ACCEPTABLE USE POLICY
Policy IJNDB Use of Technology Resources in Instruction

Purpose: To establish the board's vision and the basic structure for the use of technology resources in instruction.

DCSDNet ACCEPTABLE USE POLICY

The purpose of the DCSDNet acceptable use policy is to provide the procedures, rules, guidelines and the code of conduct for use of technology and the information network in the Darlington County School District.

Definition

The definition of "information network" is any configuration of hardware and software that connects users. The network includes all of the computer hardware, operating system software, application software and stored files. This includes but is not limited to electronic mail, local databases, externally accessed databases, recorded magnetic or optical media, clip art, digital images, digitized information, communications technologies, portable/hand-held devices and new technologies as they become available. Stand alone workstations are also governed by this acceptable use policy.

Introduction

Darlington County School District network (DCSDNet) provides resources for teaching and collaboration, communication services and business data services by maintaining access to local, regional, national and international sources of information.

The DCSDNet information resources will be used by members of the school community with respect for the public trust through which they have been provided and in accordance with policy and regulations established by the school district. These procedures do not attempt to articulate all required or prescribed behavior by its users.

Successful operation of the network requires that all users conduct themselves in a responsible, decent, ethical and polite manner while using the network. The user is ultimately responsible for his/her actions in accessing network services inside and outside of the DCSD network while using district-issued equipment. The user is solely responsible for all resources issued or assigned to him/her. This includes equipment as well as login / specialized access information. In addition, any personal equipment used to access the Internet or other district resource is subject to the same rules and regulations outlined in this policy. The district monitors all Internet and local network activity. Disciplinary action will be taken for any individual abusing or misusing technology resources.

Disclaimer

With access to computers and people all over the world also comes the availability of materials that may not be considered to be of educational value in the context of the school setting. On a global network it is impossible to control all materials, and an industrious user may discover controversial information. The district maintains and monitors the use of filters for Internet content. The district firmly believes that the valuable information and interaction available on this worldwide network far outweighs the possibility that users may procure materials that are not consistent with the educational goals of the school/district. The district monitors all Internet and local network activity.

Guidelines
- ❖ Access to the networks and to the information technology environment within DCSDNet is a privilege and must be treated as such by all users of the network and its associated systems.
- ❖ DCSDNet will be used for the purposes of research, education and school-related business and operations.
- ❖ Any system which requires password access, or for which the district requires an account, such as Internet, may only be used by the authorized user. Account owners are ultimately responsible for all activity under their account.
- ❖ The resources of the DCSDNet are limited. All users must exercise prudence in the shared use of this resource.
- ❖ All communications and information accessible via DCSDNet should be treated as property of the district.
- ❖ The district monitors all Internet and local network activity.

UNACCEPTABLE USES

The district has the right to take disciplinary action, remove computer and networking privileges and/or take legal action for any activity characterized as unethical and unacceptable. Unacceptable use activities constitute, but are not limited to, any activity through which any user does the following.
- ❖ Violates such matters as institutional or third party copyright, license agreements or other contracts. The unauthorized use of and/or copying of software are illegal.
- ❖ Copies or reproduces any licensed software on DCSD computing equipment, except as expressly permitted by the specific software license. Unauthorized use of software is regarded as a serious matter and any such use is without the consent of DCSD.
- ❖ Installs unauthorized software for use on district computers.
- ❖ Interferes with or disrupts other network users, services or equipment. Disruptions include, but are not limited to, the following:
  - o distribution of unsolicited advertising
  - o propagation of computer worms or viruses
  - o distribution of quantities of information that overwhelm the system (for example, "chain letters," "network games" or "broadcasting" messages)
  - o utilization of the network to make unauthorized entry into any resource accessible via the network.
- ❖ Seeks to gain or gains unauthorized access to information resources, obtains copies of or modifies files or other data, or gains and communicates passwords belonging to other users.
- ❖ Uses or knowingly allows another to use any computer, computer network, computer system, program or software to devise or execute a scheme to defraud or to obtain money, property, services or other things of value by false pretenses, promises or representations.
- ❖ Destroys, alters, dismantles, disfigures, prevents rightful access to or otherwise interferes with the integrity of computer-based information and/or information resources whether on stand-alone or networked computers.
- ❖ Invades the privacy of individuals or entities.
- ❖ Uses the network for commercial or political activity.

