

# **Information Technology**

## **Overview**

The Information Technology (IT) operations provide technical support and oversight for the school's technology infrastructure along with managing the data needed to support administrative decision making and Federal and State reporting requirements for performance based goals and objectives.

The physical infrastructure includes all personal computers and peripherals, all laptop computers and peripherals, all Chromebooks and peripherals, network servers, wiring, network design, and Internet access. The software component encompasses operating system software for PC's and the network, personal productivity software, application specific software needed by individual curriculums, along with the school's student management information system and grade book reporting applications.

The IT operations continually focuses on improving the delivery and reliability of these services to its member community by assessing the effectiveness of the current environment in relation to the needs of a 21st century learning environment with respect to how well it meets the ever-evolving needs of teachers, students, and administrative/support staff.

# 1:1 Program Student Responsibilities

## 1.1 Authority

The William M. Davies, Jr. Career & Technical High School (Davies) 2017-2020 Strategic/School Improvement Plan envisions a technology enhanced teaching and learning environment for all students and educators. To that end, Davies will distribute a Chromebook to every student in grades 9-12. It is the school's intent that students will have access to high quality blended learning opportunities so that they have more control over the pace, space, and content of their learning.

## 1.2 Policy

Students are expected to demonstrate appropriate and responsible technology use that enhances, rather than detracts from, teaching and learning.

The students, along with their parents/guardians' support and oversight, recognize the following:

- Chromebooks are to be used for educational purposes only
- Davies retains ownership of the device and any peripheral components such as its case and power cord
- Davies retains ownership of the student issued Google Apps accounts
- Davies can access a student's account if there is a school related issue or technical problem
- Davies will NOT remotely access the Chromebook camera or microphone at ANY time
- Students will keep their passwords private, with the exception of parents/guardians
- Students will be the only person to use the Chromebook assigned to them
- Students will respect and protect themselves and others online
- Students will respect and protect what belongs to them and others
- Students will responsibly care for the Chromebook and peripherals assigned to them
- Students will only be able to download school approved apps or extensions
- Students will NOT tamper with or remove any asset tags from Chromebooks or peripherals
- Chromebooks may be brought home during the year, but students are expected to return them to Davies if they leave the school or at the end of the school year
- Students are expected to charge their device at home and bring it to school fully charged

- Chromebooks will be filtered in accordance with the [Children's Internet Protection Act \(CIPA\)](#) even when they are used outside of school
- Chromebooks are to be kept in their protective cases at all times and secured in lockers when not needed in class
- Cases do not prevent damage so students are expected to treat them with care
  - Always carry the Chromebook with a closed lid
  - Be sure there is never anything, like a pen or pencil on the keypad before closing the lid
- Keep Chromebooks away from all food, drinks, and pets
- Students and parents/guardians must agree to and sign off on all relevant policies prior to receiving a device
- Students and/or parents/guardians will be responsible for repeated damage, neglect, lost or stolen Chromebooks
- Optional insurance will be available for purchase

# Employee Internet Acceptable Use Policy

## 1.1 Authority

The William M. Davies, Jr. Career & Technical High School (Davies) Acceptable Use Policy (Employee AUP) defines acceptable practices for the use of Davies Internet Services. Its purpose is to inform employees about the risks of using the Internet, and provide rules for ethical and legal Internet and computer use. Its goals are to provide guidance for inappropriate Internet behavior and to encourage polite communication.

## 1.2 Definitions

**Davies Network** - All equipment, systems, facilities, and Internet Services and products used.

**Ethical** - Pertaining to or dealing with morals or the principles of morality; pertaining to right or wrong in conduct.

**Pirated Software** - Unauthorized copying of computer software.

**Virus, Worm, Trojan** - Malicious programs that can cause damage to your computer.

## 1.3 Policy

By using the Internet Service, you acknowledge that you and users that have gained access to the Internet Service through your account (Users) are responsible for full compliance with the Policy. You are also responsible for violations of this Policy by any User that accesses the Internet Service through your account. The Policy applies to all aspects of the Internet Service. This Policy is designed to assist in protecting the Davies Network, the Internet Service, our Users and the Internet community as a whole from improper and/or illegal activity over the Internet.

