



# Guidelines for Responsible Computing

## The Acceptable Use/Internet Safety Policy for the Hopewell Valley Regional School District

### **Introduction**

The computing resources in the Hopewell Valley Regional School District support the instructional, research, and administrative activities of the school district. Examples of these computing resources include, but are not limited to, the administrative and instructional computing facilities and operations, local, wide and wireless networks, electronic mail, and access to the Internet. Users of these services and facilities have access to a vast amount of resources.

Consequently, it is appropriate for all users to behave in a responsible, ethical and legal manner. In general, appropriate use means respecting the rights of other computer users, the integrity of the physical facilities and all pertinent license and contractual agreements. Individual departments and schools may have additional guidelines regarding computing equipment held in those departments and schools. Interested parties should contact the K-12 Supervisor of Educational Technology for more information concerning computing guidelines in a specific department or school. The Hopewell Valley Regional School District vests the responsibility for ensuring the integrity and performance of its computing systems in various system administrators. While respecting the rights of all users, when the integrity of the system is threatened, systems administrators are authorized to take those actions necessary to maintain the responsible, ethical and legal use of Hopewell Valley Regional School District technology systems.

The guidelines apply to all users of computing resources owned or managed by the Hopewell Valley Regional School District, including faculty, staff, students, guests of the administration, and approved external individuals or organizations. When applied to students, it is understood that these signed guidelines will apply for the rest of the student's schooling in the Hopewell Valley Regional School District. Questions regarding the use and application of the Hopewell Valley Regional School District Guidelines for Responsible Computing are welcome. A meeting with the Educational Technology Supervisor, building principal and any other appropriate individuals can be scheduled to discuss the AUP and its use in the school district in further detail. Major changes to the Guidelines for Responsible Computing will be communicated to the school community via email and posting on the HVRSD website. The Guidelines for Responsible Computing will always be available via the HVRSD Technology Office website.

### **Account Security, Passwords, and Integrity**

The person to whom an account is allocated is the only person allowed to use that account. No password sharing is permitted. Additionally, it is the user's job to be sure he or she does not create a security hole in the system. For instance, users must select passwords that are not guessable or "breakable" and should not write the password down anywhere. Breakable passwords are ones found in any common dictionary, parts of the user's name, etc. The best passwords tend to be multiple words utilizing both numbers and characters.

The Hopewell Valley Regional School District provides reasonable security against intrusion and damage to files stored on district computers. The district provides some facilities for archiving and retrieving files specified by users and for recovering files after accidental loss of data. However, neither the Hopewell Valley Regional School District nor its computing staff can be held accountable for unauthorized access by other users, nor can they guarantee protection against power or media failure, fire, flood, or other disaster. The use of personal USB keys and other storage media are acceptable as long as their use doesn't violate other components of these guidelines.

### **Privacy**

The Hopewell Valley Regional School District participates in a range of computing networks and many members of the school district community regularly use these networked computers in their work. Statements in public files in this medium are protected by the same laws, policies, and guidelines, and are subject to the same limitations as communications in other media. The same holds true for personal electronic files and communications (e.g. email). However, users should exercise caution when committing confidential information via email because the confidentiality of such material cannot be guaranteed.

Network and system administrators are expected to treat the contents of electronic files as private and confidential and to respect the privacy of all users. Members of the computing staff are forbidden to log on to a user account or to access a

user's files unless the user gives explicit permission. An exception to these privacy guidelines may be made when an individual is suspected of abusing the Hopewell Valley Regional School District Guidelines for Responsible Computing. All accounts for staff and students are monitored for viruses, SPAM/malware and inappropriate files that could be used for malicious purposes and to ensure user privacy and safety. This is done through a combination of teacher and/or technology support activities and hardware and software installed on the networks. In such instances, the system administrator will immediately notify the district Supervisor of Educational Technology and/or the building principal.

