Rockford Public Schools

Together Building A Tradition of Excellence

QUALITY COMMUNITY · QUALITY SCHOOLS

District Accredited by AdvancED/NCA
Blue Ribbon Exemplary Schools

HIGH SCHOOL – BYOD STUDENT TECHNOLOGY HANDBOOK

Table of Contents

INTRODUCTION

The following refers to the use of a Rockford Public Schools ("District")-owned and individual student computing devices ("device"). In addition to this Student Handbook, students are required to follow all the guidelines outlined in the District's current "Technology Acceptable Use Policy". As the District's technology initiative centers on new devices, software and educational methodologies, additional policies will continually be reviewed and this set of policies updated. Please refer to the District's website (www.rockfordschools.org) for the most up-to-date information.

BRING YOUR OWN DEVICE (BYOD) REQUIREMENTS

Our Operational Technology team intends to review each personal student device brought to school for this classes and help insure students can fully participate in this class.

Acceptable devices from home include:
1. Chromebooks (purchased within the last 3 years)
2. Windows Laptops (running Windows 7, 8.1 or 10)
3. Apple Laptops (purchased within the last 5 years and running Safari 3.1 or greater)
4. Tablets (including iPad Air or greater, purchased within the last 2 years)
Please note: cell phones do not qualify.

All devices must meet the following minimum requirements:
1. a 9.5" diagonal display
2. a keyboard (physically attached is preferred vs. wireless have the frustrating ability to connect to or interfere with other student devices in a room of students)
3. a web browser (such as Chrome, Safari, Microsoft IE or Edge – Note that other browsers may create frustration for students while accessing content designed for the "big 3 browsers")
4. a wireless WiFi connection capability

Hardship cases only: Should your child not have a device that meets the minimum requirements outlined above, and be in a hardship situation, the school will provide a laptop computer to access to the required materials. Your child will also have access to the course material for homework from any network attached computer you may have at home, or they may access the material with public internet connectivity. Please contact your building for hardship questions.

Hardship Cases Only
STUDENT USE OF DISTRICT TECHNOLOGY

1. All district-owned technology is the property of the District. The student should have NO expectation of privacy of materials found on any District devices and, as a result, may be seized, and owned technology or a District-supplied or supported email service can be reviewed at any time.

2. Only District-issued email IDs are allowed to be used on the device. The student should be the only one to use his/her device. No one else outside of the student should use the device. The student is responsible for anything that happens on his/her device.

3. As with all recording devices, it is expected that students will ask permission before recording an individual or group. Students must obtain school permission to publish a photograph or video of any school-related activity to the internet.

4. Devices are not to be opened or used in bathroom or locker room areas.

5. Students are responsible for bringing the device to school every day unless otherwise directed by a staff member. Failure to bring the device or any other class material(s) does not release the student from his/her responsibility for class work. If a student repeatedly fails to bring materials to class, including the device, the student will be subject to disciplinary action.

6. It is the student's responsibility to bring the device to school fully charged. A student's repeated failure to bring the device charged may result in disciplinary action.

7. While personalized screen savers or backgrounds are permitted, inappropriate or provocative images including, but not limited to, pornographic images, guns, weapons, inappropriate language, threatening language, drug, alcohol or gang-related images are not permitted and such actions are subject to disciplinary action.

8. While at school, games, music, videos and sound use, will be at the discretion of the classroom teacher and building administrator.

9. As with all electronic files, it is good practice to back up, duplicate or archive files to an independent storage space. Offline files should be backed up to the student's One Drive account.

10. The device is designed as a tool for learning; misuse of the device may result in disciplinary action.

11. All students should recognize and guard their personal and private information. While on the internet, students shall not reveal personal information including a home address or phone number or the address or phone number of other students.

12. A student should not share his/her personal security code with anyone. Responsibility for the contents/actions of the device rests solely with that individual.

13. The district expects students to take the device home at night for classwork and recharging.

14. All care, handling and appropriate use that is in effect during the school day shall extend to the use of the device at home.

15. Devices are equipped with a filter. Students should not try to disable or circumvent the filter to get to material considered inappropriate or illegal. Students browsing or possessing inappropriate or illegal material on the device will face disciplinary and possible legal consequences.

16. The district makes no guarantee, written or implied, that materials on the device, including student work, will be safe from deletion or corruption, accidental or otherwise. Backing up files to the district servers is recommended.