### Acceptable Uses

The school's Information Technology resources, including Internet access and video communications, are provided for educational purposes. All Davies computer and network equipment is available for the use of Davies employees to perform their assigned tasks. These tasks include, but are not limited to:

- Interschool communication
- Creation and storage of material for school or employee use

- Communication with outside sources
- Research
- Production of material required for daily work and/or completion of assigned tasks

Employees must:

1. Respect and protect the privacy of others
  - a. Use only assigned accounts
  - b. Protect the confidentiality of your account information
2. Respect and protect the integrity, availability, and security of all electronic resources
  - a. Observe all network security practices, as posted
  - b. Report security risks or violations, including the unauthorized use of your account information to the network administrator
  - c. Conserve, protect, and share these resources with other Internet users
3. Respect and protect the intellectual property of others
  - a. Follow the stipulations of all accepted End User License Agreements
  - b. Honor all copyright protections
4. Respect and practice the principles of community
  - a. Communicate only in ways that are kind and respectful
  - b. Report threatening or discomforting materials to the network administrator

### **Unacceptable Uses**

The lists below are by no means exhaustive, but attempt to provide a framework for activities which fall into the category of unacceptable use. Any other inappropriate activity or abuse of the Internet Service (as determined by us in our sole discretion), whether or not specifically listed in this Policy is strictly prohibited.

Employees must not:

1. Disrespect the privacy of others
  - a. View, use, or copy passwords, data, or networks to which they are not authorized
  - b. Distribute private information about others or themselves
2. Disrespect or ignore the integrity, availability, and security of all electronic resources
  - a. Destroy or damage data, networks, or other resources that do not belong to them, without clear permission of the owner
  - b. Introduce malicious programs or data into the network or server (ie. viruses, worms, Trojan horses, etc.)
  - c. Effect security breaches, cause any disruptions of network communication, or execute any form of unauthorized network monitoring

- d. Circumvent user authentication or security of any firewall, filter, host, network or account
  - e. Intentionally delete or alter another user's work
  - f. Attempt to fraudulently conceal, forge or otherwise falsify a User's identity in connection with use of the Internet Service
3. Disrespect or disregard the intellectual property of others
- a. Infringe copyrights (no making illegal copies of music, games, movies, photographs, or other software)
  - b. Distribute or install pirated software
  - c. Plagiarize
4. Disrespect or ignore the principles of community
- a. Intentionally access, transmit, copy, or create material that violates the school's code of conduct (such as messages that are pronographic, threatening, rude, discriminatory, or meant to harass)
  - b. Intentionally access, transmit, copy, or create material that is illegal (such as obscenity, stolen materials, or illegal copies of copyrighted works)
  - c. Use the resources to further other acts that are criminal or violate the school's code of conduct
  - d. Buy, sell, advertise, or otherwise conduct business, unless approved as a school project
  - e. Provide information about, or lists of Davies employees, faculty or staff to any parties especially parties outside of Davies
  - f. Download and save images or pictures to the desktop as backgrounds or screensavers that are not appropriate for the classroom setting

### **Wireless Equipment**

Davies employees are prohibited from the unauthorized use of personal laptops and may not install cellular or wireless equipment/antennae on the Davies premises without prior written permission from the Davies IT Coordinator.

### **1.4 Violations/Sanctions**

#### **Suspension or Termination of Internet Service**

Violations of these rules may result in disciplinary action, including the loss of an employee's privileges to use the school's information technology resources.

## **1.5 Disclaimer**

Davies assumes no liability for any direct or indirect damages arising from the User's connection to the Internet. Davies is not responsible for the accuracy of information found on the Internet and only facilitates the accessing and dissemination of information through its systems. Users are solely responsible for any material that they access and disseminate through the Internet. Because the Internet is an inherently open and insecure means of communication, any data or information a User transmits over the Internet may be susceptible to interception and alteration and should not be considered private and secure. We encourage you to use your Internet access responsibly. Should you have any questions regarding this Employee Internet Acceptable Use Policy, please contact Davies Administration for more information.

### **Monitoring & Filtering**

Davies may monitor any Internet activity occurring on school equipment or accounts to help ensure that uses are secure and in compliance with this policy. Davies uses filtering software to limit access to sites on the Internet. Administrators reserve the right to examine, use, and disclose any data found on the school's information networks in order to further the health, safety, discipline, or security of any employee or other person, or to protect property. They may also use this information in disciplinary actions, and will furnish evidence of crime to law enforcement.