Unacceptable Uses – continued

❖ Uses the network to store, distribute or access materials inappropriate to the school district setting.
❖ Uses DCSDNet to compromise its integrity ("hacking" software).
❖ Submits, publishes or displays any defamatory inaccurate, racially offensive, abusive, obscene, profane, sexually oriented or threatening materials or messages either public or private.
❖ Uses DCSDNet for illegal, harassing, vandalizing, inappropriate or obscene purposes, or in support of such activities. Illegal activities will be defined as a violation of local, state and/or federal laws. Harassment is defined as slurs, comments, jokes, innuendoes, unwelcome compliments, cartoons, pranks and/or other verbal conduct relating to an individual that has the following purposes or effects.
   o creating an intimidating, hostile or offensive environment
   o unreasonably interfering with an individual's work or school performance
   o interfering with school operations
❖ Vandalism is defined as any attempt to harm or destroy an operating system, application software or data, or hardware. Inappropriate use will be defined as a violation of the purpose and goal of the DCSDNet. Obscene activities will be defined as a violation of generally accepted social standards for use of a publicly-owned and operated communication vehicle.

District rights

Darlington County School District reserves the right to do the following.
   ❖ Monitor all activity on DCSDNet.
   ❖ Make determinations on whether specific uses of the network are consistent with this acceptable use policy.
   ❖ Log network use and monitor storage disk space utilization by users.
   ❖ Deem what is appropriate use based on the requirements of law, this policy and the district's legitimate pedagogical concerns.
   ❖ Remove a user's access to the network at any time it is determined that the user is engaged in unauthorized activity or violating this acceptable use policy and suspend any accounts during an investigation of possible violations of this policy.
   ❖ Cooperate fully with any investigation concerning or relating to DCSDNet.

District responsibilities

The district will do the following.
- ❖ Respect and enforce copyright laws and regulations.
- ❖ Take prudent steps to develop, implement and maintain security procedures to insure the integrity of individual and district files. However, information on any computer system cannot be guaranteed to be inaccessible by other users.
- ❖ Attempt to provide error free and dependable access to technology resources associated with DCSDNet. However, the district cannot be held liable for any information that may be lost, damaged or unavailable due to technical or other difficulties.
- ❖ Thoroughly investigate alleged misuse of the Internet and/or DCSDNet prior to permanent denial of access to DCSDNet resources.
- ❖ Conduct assessments of inappropriate sites.
- ❖ Monitor student Internet activities to ensure students and employees are not accessing inappropriate sites that have visual depictions that include obscenity, child pornography or are harmful to minors. The school district will use technology protection measures to protect students from inappropriate access.
- ❖ Expects that all students using DCSDNet resources will be monitored by an adult(s).
- ❖ Report child pornography to law enforcement. District and school technical support staff who are working with any computer or portable device and come across sexually explicit images of children must report this to local law enforcement. The report must include the name and address of the owner or person in possession of the computer.

Disciplinary action

This acceptable use policy is applicable to any member of the DCSDNet community and refers to all information resources whether individually controlled, shared, stand alone or networked. Disciplinary action, if any, for students, staff and other users will be consistent with the district's standard policies and practices. Where use of external networks is involved, policies governing such use also are applicable and must be adhered to. Violations can constitute cause of revocation of access privileges, suspension or permanent removal of access to DCSDNet resources, other school disciplinary action and/or appropriate legal action. Exact disciplinary measures will be determined on a case by case basis.

Any user who violates the terms of this policy or otherwise misuses the Internet and/or technology to access or send inappropriate material will be subject to disciplinary action up to and including a recommendation that the individual's employment with the district be terminated and/or the suspension of his/her teaching certificate. Violations of the laws of the United States or the state of South Carolina also may subject the user to criminal prosecution.