### **Encountering Controversial Material**

Users may encounter material which is controversial and which users (parents, students, teachers, staff, and administration) may consider inappropriate or offensive. This is much more easily monitored and tracked on the Hopewell Valley Regional School District computing resources. A content filtering software application is utilized to minimize encounters of controversial material. The content filter blocks and filters Internet access to content, including audio and pictures that are (a) obscene; (b) pornographic; and (c) harmful to minors. If it is believed a website is blocked in error, please note this to district technical support personnel via the help desk. On a global network such as the Internet, it is impossible to control effectively all data and a user may inadvertently discover controversial material. It is the user's responsibility not to initiate access to such material.

### **Student Instruction Relative to the Guidelines for Responsible Computing**

All students K-12 who use Hopewell Valley Regional School District technology are provided age-appropriate instruction on all facets of the HVRSD Guidelines for Responsible Computing. That instruction will include: (a) access by minors to inappropriate matter on the Internet; (b) the safety and security of minors when using email and other forms of electronic communications and social media; (c) unauthorized access, "hacking," and other unlawful activities by minors online; (d) cyber bullying; and (e) social networking. Normal instructional procedure is to treat Internet safety instruction as not just a unit of instruction, but instruction that it is practiced and preached every day.

### **Personal Information**

No personal information of students, including photos, is to be shared and available online without parent consent. Parents are to complete the Publicity Consent Form. On this form, parents can give permission to (a) use technology resources as part of the student's instruction including Internet; (b) public releases from the school district that includes name, school, grade/teacher, performance role, name of course or activity, work product and/or photograph; (c) putting photo image and/or other personal identifiers as noted previously in (b).

Student information, including name, grade, student ID, school, teacher, and/or email address can be shared with third-party instructional technology resources that are to be used within the curriculum but are not publically viewable. An example of this is Study Island which is an online instructional and diagnostic tool that enables teachers to help students master the state standards in many content areas.

### **Appropriate Computer Behavior**

Those who avail themselves of the district computing resources are required to behave in their use of the technology in a manner consistent with the Hopewell Valley Regional School District's discipline policies as well as the Guidelines for Responsible Computing.

The following list does not cover every situation that pertains to proper or improper use of computer resources, but it does suggest some of the responsibilities that users accept if they choose to use a computer resource or the network access that the Hopewell Valley Regional School District provides.

1. If you have any computer account, you are responsible for the use made of that account. You should set a password which will protect your account from unauthorized use, and which will not be guessed easily. If you discover that someone has made unauthorized use of your account, you should change the password and report the intrusion to the Supervisor of Educational Technology, the technology support staff or a classroom teacher immediately. You should change your password on your account(s) on a regular basis to assure continued security of your account. You are to only use a computer account that belongs to you.
2. You must not intentionally seek information about, browse, obtain copies of, or modify files, passwords, or online content belonging to other people, whether in the Hopewell Valley Regional School District or elsewhere, unless specifically authorized to do so by those individuals. You must not attempt to decrypt or translate encrypted material to which you are not entitled. Nor may you seek to obtain system privileges to which you are not entitled. Attempts to do any of these things will be considered serious transgressions.
3. If you encounter or observe a gap in system or network security, you must report the gap to the Supervisor of Educational Technology, the technology support staff or a classroom teacher immediately. You must refrain from exploiting any such gaps in security.