### **Modifications to Policy**

Davies reserves the right to modify this Policy at any time without notice. We will attempt to notify our users on any such modifications either via an electronic communication to employees or by posting a revised version of the Policy on our Website.

# Help Desk/IT Work Order Policy

## 1.1 Authority

The William M. Davies, Jr. Career & Technical High School's (Davies) Help Desk was created in order to assist faculty and staff who require assistance with school-related technology.

## 1.2 Definitions

**HelpDesk (eHD)** is a software package that is installed on all Davies-owned technical devices. This software is meant to improve work flow and better manage IT resources, along with an anticipated reduction in service level response times.

## 1.3 Policy

Anyone wishing to receive support from the IT Department must open a ticket in this system before any technical resources will be assigned to work on the issue. Support requests include, but are not limited to: hardware issues, software issues, Internet problems, network problems, slow response times, equipment moves, quote requests, report requests, virus issues, printing problems, network access, account creation and/or deletion, data concerns, etc. Tickets can be created manually by the person requesting support.

The IT Department will no longer accept paper based support requests, phone calls, voice mail messages, emails, or hallway conversations as a legitimate request for support. Any requests received in this fashion will not be acted upon until the proper procedure has been followed.

## 1.4 Procedure

Once a ticket has been opened, the individual requesting technical assistance will receive an email from the eHD system. Users may track the status of their tickets by logging into the system directly. Please refer to the next section for instructions on how to access this system.

### *Creating Your Own Ticket*

The everything HelpDesk application will be used to open a new ticket or to track the status of an existing ticket. To access the eHD application, click on the "Help Desk" icon. A copy of this icon may be copied to your desktop from the SCH\_DOCS folder. In the event that your icon



disappears or becomes corrupted, you can replace it in the same manner. Your login credentials are the same as your network user id and password.

This system also has a Knowledge-Base (KB) feature which the IT department hopes will become an additional resource for you in time. The Knowledge-Base can be populated with resolutions to in-house tickets, responses to Frequently Asked Questions and/or filled with article, tips, suggestions, ideas, etc. from industry trends, best practices, colleagues or other sources to assist with technology related concerns. Please submit any suggestions for Knowledge-Base content to the IT Coordinator. You do not need to log into the eHD system in order to access the KB, simply launch the program and select the Search Knowledge-Base link from the home page.

For step-by-step instructions on how to create and track your own tickets, please refer to the everything HelpDesk End User Files PDF, located in the SCH\_DOCS\Help Desk folder. The eHD system has been pre-populated for you with drop down selections available for key fields such as Location, Group, Category, Category Option, and Room Number. Please be as descriptive as possible when requesting service or reporting problems. The system can accept attachments for additional information such as capturing screenshots, error logs, or files.

# Portable Computing Policy and Equipment Use Agreement

## 1.1 Authority

William M. Davies, Jr. Career & Technical High School (Davies) provides portable electronic devices (laptops, iPad, Chromebooks, etc) for employee use. The use of mobile technology will help to enhance the learning process and increase employee productivity. Certain guidelines are necessary to protect Davies' hardware as well as protect the security of the school's networks. This policy is to be used in addition to the [Employee Internet Acceptable Use Policy](#).

## 1.2 Policy

All employees of Davies must agree to the following when issued a school-owned portable electronic device:

1. The employee agrees to follow all school regulations and policies governing the use of electronic devices as well as all applicable State and Federal laws including copyright and intellectual property laws pertaining to software and information.
2. The employee shall not remove or alter any school or State identification labels attached to or displayed on the device, nor shall the employee change identification within the device, such as the device name.
3. The school will keep an inventory and log of employee electronic device assignments. The use of this equipment is for school educational initiatives and district school business. Therefore, only software purchased directly by Davies or obtained by Davies through grant funding may be installed on these devices. This included applications uploaded to iPads and other portable devices.
4. All software must be installed by Davies IT personnel. Illegal use or transfer of copyrighted materials is prohibited using school owned devices.
5. The user will not attempt to enable the fingerprint identification feature (if it exists) nor will the user change any other security settings.
6. No unauthorized network access is allowed and/or personal devices cannot be connected to the school's network.
7. Portable devices will be allowed to connect to the Internet, but no other school network resources, due to network security issues. Therefore, to backup important files, users will need to save files to an external storage device (USB drive or CD). Once files are saved to an external storage device, users can copy these files to the school network or to their home computer as a backup copy. This is important, since devices may need to

be re-imaged when they are updated and any files saved to the local drive of the device will be lost.