FILE: IJNDB-E(1) Internet Code of Conduct

Use of the Internet by students and staff of Darlington County School District will be in support of education and research that is consistent with the mission of the district. Internet use is limited to those persons who have been issued district approved accounts. Guest users must follow guidelines established for access to the Internet through district resources. Guest access will be monitored in the same manner as DCSD students and staff. Use will be in accordance with the district's acceptable use policy and this code of conduct.

- ❖ Protect your log-on information from others.

- ❖ Respect the privacy of other users. Do not use other users' passwords.

- ❖ Be ethical and courteous. Do not send hate, harassing or obscene mail, discriminatory remarks or demonstrate other antisocial behaviors.

- ❖ Maintain the integrity of files and data. Do not modify or copy files/data of other users without their consent.

- ❖ Treat information created by others as the private property of the creator. Respect copyrights.

- ❖ Use the network in a way that does not disrupt its use by others.

- ❖ Do not destroy, modify or abuse the hardware or software in any way.

- ❖ Do not develop or pass on programs that harass other users or infiltrate a computer or computing system and/or damage the software components of a computer or computing system. Do not "hack" the system.

- ❖ Do not use the Internet to access or process pornographic or otherwise inappropriate material.

- ❖ Do not use the Internet for commercial purposes.

- ❖ The district reserves the right to suspend any account for purposes of investigating possible violations of district technology use polices and to remove a user's account if it is determined that the user is engaged in unauthorized activity is violating this code of conduct.

- ❖ The district reserves the right to review content of all files stored, of all information accessed via the Internet and/or of e-mails sent or received through DCSDNet.

DARLINGTON COUNTY SCHOOL DISTRICT

FILE: IJNDB-E(2) Sample Letter to Parents

Dear Parents/Legal Guardian(s):

Darlington County School District has the ability to enhance your child's education by providing Internet access. The Internet is a worldwide network of computers. It allows your child the opportunity to access rich information sources, share information, learn concepts and communicate with children and adults from other parts of the country and the world.

It is our intention to provide an Internet environment that is safe and appropriate for the maturity level and need to student users. However, with access to computers and people all over the world also comes the availability of materials that may be of no educational value, abusive, racially biased or otherwise offensive. Once students become knowledgeable in the use of the Internet, they may discover this controversial information. It is impossible to control all materials on a global network, but the district maintains and monitors the use of content filters for Internet content. The district cannot guarantee that students will not locate this type of material as they explore the Internet's resources. However, the district firmly believes that the valuable information and interaction available on this worldwide network far outweighs the possibility that users may procure materials that are not consistent with the educational goals of the school/district.

Personal devices available today such as cell phones, ipads/ipods, etc., provide students with Internet access. The district is not responsible for content that students may access through networks outside of DCSD (such as cellular service providers). However, any personal device that accesses resources through DCSDNet will be monitored and are subject to confiscation pending an investigation of abuse or misuse.

Darlington County School District is using DCSDNet (Darlington County School District Network) as our access to the Internet. Use of the Internet is an educational opportunity that requires users to act responsibly, ethically and in accordance with network use guidelines. Student Internet activities will be monitored by the district to ensure students are not accessing inappropriate sites that have visual depictions that include obscenity, child pornography or are harmful to minors. The student is responsible for his/her conduct on the Internet. Internet monitoring by district and school personnel will be in full compliance with the Children's Internet Protection Act.

If you wish your child to have access to the Internet, please review the attached code of conduct and the DCSDNet acceptable use policy with your child. You and your child must both sign the Student User Internet Access release form indicating your agreement with the conditions for Internet use. The signed release form must be returned to your child's school before access will be provided.
Sincerely,

Superintendent

FILE: IJNDB-E(3) STUDENT INTERNET USE AGREEMENT

Student name_____
Last name printed   First name printed   Middle initial

I have read and understand the rules and requirements for accessing information on the Internet. I agree to abide by the rules and I further understand that any violation of the rules is unethical and may constitute a criminal offense. I understand that the district is monitoring all of my activity on the Internet while using DCSDNet. Should I commit any violation, my access privileges may be revoked for the remainder of the year. School disciplinary and/or appropriate legal action may be taken.