17. Parents have the right to limit use of the device at home to school work only.

CARE AND MAINTENANCE OF THE DEVICE

1. Do not attempt to gain access to the internal electronics or to repair the device. If the district device fails to work or is damaged, report the problem to your school's Media Center as soon as possible. Device repair/replacement options for district owned devices will be determined by school administration. You may be issued a temporary district device or other materials until the device is working properly or replaced.

2. Never expose a device to long-term extremes in temperature or direct sunlight. A car is not a good place to store the device.

3. Avoid applying liquids to any device. The device should be cleaned with a soft, dry, lint-free cloth only. <u>Do not use window cleaners, household cleaners, aerosol sprays, solvents, alcohol, ammonia or abrasives to clean the device</u>. Use of unapproved cleaners may remove the protective film covering the screen or face of the device.

4. Any district owned device and the case must remain free of stickers, writing, painting or any other forms of adornment. Students may purchase and decorate their own case if approved by the Technology Department.

5. Never leave a device unattended. When not in your personal possession, the device should be in a secure, locked environment. Unattended devices will be collected and stored in the school's Tech Center.

6. Never throw or slide the device.

7. Avoid placing weight on the device.

8. Each district owned device has a unique identification number and at no time should the numbers or labels be modified or removed.

9. Care must be exercised when plugging and unplugging accessories from the USB, charging or HDMI ports. Device accessories issued to the student are his/her responsibility.

10. All district owned devices have the ability to be remotely located. Modifying, disabling or attempting to disable the locator is a violation of the acceptable use policy and grounds for disciplinary action.

11. The device is an electronic device and care must be exercised when handling. Never throw a backpack that contains a device. Never place a device in a backpack that contains food, liquids and/or heavy, sharp or wet objects.

12. Each device is assigned to an individual and the responsibility for the care of the device rests solely with that individual. <u>Do not</u> lend your device to another person.

13. The device is designed for daily use; therefore, each device must be charged and ready for use each school day. **The device(s) should be charged at home.** Extra batteries, power cords or power adapters will <u>not</u> be provided.

DAMAGED, LOST OR STOLEN DEVICES

In the event a device is lost or stolen, the student and parent should immediately notify the school administrator. The filing of a police report by the parent is mandatory for insurance claim processing. In the absence of a police report, the parent will assume responsibility for the full replacement cost.

In the event that a district owned device (hardship cases only) is intentionally damaged, any future use of a district device will be restricted.

In the event that a police report is filed for a lost or stolen device, the district may aid the police in recovering the device. All devices are tagged with an asset label. The label is not to be tampered with or removed.

In hardship cases only, students who un-enroll from the district during the school year must return the district device, along with any issued accessories, at the time they leave the district. The district device and all accessories should be returned to the school's Tech Center. Failure to return a device in a timely fashion may result in legal action.

PARENT/GUARDIAN RECOMMENDATIONS

It is essential that the following guidelines be followed to ensure the safe, efficient and ethical operation of the device. As a parent, you:

- will supervise your student's use of the device at home;

- will discuss your family's values and expectations regarding the use of the internet and the use of email at home;

- will supervise your student's use of the internet, email and apps;

- will not attempt to repair the device, nor attempt to clean it with anything other than a soft, dry, lint-free cloth;

- will report to the school any problems with the device;

- will make sure your student recharges the device nightly;

- will make sure your student brings the device to school every day;

- understand that if your student comes to school without the device, you may be called to bring it to school;

- will make sure your student has a good bag or backpack to transport the device to and from school;

- agree to return the district device, along with any other accessories, to school when requested and upon your student's withdrawal from the district.

STUDENT EDUCATION TECHNOLOGY ACCEPTABLE USE AND SAFETY

Students are authorized to use the Board's ("District's") computers, laptops, tablets, personal communication devices (as defined by Policy 5136), network and internet connection and online educational services ("Education Technology") for educational purposes. Use of the Education Technology is a privilege, not a right. When using the Education Technology, students must conduct themselves in a responsible, efficient, ethical and legal manner. Unauthorized or inappropriate use of the Education Technology, including any violation of these guidelines, may result in cancellation of the privilege, disciplinary action consistent with the Student Handbook and/or civil or criminal liability. Prior to accessing the Education Technology, students and parents of minor students must sign the Student Education Technology Acceptable Use and Safety Agreement. Parents are encouraged to discuss their values with their students and encourage students to make decisions regarding their use of the Education Technology that is in accord with their personal and family values, in addition to the Board's standards.