8. The employee agrees to handle the device carefully and protect it from potential sources of damage. Should loss, damage or destruction of the loaned equipment occur the employee must immediately notify the IT Department.
9. Upon request, the employee agrees to deliver the device to the IT staff for technical inspection or to verify inventory or other information; this may include random screening.

# Responsible Use of Technology Policy

## 1.1 Authority

William M. Davies, Jr. Career & Technical High School (Davies) provides technologies and access to those technologies to staff and students to engender a more enriching educational experience. By using the Internet Service, you acknowledge that you and users that have gained access to the Internet Service through your account (Users) are responsible for full compliance with the policy. You are also responsible for violations of this policy by any User that accesses the Internet Service through your account. The policy applies to all aspects of the Internet Service.

## 1.2 Definitions

**Davies Network** refers to all equipment, systems, facilities, Internet Services, and products used by and for Davies staff and students.

**PEDs** refers to Personal Electronic Devices

## 1.3 Policy

This policy is designed to assist in protecting the Davies Network, the Internet Service, our Users and the Internet community as a whole from improper and/or illegal activity over the Internet whether it be through the use of any Davies equipment or PEDs used within the Davies building or as a representation of Davies with the use of Davies Network or any private Internet provider.

## 1:1 Program

Davies 1:1 Program provides a chromebook to all students grades 9-12 for their educational use while both at school and at home. Students will be required to care for their registered device properly while it is assigned to them. They are required to return their device at the end of the school year or at the termination of their enrollment. Students returning the following year will be reissued the same device registered to them. Students will be invoiced for the replacement cost of any equipment they fail to return. If items are returned in a damaged or defective state, students may also be billed for parts needed to repair the device or item. Students unable to comply with all policies and responsibilities associated with technology use at Davies may lose temporary or permanent access to all technology and forfeit possession of student

chromebook, which does not absolve students from full responsibility of completing all school work through alternative methods assigned by classroom teachers.

### **Acceptable Uses**

The school's Information Technology resources, including Internet access, are provided for educational purposes. All Davies computer and network equipment is available for the use of Davies staff, students and guests to perform their assigned tasks. PEDs may be permissible in approved settings to complete classroom tasks, also. These tasks include, but are not limited to:

- Interschool communication
- Creation and storage of material for school or User use
- Communication with outside sources
- Research
- Production of material required for class work and/or completion of assigned tasks

Users must always employ Network Etiquette (Netiquette) as follows:

1. Respect and protect the privacy of others
  - a. Use only assigned accounts
  - b. Protect the confidentiality of your account information
2. Respect and protect the integrity, availability, and security of all electronic resources
  - a. Observe all network security practices, as posted
  - b. Report security risks or violations, including the unauthorized use of your account information to a teacher or network administrator
  - c. Conserve, protect, and share these resources with other staff, students and Internet users
3. Respect and protect the intellectual property of others
  - a. Follow the stipulations of all accepted End User License Agreements
  - b. Honor all copyright protections
4. Respect and practice the principles of community
  - a. Communicate only in ways that are kind and respectful
  - b. Report threatening or discomfoting materials to a teacher

### **Unacceptable Uses**

Equipment use and network access is a privilege, not a right. Inappropriate use of the equipment and the network by a student will result in disciplinary action up to and including suspension, cancellation of student user privileges, and/or legal action (criminal and/or civil) in accordance with the law and the Davies policy. All Users will be held accountable for inappropriate use. Users must follow appropriate online behavior at all times, including interacting with other individuals on social networking websites and in chat rooms.

Cyberbullying will not be tolerated. The following uses of the network are considered unacceptable by Davies.