_____   _____
Student signature   Date

Sponsoring teacher's name _____
Last name printed   First name printed   Middle initial

_____   _____
Sponsoring teacher's signature   Date

PARENT / GUARDIAN PERMISSION

As the parent/guardian of this student, I have read the Darlington County School District Acceptable Use Policy. I understand that this access is designed for educational purposes. I recognize it is impossible for Darlington County School District to restrict access to all controversial materials and I will not hold them responsible for materials acquired on the network.

I understand that I can be contacted at the phone number below to verify my permission and that if I have questions regarding topics my child is researching or how my child is using the Internet, I will contact his/her teacher. I understand that the district is monitoring all of my child's activity on the Internet while using DCSDNet. I hereby give permission to have my child access information on the Internet.

Parent/Guardian name_____
Last name printed   First name printed   Middle initial

_____
Phone number and time to call

_____   _____
Parent/Guardian signature   Date

FILE: IJNDB-E(4) EMPLOYEE INTERNET USE AGREEMENT

Employee name _____
Last name printed   First name printed   Middle initial

The Darlington County School District strongly believes in the educational value of the Internet and recognizes its potential to support curriculum and student learning by facilitating resource sharing, innovation and communication. The district also believes this educational opportunity demands personal responsibility and an understanding of the acceptable use policy for the Internet by students and staff.

I have read and understand the rules and requirements of accessing information on the Internet. I agree to abide by the rules and I further understand that any violation of the rules is unethical and may constitute a criminal offense. I understand that all network activity is being monitored. This includes, but is not limited to, the use of the Internet, files I create and/or save and e-mails sent or received. I understand that technological resources are provided by the school district solely for the purpose of supporting me in my role as a DCSD employee. I understand I am responsible for any activity on my computer. If I am not physically at my computer, it will not be logged in with my credentials. I understand it is my responsibility to monitor students under my supervision any time they are using technology tools. Should I commit any violation, my access privileges may be revoked. Disciplinary and/or appropriate legal action may also be taken.

_____   _____
Employee signature   Date

_____
Location

This form is to be completed annually by every employee.
Principals and Supervisors are responsible for maintaining signed copies of these forms.

DARLINGTON
COUNTY SCHOOL DISTRICT

DIGITAL CITIZENSHIP CONTRACT – IJNDB-E (5)

CODE OF CONDUCT

Proper behavior, as it relates to the use of technology, is no different than proper behavior in all other aspects of district activities. All users are expected to use the district technology resources in a legal, responsible, ethical, and polite manner. The Digital Citizenship Guidelines are intended to clarify those expectations as they apply to computer and network usage and are consistent with the Darlington County School Board Policy on Use of Technology Resources in Instruction (Policy IJNDB). A student who knowingly violates any portion of the Digital Citizenship Expectations will be subject to suspension of access and/or revocation of privileges on the District's system and will be subject to disciplinary action in accordance with the school district disciplinary handbook.