Smooth operation of the Education Technology relies upon users adhering to the following guidelines. The guidelines outlined below are provided so that users are aware of their responsibilities:

A. Students are responsible for their behavior and communication using all of the Education Technology devices. All use of the Education Technology must be consistent with the educational mission and goals of the district.

B. Students may only access and use the Education Technology by using their assigned account and may only send school-related electronic communications using their district-assigned email addresses. Use of another person's account/email address/password is prohibited. Students may not allow other users to utilize their account/email address/password. Students may not go beyond their authorized access. Students are responsible for taking steps to prevent unauthorized access to their accounts by logging off or "locking" their computers/laptops/tablets/personal communication devices when leaving them unattended.

C. Students may not intentionally seek information on, obtain copies of or modify files, data or passwords belonging to other users, or misrepresent other users on the district's network. Students may not intentionally disable any security features of the Education Technology.

D. Students may not use the Education Technology to engage in hacking or other unlawful activities.

   1. Students shall not use the Education Technology, either at school or outside of school, to transmit material that is threatening, obscene, disruptive or sexually explicit or that can be construed as harassment or disparagement of others based upon their race, color, national origin, sex, sexual orientation or transgender identity, age, height, weight, disability, religion or political beliefs. Sending, sharing, viewing or possessing pictures, text messages, emails or other materials of a sexual nature (i.e., sexting) in electronic or any other form, including the contents of a personal communication device or other electronic equipment, is grounds for discipline. Such actions will be reported to local law enforcement and child protective services as required by law.

   2. Use of the Education Technology to engage in cyber bullying is prohibited.
      Cyber bullying includes, but is not limited to, the following:
         a. posting slurs, rumors or other disparaging remarks about a student on a website or on weblog;

2/18   7

    b. sending email or instant messages that are mean or threatening, or so numerous as to drive up the victim's cell phone bill;

    c. using a camera phone to take and/or send embarrassing and/or sexually explicit photographs/recordings of students;

    d. posting misleading or fake photographs of students on the internet.

E. Transmission of any material in violation of any state or federal law or regulation or Board policy is prohibited.

F. Any use of the Education Technology for commercial purposes, advertising or political lobbying is prohibited.

G. Students are expected to abide by the following generally-accepted rules of online etiquette:

  1. Be polite, courteous and respectful in your messages to others. Use language appropriate to school situations in any communications made through the Education Technology. Do not use obscene, profane, vulgar, sexually explicit, defamatory or abusive language in your messages.

  2. Never reveal names, addresses, phone numbers or passwords of yourself or other students, family members, teachers, administrators or other district staff members while communicating on the Education Technology.

  3. Do not transmit pictures or other information that could be used to establish your identity without prior approval of a teacher.

  4. Never agree to get together with someone you "meet" online without prior parent approval.

  5. Check email frequently and delete email promptly to avoid excessive use of the electronic mail disk space.

  6. Students should promptly disclose to their teacher or other district staff member any message and/or photograph(s) they receive that is/are inappropriate or makes them feel uncomfortable, especially any email that contains sexually explicit content (e.g., pornography). Students should not delete such messages until instructed to do so by a district staff member.

H. Use of Education Technology to access, process, distribute, display or print child pornography and other material that is obscene, objectionable, inappropriate and/or harmful to minors is prohibited. As such, the following material is prohibited: material that appeals to a prurient interest in nudity, sex and excretion; material that depicts, describes or represents in a patently offensive way with respect to what is suitable for minors an actual or simulated sexual act or sexual contact, actual or stimulated normal or perverted sexual acts or a lewd exhibition of the genitals; and material that lacks serious literary, artistic, political or scientific value as to minors. Offensive messages and pictures, inappropriate text files or files dangerous to the integrity of the Board's computers/network (e.g., viruses) are also prohibited.

I. Malicious use of the Education Technology to develop programs that harass other users or infiltrate a computer or computer system and/or damage the software components of a computer or computing system is prohibited. Students may not engage in vandalism or use the Education Technology in such a way that would disrupt its use by others. Vandalism is defined as any malicious or intentional attempt to harm, steal or destroy data of another user, school networks or

technology hardware. This includes, but is not limited to, uploading or creation of computer viruses, installing unapproved software, changing equipment configurations, deliberately destroying or stealing hardware and its components or seeking to circumvent or bypass network security and/or the Board's technology protection measures. Students also must avoid intentionally wasting limited resources. Students must immediately notify the teacher, building principal or Security Department if they identify a possible security problem. Students should not go looking for security problems because this may be construed as an unlawful attempt to gain access (hacking).