1. Personal Safety

- a. Users may not post, use, or store personal contact information about themselves or other people when using electronic communication forms, such as but not limited to email, chat rooms, or social media sites. Personal contact information includes the User's address, telephone, social security number, or other personal data, or school address.
- b. Users may not provide information about Davies students, faculty, staff, or guests to any parties inside or outside of Davies.
- c. Students will immediately disclose to their teacher or building administrator any message they receive that is inappropriate, makes them feel uncomfortable, or is threatening.
- d. All other users will immediately disclose to their supervisor or building administrator any message they receive that is inappropriate, makes them feel uncomfortable, or is threatening.

2. Illegal Activity

- a. Users may not post, submit, publish or display harmful or inappropriate material that is harassing, insulting, threatening, or attacking any individual, including prejudicial or discriminatory attacks or insults.
- b. Users may not access, transmit, copy, or create any material that violates the Davies code of conduct including pornographic material, obscene images, or vulgar communications.
- c. Users may not vandalize, misuse or harm, and/or steal computers, software, computer systems, or computer networks.
- d. Users may not participate in hacking activities or any form of unauthorized access to other accounts (online or site stored), computers, networks, or information systems.
- e. Users may not deliberately attempt to disrupt the computer system or destroy data by uploading, downloading, or creating computer viruses.
- f. Users may not use the system to engage in any other illegal act, such as arranging for illegal drug activities, purchasing of alcohol, engaging in gang activity, or threatening the safety of a person.

3. System Security

- a. Users are responsible for their individual account and may not reveal their personal computer log-on identification or those of other students or staff members.

- b. Students must immediately notify a teacher or other school employee if they have identified a security problem.
  - c. All other users must immediately notify their supervisor or building administrator if they identify a security problem.
  - d. Users may not download software to any computer unless instructed to do so by a teacher or building administrator.
  - e. The system may not be used to connect personal hardware such as iPods unless it is needed for educational purposes.
  - f. Users may not effect security breaches, cause any disruptions of network communication, or execute any form of unauthorized network monitoring.
  - g. Users may not circumvent user authentication or security of any firewall, filter, host, network or account.
  - h. Users shall not attempt to fraudulently conceal, forge or otherwise falsify a User's identity in connection with use of the Internet service.
4. Inappropriate Language and Behavior
- a. Users may not use obscene, profane, vulgar, inflammatory, threatening, disrespectful or other inappropriate language on the system. This includes use of Davies equipment and software and any use of the Internet.
  - b. User will not display inappropriate materials (ie. offensive messages or pictures, obscene language references, etc.) on the system. This includes use of Davies equipment and software and any use of the Internet. This also includes the use of any and all PEDs that gain access technology outside of the Davies network.
  - c. Users will not post, submit, or publish information that could cause damage or danger of disruption to Davies, the students or others.
5. Inappropriate Access to Materials
- a. Users may not use the system to access materials that are profane or obscene, that advocates illegal or dangerous acts, or that advocates violence or discrimination towards other (ie. hate literature).
  - b. If a student mistakenly accesses inappropriate information, they should immediately report it to their teacher. This may protect students from any claim that they have intentionally violated the policy.
  - c. All other users who mistakenly accesses inappropriate information should immediately report it to their supervisor or building administrator.
  - d. Messages relating to or in support of illegal, inappropriate activities are to be reported to a building administrator.
6. Respecting Resources
- a. Users should frequently delete unnecessary files from their network folders. This must be done at the end of every school year, at least.

- b. User will not engage in vandalism (ie. uploading/downloading inappropriate files, introducing computer viruses, disrupting the operation or the system through the abuse of hardware or software, modifying another person's files or data).
  - c. Users may not attempt to read, delete, copy, modify or forge the content of other Users' folders, files, electronic communications, or online accounts.
  - d. Students will subscribe to only high-quality discussion group mail lists that are relevant to education and/or career development.
  - e. Students will be supervised while accessing the Internet; however, they are still responsible for their proper use and access.
7. Plagiarism and Copyright Infringement
- a. Users will not plagiarize works that they find on the Internet. Plagiarism is adopting the ideas or writing of others and presenting them as your own.
  - b. Users must respect the copyright owners. Copyright infringement occurs when the User inappropriately reproduces a work that is protected by a copyright. If a student has a question about this, they should ask a teacher.
  - c. Copyrighted material may not be placed on the system without the author's permission. Users may download copyrighted material when used in academic work.
  - d. Users may not distribute or install pirated software onto the Davies network or technologies.
  - e. Users may not make illegal copies of music, games, movies, photographs, or other software made available through the Davies network or technologies.
8. Other Misuse
- a. Users shall not use Davies technology for commercial uses, including offering to sell or purchase products or services, advertise, or otherwise conduct business, unless approved as a school project.
  - b. Users shall not use Davies technology for games, entertainment, or personal non-education-related uses.
  - c. Users shall not use Davies technology for political campaigning, but it may be used for communication with elected representatives or expressing views on political issues.