1. Students will practice responsible use of digital information regarding intellectual property including complying with software licenses, copyright laws, and all other state and federal laws governing intellectual property. See district fair use and copyright guidelines for more information (Policy EGAD). Students will practice safe and appropriate online behavior including using professional etiquette while communicating online. Improper use of district technology resources is prohibited including but not limited to:
    A. Using racist, profane, pornographic, sexually oriented, or obscene language or materials
    B. Attempting to send or sending anonymous messages of any kind
    C. Using the network to access inappropriate and / or harmful materials
    D. Bypassing the district's security measures to access sites that are filtered on the district network
    E. Encrypting communications so as to avoid security review or monitoring by the system administrator.
    F. Using the network to provide addresses or other personal information that others may use inappropriately.
    G. Purposely engaging in activity that may: harass, threaten, defame, slander, libel, malign, or abuse another (i.e., individual or group).
    H. Forgery or attempted forgery of electronic messages is prohibited. Attempts to read, delete, copy, or modify the electronic mail of other system users or deliberate interference with the ability of other system users to send/receive electronic mail is prohibited.
    I. Using the network for illegal purposes, in support of illegal activities, or for any other activity prohibited by district policy or guidelines
2. Students will use the technology resources in a positive and responsible manner that promotes creativity & innovation, collaboration, communication, critical thinking & problem solving. Improper use of the district's technology resources is prohibited including but not limited to:
    A. Using the network for political activity, financial gain, or commercial activity
    B. Attempting to harm or harming equipment, materials or data
    C. Changing any computer configurations and/or settings.
    D. Installing software, including freeware and file sharing services, without permission from permission from the Director of Technology or designee.
    E. Deliberate attempts to degrade or disrupt system performance may be viewed as violation of district guidelines and possibly, as criminal activity under applicable state and federal laws, including the South Carolina Code of Laws, Computer Crimes Act, Title 16 Chapter 16. This includes, but is not limited to, the uploading or creating of computer viruses, malware or spyware.
    F. Streaming media, such as radio, games, video, etc., for non-educational purposes
    G. Proxy sites - Attempting to bypass or bypassing, the filtering device by using sites such as but not limited to proxy sites on the district's electronic communications system
    H. Running security programs or utilities that reveal or exploit weaknesses in the security of a system such as password cracking programs, packet sniffers, or port scanners or any other non-approved programs on district technology resources
    I. Otherwise engaging in acts against the aims and purposes of the district as specified in its governing documents or in rules, regulations and procedures adopted from time to time
3. Students will understand the negative impact of inappropriate technology use including online bullying and harassment, hacking, intentional virus setting, invasion of privacy, and piracy such as software, music, video and other media.

4. Students will login to the district network using their own login credentials. Account information and passwords, or similar information used for identification and authorization purposes, must be kept private. Passwords should not be written down and left in a location others may find it. The individual in whose name a system account is issued will be responsible at all times for its proper use.

5. In order to help preserve both privacy and security, neither still photography nor video capturing is allowed on campus unless directed by a member of a faculty member to meet an educational goal or approved by an authorized member of the administration, faculty or staff. Both behavioral and legal action may be taken against individuals not respecting the privacy and security rights.

6. Students will use technology resources cautiously to prevent damage.

7. System users must maintain their personal files including backing up files and deleting outdated files on a regular basis.

8. Students are asked to conserve district technology resources (such as network bandwidth and storage) by limiting usage to educational purposes. System users must not: degrade the performance of district technology resources (i.e. streaming video, streaming audio, and Internet radio); deprive an authorized district user access to a district resource; obtain extra resources beyond those allocated; circumvent district computer security measures.

9. Creative Credit and Copyright. Students have the right to protect their own creative works. Additionally, students must exercise academic integrity in a fair and legal manner when using other people's creative works. Failure to appropriately cite ideas or work other than your own will result in adverse academic and behavioral action. Academic integrity protects against the following:

   A. *Cheating* is fabricating written assignments; giving or receiving aid to another student without the consent of the instructor on tests, quizzes, assignments, exams; unauthorized accessing of teacher's editions or answer keys. Cheating also includes the use of technology such as computers, phones, cameras, or any other device that provides access to unauthorized information related to graded course material, tests, quizzes, assignments or examinations.

   B. *Double Assignments* are also a form of cheating. This is defined as an assignment that is used to fulfill the requirements of more than one course without prior approval from all involved instructors.

   C. *Colluding* is allowing one's work to be copied or submitted by another student. This applies to individual as well as group work where the students are given individual grades. It also applies to work that is transferred electronically and then submitted by another student. Joint student projects where information is combined for a final product submission are acceptable.

   D. *Plagiarizing* is the act of presenting the ideas or works of another person as one's own. This includes presenting information, ideas, phrasing, words, artwork, music, figures, diagrams, graphs, song lyrics, films, maps, illustrations, data, computer programs, emails, CDs, and electronic files from the Internet. All of these must be acknowledged with the proper documentation. Consult your instructor or the school links for proper citation practices. All assignments submitted to instructors should contain the proper citation. Plagiarism occurs when a student does one of the following: 1) fails to cite borrowed, quoted or paraphrased material, even by accident 2) deliberately intends to deceive through lack of citation 3) Uses strings of words from a cited source without indicating these words are not his own (attempted paraphrase without quotations, even if there is a correct citation)

   E. Carelessly or inaccurately citing quoted or paraphrased material is not plagiarism. This type of error is attributed to style or formatting. For example, if you submit a MLA works cited instead of an APA, then this is an inaccurate citation. You may lose style or formatting points; however, it is not plagiarism.

