more information about Internet safety, please visit www.isafe.org.

Data Access

Students can save important files to their "My Documents" folder which is re-directed to a network storage area, and backed-up nightly. Students can access this data from any computer connected to the Durant ISD network. While working off-site, student data will be cached locally and synchronized once network access is established.

Students will also be able to save files to the desktop of their netbook, such as electronic textbooks, photos, temporary files, etc. However, a backup of these items is not done automatically, so students might want to keep a copy of these files on a flash drive or other external device.

Profiles and Policies

Student policies are pushed from Active Directory Services for all student log-ins giving sufficient access to complete tasks. While allowing for windows security updates, students will not have install capabilities for other software. Requests for additional software packages can be made through their campus "Help Desk". A district approved default software package will be installed on all netbooks prior to checkout.

Tracking System

BIOS level software will be installed at the manufacturer providing the ability to GPS track, locate and recover lost or stolen netbooks.

Help Desk Requests

The Durant ISD Information Technology Department will strive to provide "same day" turn around on all student/teacher netbook problems. All Help Desk requests will be submitted to the campus technology office and prioritized accordingly.

Summer Storage

Netbooks will be returned during the textbook check-in process at each campus and stored appropriately. All netbooks will be thoroughly inspected and re-imaged during the summer months by the IT Dept client services staff.

Parental Involvement
In addition to the Student Netbook Handbook, informative presentations will be provided both in person, as a file on the netbooks, and through our District website for parents regarding the One-to-One initiative. A parental permission form must be signed and on file before netbook receipt.

Classroom Computers
The District currently has 6 computer labs on campus. These computers can be used by students if they do not have their netbook. They will be able to access their work saved in the "My Documents" folder from any computer on the Durant ISD network.

No Loaning or Borrowing Netbooks
- Do NOT loan netbooks or other equipment to anyone.
- Do NOT borrow a netbook from another student.
- Do NOT share passwords or usernames with others.

General Netbook Rules
Inappropriate Content & Graffiti
- Inappropriate content will not be allowed on netbooks.
- Physical appearance of the netbook may not be modified by any means, including skins, stickers, markers, etc.
- Presence of weapons, pornographic materials, inappropriate language, alcohol, drug, gang-related symbols or pictures on the netbook will result in disciplinary actions.
- In the case of intentional damage, students will be charged for replacement parts.
- See Table of Estimated Repair Pricing on page 3.

Sound
- Sound will be muted at all times unless permission is obtained from the teacher for instructional purposes. Headphones, provided by the student, may be used when approved by the teacher.

Deleting Files
- Do not delete any folders or files that you did not create or that you do not recognize. Deletion of certain files will result in a computer failure and will interfere with your ability to complete class work and may affect your grades.

Music, Games, or Programs
- Music and games may not be downloaded or streamed over the Internet. This may be a violation of copyright laws.
- All software loaded on the system must be District approved.
- See Table of Estimated Repair Pricing on page 3.

Unauthorized Access (Board Policy)
- Access to another person's account or computer without their consent or knowledge is considered hacking and is unacceptable.

Oklahoma Penal Code §21-1951

A person who is subject to prosecution under this section and any other section of this code may be prosecuted under either or both sections.

This act shall be known and may be cited as the "Oklahoma Computer Crimes Act".

§21-1952.

As used in the Oklahoma Computer Crimes Act:

1. "Access" means to approach, gain entry to, instruct, communicate with, store data in, retrieve data from or otherwise use the logical, arithmetical, memory or other resources of a computer, computer system or computer network;
2. "Computer" means an electronic device which performs work using programmed instruction having one or more of the capabilities of storage, logic, arithmetic or communication. The term includes input, output, processing, storage, software and communication facilities which are connected or related to a device in a system or network;
3. "Computer network" means the interconnection of terminals by communication modes with a computer, or a complex consisting of two or more interconnected computers;
4. "Computer program" means a set or series of instructions or statements and related data which when executed in actual or modified form directs or is intended to direct the functioning of a computer system in a manner designed to perform certain operations;
5. "Computer software" means one or more computer programs, procedures and associated documentation used in the operation of a computer system;
6. "Computer system" means a set of related, connected or unconnected, computer equipment, devices including support devices, one or more of which contain computer programs, electronic instructions, input data, and output data, that performs functions including, but not limited to, logic, arithmetic, data storage and retrieval, communication, and control and software. "Computer system" does not include calculators which are not programmable and are not capable of being connected to or used to access other computers, computer networks, computer systems or support devices;
7. "Data" means a representation of information, knowledge, facts, concepts, computer software, computer programs or instructions. Data may be in any form, in storage media, or as stored in the memory of the computer or in transit or presented on a display device;
8. "Property" means any tangible or intangible item of value and includes, but is not limited to, financial instruments, geophysical data or the interpretation of that data, information, computer software, computer programs, electronically-produced data and computer-produced or stored data, supporting documentation, computer software in either machine or human readable form, electronic impulses, confidential, copyrighted or proprietary information, private identification codes or numbers which permit access to a computer by authorized computer users or generate billings to consumers for purchase of goods and services, including but not limited to credit card transactions and telecommunications services or permit electronic fund transfers and any other tangible or intangible item of value;
9. "Services" includes, but is not limited to, computer time, data processing and storage functions and other uses of a computer,computer system or computer network to perform useful work;
10. "Supporting documentation" includes, but is not limited to, all documentation in any form used in the construction, design, classification, implementation, use or modification of computer software, computer programs or data; and
11. "Victim expenditure" means any expenditure reasonably and necessarily incurred by the owner or lessee to verify that a computer system, computer network, computer program or data was or was not altered, deleted, disrupted, damaged or destroyed by the access.