4. You must refrain from any unauthorized action that deliberately interferes with the operating system, software functions of either individual workstations or of network servers and of the hardware infrastructure. This would include the creation and distribution of destructive and interfering programs such as worms and viruses as well as interfering with the wireless network operation.
5. You must be sensitive to the public nature of shared facilities, and take care not to display on screens in such locations images, sounds, or messages that could create an atmosphere of discomfort or harassment for others. You must also refrain from transmitting to others in any location inappropriate images, sounds or messages which might violate the Hopewell Valley Regional School District policies on harassment.
6. You must avoid the following activities: tying up shared computing resources for anything other than instructional applications and staff work requirements; sending frivolous or excessive email or messages locally or over the Internet; or printing excessive copies of documents, files, images or data. You must refrain from using unwarranted or excessive amounts of storage, printing documents or files numerous times because you have not checked thoroughly for all errors and corrections. You must be sensitive to special needs for software and services available in only one location to those whose work requires the special items.
7. You must not create, send, post or forward, electronic chain letters.
8. Non-district hardware or software is not to be installed on the district networks without authorization. This includes document cameras, network hubs, wireless routers, etc. Copying of commercial software in violation of copyright laws will not be tolerated. In addition, no installation of computer programs, commercial or otherwise, will be configured on district computers without the knowledge of network and/or systems administrators. Contact the Supervisor of Educational Technology if there are specific requests for hardware and/or software.
9. Use of Hopewell Valley Regional School District computing resources for personal financial gain or for political purposes is not permitted
10. Use of impolite or abusive language or photographs will not be tolerated.
11. Because electronic information is volatile and easily reproduced, respect for the work and personal expression of others is especially critical in computer environments. Violations of authorial integrity, including plagiarism, invasion of privacy, unauthorized access, and trade secret and copyright violations, may be grounds for sanctions against members of the academic community.

### **Personal Technology Devices**

Students may find it beneficial and may be encouraged to use personal technology devices for instructional purposes during the school day. The Hopewell Valley Regional School District is committed to moving students and staff forward in a 21st century learning environment. As part of this vision, the school district allows students, staff, parents, and guests to access our wireless network using their own technology tools during the learning day. Any personal technology devices that are capable of merging onto Hopewell Valley Regional School District wireless networks will be governed by the Hopewell Valley Regional School District Guidelines for Responsible Computing. With classroom teacher approval, students may use their own devices in the classroom to access information from the Internet and to communicate and use a variety of productivity tools that may be loaded on their personal technology devices.

No personal mobile devices are to attach to the school district wired network. They are to connect only to the school district wireless network. It is understood that the school district assumes no obligation for the support, either onsite or by other means, of the personal mobile equipment. It will not accept any liability for modifications made to the equipment as a result of establishing a connection within the school district. Users will not have any network services like DNS, DHCP, file-sharing programs or network utilities running on their personal device. Furthermore, no personal network routers, access points, switches, hubs, network printers, or any other devices may be plugged into the district network at any time. Users are prohibited from tethering, a technique in which a mobile device is used as a wireless modem to provide Internet access to other wireless-enabled devices. The network continues to be configured in the best interests of the district-owned devices that are using it. Users will not hold the Hopewell Valley Regional School District liable for theft, damage or loss of personal equipment.

### **1:1 Technology**

The Hopewell Valley Regional School District wants to ensure students develop the skills and knowledge necessary to responsibly navigate this emerging modern world. Therefore, the school district has implemented a 1:1 student to computing device program to create a seamless and dynamic educational experience for students. In most cases, students will be able to have these devices for use 24/7 throughout the school year. Students and parents that are a part of the 1:1 Technology Program must understand and agree to the guidelines for the program and are subject to the same behavioral standards set forth in the Student Code of Conduct, faculty and staff employee handbook and the HVRSD Guidelines for Responsible Computing (Acceptable Use Policy). Please reference 1:1 Technology Guidelines, the 1:1 technology policy for the Hopewell Valley Regional School District.

### **Violations of the Guidelines for Responsible Computing**

Violations of the Hopewell Valley Regional School District Guidelines for Responsible Computing are to be treated like any other legal or ethical violation as outlined in the Student Handbook, relevant contractual agreements, and applicable faculty and staff handbooks. Violators may also be subject to prosecution under applicable Federal and New Jersey statutes.

Any violation of the policy may result in a cancellation of network computing privileges and/or disciplinary action. The administration, faculty and staff of the Hopewell Valley School District may request through each building administrator or their designees that the network administrators deny, revoke, or suspend specific use privileges. Anyone identified as a security risk or having a history of problems with other computer systems may be denied access to the Hopewell Valley Regional School District wide area network and Internet resources.

### **Acknowledgment**

This document contains excerpts and paraphrased sections from similar documents prepared by the FCC, CIPA (Children's Internet Protection Act), Montclair State University, Brown University, and Kings County Office of Education. We gratefully acknowledge their contributions.

Updated: August 7, 2018