We have read and fully understand the responsibilities and consequences outlined the Darlington County School District Digital Citizenship Contract. We agree to the above rules and conditions of the Digital Citizenship Contract. We have discussed the importance of this policy and understand the expectations, responsibilities, and possible consequences associated with the misuse of any technological device at school or school related events.

_____   _____
Student Name (Printed)   Parent/Guardian Name (Printed)

_____   _____
Student Signature   Parent/Guardian Signature

_____   _____   _____
Grade   Academic Advisor   Date

DIGITAL RIGHTS – IJNDB-E(6)

In Darlington County School District (DCSD), we work hard to ensure the following digital rights for all of our students.

1. Each student shall have access to current, updated, and fully functioning technologies to be used in the learning process.

2. Each student shall be given access to his or her Darlington County School District (DCSD) username and password.

3. Each student shall be taught how to access resources such as DCSD Student Portal, Gmail and Google Drive, and learning management system (LMS) accounts connected to his or her DCSD account.

4. Each student shall attend classes led by teachers who continuously blend technology into learning and assessment activities.

5. Each student shall have spaces in the building that support individual technology use before, during, and after the school day.

6. Each student shall be supported as he or she learns how to productively incorporate personal technology into the learning process.

7. Each student shall be offered ongoing workshops and educational opportunities to learn how to better blend technology into the learning process.

8. Each student shall have the opportunity to use social media or other online collaborative tools in the learning process.

9. Each student shall enjoy educational experience that is free from any form of cyber bullying, harassment or threats.

CODE OF CONDUCT

Proper behavior, as it relates to the use of technology, is no different than proper behavior in all other aspects of district activities. All users are expected to use the district technology resources in a legal, responsible, ethical, and polite manner. The Digital Citizenship Guidelines are intended to clarify those expectations as they apply to computer and network usage and are consistent with the Darlington County School Board Policy on Use of Technology Resources in Instruction (Policy IJNDB). A student who knowingly violates any portion of the Digital Citizenship Expectations will be subject to suspension of access and/or revocation of privileges on the District's system and will be subject to disciplinary action in accordance with the school district disciplinary handbook.

1. Students will practice responsible use of digital information regarding intellectual property including complying with software licenses, copyright laws, and all other state and federal laws governing intellectual property. See district fair use and copyright guidelines for more information (Policy EGAD). Students will practice safe and appropriate online behavior including using professional etiquette while communicating online. Improper use of district technology resources is prohibited including but not limited to:

   A. Using racist, profane, pornographic, sexually oriented, or obscene language or materials

   B. Attempting to send or sending anonymous messages of any kind

   C. Using the network to access inappropriate and / or harmful materials

   D. Bypassing the district's security measures to access sites that are filtered on the district network

   E. Encrypting communications so as to avoid security review or monitoring by the system administrator.

   F. Using the network to provide addresses or other personal information that others may use inappropriately.

   G. Purposely engaging in activity that may: harass, threaten, defame, slander, libel, malign, or abuse another (i.e., individual or group).

   H. Forgery or attempted forgery of electronic messages is prohibited. Attempts to read, delete, copy, or modify the electronic mail of other system users or deliberate interference with the ability of other system users to send/receive electronic mail is prohibited.

   I. Using the network for illegal purposes, in support of illegal activities, or for any other activity prohibited by district policy or guidelines

2. Students will understand the negative impact of inappropriate technology use including online bullying and harassment, hacking, intentional virus setting, invasion of privacy, and piracy such as software, music, video and other media

3. Students will use technology resources cautiously to prevent damage.

4. System users must maintain their personal files including backing up files and deleting outdated files on a regular basis.