J. All communications and information accessible via the internet should be assumed to be private property (i.e., copyrighted and/or trademarked). All copyright issues regarding software, information and attributions of authorship must be respected.

K. Downloading information onto district-owned equipment or contracted online education services is prohibited; all downloads must be to an external storage device. If a student transfers files from information services and electronic bulletin board services, the student must check the file with a virus-detection program before opening the file for use. Only public domain software may be downloaded. If a student transfers a file or software program that infects the Education Technology with a virus and causes damage, the student will be liable for any and all repair costs to make the Education Technology once again fully operational.

L. Students must secure prior approval from a teacher or building principal before joining a Listserv (electronic mailing lists) and should not post personal messages on bulletin boards or Listservs.

M. Students may use real-time electronic communication, such as chat or instant messaging, only under the direct supervision of a teacher or in moderated environments that have been established to support educational activities and have been approved by the Board, Superintendent or building principal. Students may only use their district-assigned accounts/email addresses when accessing, using or participating in real-time electronic communications for education purposes.

N. Privacy in communication over the internet and through the Education Technology is not guaranteed. To ensure compliance with these guidelines, the Board reserves the right to monitor, review and inspect any directories, files and/or messages residing on or sent using the Education Technology. Messages relating to, or in support of, illegal activities will be reported to the appropriate authorities.
Users have no right or expectation to privacy when using the Education Technology. The district reserves the right to access and inspect any facet of the Education Technology including, but not limited to, computers, laptops, tablets, personal communication devices, networks or internet connections, online educational services, email or other messaging or communication systems or any other electronic media within its technology systems or that otherwise constitutes its property and any data, information, email, communication, transmission, upload, download, message or material of any nature or medium that may be contained therein.

A student's use of the Education Technology constitutes his/her waiver of any right to privacy in anything s/he creates, stores, sends, transmits, uploads, downloads or receives on or through the Education Technology and related storage medium and equipment.

Routine maintenance and monitoring, utilizing both technical monitoring systems and staff monitoring, may lead to discovery that a user has violated Board policy and/or the law. An individual search will be conducted if there is reasonable suspicion that a user has violated Board

policy and/or law, or if requested by local, state or federal law enforcement officials. Students' parents have the right to request to see the contents of their student's files, emails and records.

O. Use of the Education Technology and any information procured from the internet is at the student's own risk. The Board is not responsible for any damage a user suffers, including loss of data resulting from delays, non-deliveries, mis-deliveries or service interruptions. The Board is not responsible for the accuracy or quality of information obtained through its services. Information (including text, graphics, audio, video, etc.) from internet sources used in student papers, reports and projects should be cited the same as references to printed materials.

P. Disclosure, use and/or dissemination of personally-identifiable information of minors via the Education Technology is prohibited, except as expressly authorized by the minor student's parent on the Student Education Technology Acceptable Use and Safety Agreement Form.

Q. Proprietary rights in the design of websites hosted on Board–owned or leased servers remains at all times with the Board.

   1. Since there is no central authority on the internet, each site is responsible for its own users. Complaints received from other sites regarding any of the district's users will be fully investigated and disciplinary action will be taken as appropriate.

   2. Preservation of Resources and Priorities of Use: Computer resources are limited. Because space on disk drives and bandwidth across the lines which connect the Education Technology (both internally and externally) are limited, neither programs nor information may be stored on the system without the permission of the district's Director of Technology. Each student is permitted reasonable space to store email, web and personal files. The Board reserves the right to require the purging of files in order to regain disk space. Students who require access to the Education Technology for class or instruction-related activities have priority over other users. Students not using the Education Technology for class-related activities may be "bumped" by any student requiring access for class or instruction-related purposes. The following hierarchy will prevail in governing access to the Education Technology:

       a. Class work, assigned and supervised by a district staff member.
       b. Class work, specifically assigned but independently conducted.
       c. Personal correspondence (email – checking, composing and sending).
       d. Training (use of such programs as typing tutors, etc.).
       e. Personal discovery ("surfing the internet").
       f. Other uses – access to resources for "other uses" may be further limited during the school day at the discretion of the building principal or district's Director of Technology.

Game playing is not permitted unless under the supervision of a teacher. Any individual who is aware of a violation of the Board policy or this guideline, including inappropriate online contact, content or conduct, such as sexting, harassment or cyber bullying, should bring it to the attention of the building principal or Superintendent immediately.