#### **1.4 Disclaimer**

Davies assumes no liability for any direct or indirect damage arising from the User's connection to the Internet. Davies is not responsible for the accuracy of information found on the Internet and only facilitates the accessing and dissemination of information through its systems. Davies makes use of an Internet content filter to prevent access to sites with obscene, pornographic, or



harmful content. Given the nature of the Internet and the limitations of content filtering systems, it is impossible to block all inappropriate sites. If you believe the content filter is blocking access to appropriate sites, please contact the technology administrator. Users are solely responsible for any material that they access and disseminate through the Internet.

Because the Internet is an inherently open and insecure means of communication, any data or information a User transmits over the Internet may be susceptible to interception and alteration and should not be considered private or secure. We encourage you to use your Internet access responsibly. Should you have any questions regarding this *Responsible Use of Technology Policy*, please contact Davies Administration for more information.

Users should have no expectation of privacy when using Davies network or equipment. Davies reserves the right to inspect student folders, personal files, electronic communications, downloaded material, including deleted files from a User's computer, records of online activity and other information on the Davies network or equipment when necessary to ensure proper use of the system. Administrators reserve the right to examine, use, and disclose any data found on the school's information networks in order to further the health, safety, discipline, or security of any student or other person, or to protect property. They may also use this information in disciplinary actions and will furnish evidence of crime to law enforcement.

Davies will strive to protect User privacy; however, Davies will not be responsible for any damages (consequential, incidental or otherwise), which a User may suffer arising from access to or use of the Davies computers and computer network, including damages arising as a result of the actions of Davies. These damages include loss of data and delayed, lost or damaged electronic correspondence or files due to system or service provider interruptions and system shutdowns for emergency or routine maintenance of the system. Use or conveyance of information via Davies computer technology is at the User's own risk.

Davies reserves the right to modify this Policy at any time without notice. We will attempt to notify our Users of any such modifications either via an electronic communication to staff, parents, and students or by posting a revised version of the Policy on our Website.

# Student Internet Acceptable Use Policy

## 1.1 Authority

The William M. Davies, Jr. Career & Technical High School (Davies) Student Internet Acceptable Use Policy (Student AUP) defines acceptable practices for the use of Davies Internet Services. Its purpose is to inform students and parents about the risks of using the Internet, and provide rules for ethical and legal Internet and computer use. Its goals are to protect children from inappropriate Internet use behavior and to encourage polite communication.

## 1.2 Definitions

**Davies Network** - All equipment, systems, facilities, and Internet Services and products used.

**Ethical** - Pertaining to or dealing with morals or the principles of morality; pertaining to right or wrong in conduct.

**Pirated Software** - Unauthorized copying of computer software.

**Virus, Worm, Trojan** - Malicious programs that can cause damage to your computer.

## 1.3 Policy

By using the Internet Service, you acknowledge that you and users that have gained access to the Internet Service through your account (Users) are responsible for full compliance with the Policy. You are also responsible for violations of this Policy by any User that accesses the Internet Services through your account. The Policy applies to all aspects of the Internet Service. This Policy is designed to assist in protecting the Davie Network, the Internet Service, our Users and the Internet community as a whole from improper and/or illegal activity over the Internet.