5. Students will use the technology resources in a positive and responsible manner that promotes creativity & innovation, collaboration, communication, critical thinking & problem solving. Improper use of the district's technology resources is prohibited including but not limited to:

A. Using the network for political activity, financial gain, or commercial activity

B. Attempting to harm or harming equipment, materials or data

C. Changing any computer configurations and/or settings.

D. Installing software, including freeware and file sharing services, without permission from permission from the Director of Technology or designee.

E. Deliberate attempts to degrade or disrupt system performance may be viewed as violation of district guidelines and possibly, as criminal activity under applicable state and federal laws, including the South Carolina Code of Laws, Computer Crimes Act, Title 16 Chapter 16. This includes, but is not limited to, the uploading or creating of computer viruses, malware or spyware.

F. Streaming media, such as radio, games, video, etc., for non-educational purposes

G. Proxy sites - Attempting to bypass or bypassing, the filtering device by using sites such as but not limited to proxy sites on the district's electronic communications system

H. Running security programs or utilities that reveal or exploit weaknesses in the security of a system such as password cracking programs, packet sniffers, or port scanners or any other non-approved programs on district technology resources

I. Otherwise engaging in acts against the aims and purposes of the district as specified in its governing documents or in rules, regulations and procedures adopted from time to time

6. Students will log into the district network using their own login credentials. Account information and passwords, or similar information used for identification and authorization purposes, must be kept private. Passwords should not be written down and left in a location others may find it. The individual in whose name a system account is issued will be responsible at all times for its proper use.

7. In order to help preserve both privacy and security, neither still photography nor video capturing is allowed on campus unless directed by a member of a faculty member to meet an educational goal or approved by an authorized member of the administration, faculty or staff. Both behavioral and legal action may be taken against individuals not respecting the privacy and security rights.

8. Students are asked to conserve district technology resources (such as network bandwidth and storage) by limiting usage to educational purposes. System users must not: degrade the performance of district technology resources (i.e. streaming video, streaming audio, and Internet radio); deprive an authorized district user access to a district resource; obtain extra resources beyond those allocated; circumvent district computer security measures.

9. **Creative Credit and Copyright**. Students have the right to protect their own creative works. Additionally, students must exercise academic integrity in a fair and legal manner when using other people's creative works. Failure to appropriately cite ideas or work other than your own will result in adverse academic and behavioral action. Academic integrity protects against the following:

A. *Cheating* is fabricating written assignments; giving or receiving aid to another student without the consent of the instructor on tests, quizzes, assignments, exams; unauthorized accessing of teacher's editions or answer keys. Cheating also includes the use of technology such as computers, phones, cameras, or any other device that provides access to unauthorized information related to graded course material, tests, quizzes, assignments or examinations.

B. *Double Assignments* are also a form of cheating. This is defined as an assignment that is used to fulfill the requirements of more than one course without prior approval from all involved instructors.

C. *Colluding* is allowing one's work to be copied or submitted by another student. This applies to individual as well as group work where the students are given individual grades. It also applies to work that is transferred electronically and then submitted by another student. Joint student projects where information is combined for a final product submission are acceptable.

D. *Plagiarizing* is the act of presenting the ideas or works of another person as one's own. This includes presenting information, ideas, phrasing, words, artwork, music, figures, diagrams, graphs, song lyrics, films, maps, illustrations, data, computer programs, emails, CDs, and electronic files from the Internet. All of these must be acknowledged with the proper documentation. Consult your instructor or the school links for proper citation practices. All assignments submitted to instructors should contain the proper citation. Plagiarism occurs when a student does one of the following: 1) fails to cite borrowed, quoted or paraphrased material, even by accident 2) deliberately intends to deceive through lack of citation 3) Uses strings of words from a cited source without indicating these words are not his own (attempted paraphrase without quotations, even if there is a correct citation.

E. Carelessly or inaccurately citing quoted or paraphrased material is not plagiarism. This type of error is attributed to style or formatting. For example, if you submit a MLA works cited instead of an APA, then this is an inaccurate citation. You may lose style or formatting points; however, it is not plagiarism

Students and parents will be expected to sign a Digital Citizenship Contract.