§21-1953.

A. It shall be unlawful to:

1. Willfully, and without authorization, gain or attempt to gain access to and damage, modify, alter, delete, destroy, copy, make use of, disclose or take possession of a computer, computer system, computer network or any other property.
2. Use a computer, computer system, computer network or any other property as hereinbefore defined for the purpose of devising or executing a scheme or artifice with the intent to defraud, deceive, extort or for the purpose of controlling or obtaining money, property, services or other thing of value by means of a false or fraudulent pretense or representation.
3. Willfully exceed the limits of authorization and damage, modify, alter, destroy, copy, delete, disclose or take possession of a computer, computer system, computer network or any other property.
4. Willfully and without authorization, gain or attempt to gain access to a computer, computer system, computer network or any other property.
5. Willfully and without authorization use or cause to be used computer services.
6. Willfully and without authorization disrupt or cause the disruption of computer services or deny or cause the denial of access or other computer services to an authorized user of a computer, computer system or computer network.
7. Willfully and without authorization provide or assist in providing a means of accessing a computer, computer system or computer network in violation of this section.

B. Any person convicted of violating paragraph 1, 2, 3, 6 or 7 of subsection A of this section shall be guilty of a felony.

C. Any person convicted of violating paragraph 4 or 5 of subsection A of this section shall be guilty of a misdemeanor.

§21-1954.

Proof that any person has accessed, damaged, disrupted, deleted, modified, altered, destroyed, caused to be accessed, copied, disclosed or taken possession of a computer, computer system, computer network or any other property, or has attempted to perform any of these enumerated acts without authorization or exceeding the limits of authorization, shall be prima facie evidence of the willful violation of the Oklahoma Computer Crimes Act.

§21-1955.

A. Upon conviction of a felony under the provisions of the Oklahoma Computer Crimes Act, punishment shall be by a fine of not less than Five Thousand Dollars ($5,000.00) and not more than One Hundred Thousand Dollars ($100,000.00), or by confinement in the State Penitentiary for a term of not more than ten (10) years, or by both such fine and imprisonment.

B. Upon conviction of a misdemeanor under the provisions of the Oklahoma Computer Crimes Act, punishment shall be by a fine of not more than Five Thousand Dollars ($5,000.00), or by imprisonment in the county jail not to exceed thirty (30) days, or by both such fine and imprisonment.

C. In addition to any other civil remedy available, the owner or lessee of the computer, computer system, computer network, computer program or data may bring a civil action against any person convicted of a violation of the Oklahoma Computer Crimes Act for compensatory damages, including any victim expenditure reasonably and necessarily incurred by the owner or lessee to verify that a computer system, computer network, computer program or data was or was not altered, damaged, deleted, disrupted or destroyed by the access. In any action brought pursuant to this subsection the court may award reasonable attorney's fees to the prevailing party.

§21-1957.

For purposes of bringing a civil or a criminal action under the Oklahoma Computer Crimes Act, a person who causes, by any means, the access of a computer, computer system or computer network in one jurisdiction from another jurisdiction is deemed to have personally accessed the computer, computer system or computer network in each jurisdiction.

§21-1958.

No person shall communicate with, store data in, or retrieve data from a computer system or computer network for the purpose of using such access to violate any of the provisions of the Oklahoma Statutes.

Any person convicted of violating the provisions of this section shall be guilty of a felony punishable by imprisonment in the State Penitentiary for a term of not more than five (5) years, or by a fine of not more than Five Thousand Dollars ($5,000.00), or by both such imprisonment and fines