### Acceptable Uses

The school's Information Technology resources, including Internet access, are provided for educational purposes. All Davies computer and network equipment is available for the use of Davies students to perform their assigned tasks. These tasks include but are not limited to:

- Interschool communication
- Creation and storage of material for school or student use
- Communication with outside sources

- Research
- Production of material required for class work and/or completion of assigned tasks

Students must:

1. Respect and protect the privacy of others
  - a. Use only assigned accounts
  - b. Protect the confidentiality of your account information
2. Respect and protect the integrity, availability and security of all electronic resources
  - a. Observe all network security practices, as posted
  - b. Report security risks or violations, including the unauthorized use of your account information to a teacher or network administrator
  - c. Conserve, protect, and share these resources with other students and Internet users
3. Respect and protect the intellectual property of others
  - a. Follow the stipulations of all accepted End User License Agreements
  - b. Honor all copyright protections
4. Respect and practice the principles of community
  - a. Communicate only in ways that are kind and respectful
  - b. Report threatening or discomforting materials to a teacher

### **Unacceptable Uses**

The lists below are by no means exhaustive, but attempt to provide a framework for activities which fall into the category of unacceptable use. Any other inappropriate activity or abuse of the Internet Service (as determined by us in our sole discretion), whether or not specifically listed in this Policy is strictly prohibited.

Students must not:

1. Disrespect the privacy of others
  - a. View, use, or copy passwords, data, or networks to which they are not authorized
  - b. Distribute private information about others or themselves
2. Disrespect or ignore the integrity, availability, and security of all electronic resources
  - a. Destroy or damage data, networks, or other resources that do not belong to them, without clear permission of the owner
  - b. Introduce malicious programs or data into the network or server (ie. viruses, worms, Trojan horses, etc.)
  - c. Effect security breaches, cause any disruptions of network communication, or execute any form of unauthorized network monitoring

- d. Circumvent user authentication or security or any firewall, filter, host, network or account
  - e. Intentionally delete or alter another student's work
  - f. Attempt to fraudulently conceal, forge or otherwise falsify a User's identity in connection with use of the Internet Service
3. Disrespect or disregard the intellectual property of others
- a. Infringe copyrights (no making illegal copies of music, games, movies, photographs, or other software)
  - b. Distribute or install pirated software
  - c. Plagiarize
4. Disrespect or ignore the principles of community
- a. Intentionally access, transmit, copy, or create material that violates the school's code of conduct (such as messages that are pornographic, threatening, rude, discriminatory, or meant to harass)
  - b. Intentionally access, transmit, copy, or create material that is illegal (such as obscenity, stolen materials, or illegal copies of copyrighted works)
  - c. Use the resources to further other acts that are criminal or violate the school's code of conduct
  - d. Buy, sell, advertise, or otherwise conduct business, unless approved as a school project
  - e. Provide information about, or lists of Davies students, faculty or staff to any parties especially parties outside of Davies

### **Wireless Equipment**

Davies students are prohibited from the unauthorized use of personal laptop and may not install cellular or wireless equipment/antennae on the Davies premises without prior written permission from the Davies IT Coordinator.

### **1.4 Violations/Sanctions**

#### **Suspension or Termination of Internet Service**

Violations of these rules may result in disciplinary action, including the loss of a student's privileges to use the school's information technology resources. Please refer to the Student Handbook for a list of actionable offenses and their consequences.

## **1.5 Disclaimer**

Davies assumes no liability for any direct or indirect damages arising from the User's connection to the Internet. Davies is not responsible for the accuracy of information found on the Internet and only facilitates the accessing and dissemination of information through its systems. Users are solely responsible for any material that they access and disseminate through the Internet. Because the Internet is an inherently open and insecure means of communication, any data or information a User transmits over the Internet may be susceptible to interception and alteration and should not be considered private or secure. We encourage you to use your Internet access responsibly. Should you have any questions regarding this Student Internet Acceptable Use Policy, please contact Davies Administration for more information.

### **Monitoring & Filtering**

Davies may monitor any Internet activity occurring on school equipment or accounts to help ensure that uses are secure and in compliance with this policy. Davies uses filtering software to limit access to sites on the Internet. Administrators reserve the right to examine, use, and disclose any data found on the school's information networks in order to further the health, safety, discipline, or security of any student or other person, or to protect property. They may also use this information in disciplinary actions, and will furnish evidence of crime to law enforcement.

### **Modifications to Policy**

Davies reserves the right to modify this Policy at any time without notice. We will attempt to notify our users of any such modifications either via an electronic communication to parents and students or by posting a revised version of the Policy on our Website.