Responsibilities and Expectations

Students:

- Are required to abide by the Acceptable Use Policy.

- Will receive a laptop as an educational tool and it should only be used in that capacity.

- Must attend or have attended a designated training program.

- Are responsible for the care of the laptop issued to them whether in or out of school.

- Are responsible for ensuring the laptop is charged and ready for use every day.

- Are responsible for bringing the assigned laptop to school each day. A computer that is left at home will be treated the same as if textbooks or homework were left at home. **NO SPARE**

- Are given a power cord and laptop bag and must carry the laptop in the school issued bag. If the power cord or bag is lost, damaged, or stolen, the student will pay for a new one.

- Will lose laptop privileges if the student is responsible for any vandalism, hacking, network disruption, or any actions that disable, damage, or ***negatively*** affect the laptop or network in any way.

- Will only use software that is permitted and installed by the school district.

- Will back up all data and have files stored in at least two locations.

- Acknowledge there is no expectation of privacy with files stored on the computers or with websites visited with the laptops. The school district has the right to monitor laptops and/or block access to applications and websites.

- Will NOT loan/borrow laptop, power cord, or bag to/from other students and will NOT share usernames and passwords.

- ***Will NOT deface laptop by writing on or placing stickers on the outside surfaces. The preferred method of protection is a case that can be purchased for a nominal fee at the school.***

- ***Will report damages IMMEDIATELY to the Media Specialist or designated school personnel.***

- Will return the laptop, bag, and power cord at the end of the school year in clean and good condition. Laptops will be re-distributed to students at the start of the following school year.

Warranty and Damage Protection Information

Warranty Information
All laptops are covered by the manufacturer's warranty for malfunction due to manufacturing or non-performance issues. The warranty does not cover damage that is determined to be accidental, the result of negligent use or treatment; nor does it cover outright loss or damage of the laptop, power cord, or batteries through inattention or negligence

Negligence
Warranty coverage and damage insurance do not cover damages that are determined to be caused by negligent use/treatment, nor do they cover the power cord, battery, or laptop bag. **When the administration determines that damage was caused by negligent actions, the student or parent/guardian will be responsible for all costs.**   A temporary computer will be provided when a $200 deposit is received.

Accidental Damage Protection
Accidental Damage Protection (ADP) will cover any accidental damage that occurs to the laptop up to the total value of the laptop but does not cover the laptop bag, battery, or power cord. **Accidental damage protection WILL NOT cover liquid damage, loss or theft. Payments can be submitted in cash or by money order payable to the Darlington County School District. Money orders must be signed and must show the student's name in the memo section. This form MUST be signed by student AND parent. Completed form and payment MUST be submitted before laptop will be issued.**

Reporting Procedure
Damage must be reported immediately to the Media Specialist. If the damage is determined to be accidental, a damage claim will be processed and an invoice will be sent to the parents. A spare laptop will be provided until the student's laptop is repaired. A police report must be filed to process a theft claim.

Last Name_____   First Name_____   Middle Name_____
Called_____   Grade_____
Please check one of the following:

I am purchasing accidental damage protection provided by the DCSD.
If damage occurs, ***repair costs will be assessed as identified below***. Accidental damage protection will cover 1 broken screen ($25 deductible). **Accidental damage protection WILL NOT cover liquid damage, loss or theft.**
   Non-refundable Fee:

_____$50 per year

_____$25 per year for students with financial need*

_____
Student Signature

_____
Parent Signature

_____
Date

2017-18 *REPAIR FEES*	
2nd or more Broken Screen	*$250*
Broken Trackpad	*$100*
Liquid Damage	*$800*
Loss or Theft	*$900*
Other	*50% of the charge to repair*

**Your signature indicates you agree to abide by all responsibilities listed in this form.
All students must submit this form each year no matter which option is selected.**

FOR OFFICE USE ONLY

Payment Date: _____   Payment Type: ☐   Cash   ☐   Money Order

Received By: _____