Richland-Bean Blossom Community School Corporation
ACCEPTABLE USE POLICY FOR ELECTRONIC RESOURCES
(REVISED 07/11/2016)

All Richland-Bean Blossom (RBBCSC) students and staff are responsible for their actions and activities involving the school corporation's computers, electronic devices, network and Internet services, and for their computer files, passwords, and accounts. These rules provide general guidance concerning the use of school computers and other electronic devices and provide examples of prohibited uses. The rules and guidelines detail acceptable use of electronic information resources under which students, staff, and all members of the RBBCSC community, herein referred to as "users," will be held accountable. The rules do not attempt to describe every possible prohibited activity. Students, parents, and school staff who have questions about whether a particular activity is prohibited are encouraged to contact a building administrator. These rules apply to all school computers, all school-provided electronic devices wherever used, all uses of school servers, and Internet access and networks regardless of how they are accessed.

Acceptable Use

1. School computers, network and Internet services, and electronic resources are provided for educational purposes and research consistent with RBBCSC's educational mission, curriculum, and instructional goals.
2. Users must comply with all school board policies, the student handbook, and school rules and expectations concerning conduct and communication when using school computers or school-issued electronic resources, whether on or off school property.
3. Students also must comply with all specific instructions from school staff.

Prohibited Uses

Unacceptable uses of school electronic resources include, but are not limited to, the following:

1. Accessing or Communicating Inappropriate Materials – Users may not access, submit, post, publish, forward, download, scan, or display defamatory, abusive, obscene, vulgar, sexually explicit, sexually suggestive, threatening, discriminatory, harassing, bullying, and/or illegal materials or messages.
2. Illegal Activities – Users may not use the school corporation's computers, electronic devices, networks, or Internet services for any illegal activity or in violation of any board policy/procedure or school rules. RBBCSC and its employees and agents assume no responsibility for illegal activities of students while using school computers or school-issued electronic resources.
3. Violating Copyrights or Software Licenses – Downloading, copying, duplicating, and distributing software, music, sound files, movies, images, or other copyrighted materials without the specific written permission of the copyright owner is prohibited, except when the use falls within the Fair Use Doctrine of the United States Copyright Law (Title 17, USC) and content is cited appropriately.

4. Plagiarism – Users may not represent as their own work any materials obtained on the Internet (ie: term papers, articles, music, etc). When using other sources, credit must be given to the copyright holder.
5. Use for Non-School-Related Purposes - School corporation's computers, electronic devices, and network and Internet services are provided for purposes related to educational programs, school operations, and performance of job responsibilities. Incidental personal use of school devices is permitted as long as such use: 1) does not interfere with the user's responsibilities and performance; 2) does not interfere with system operations or other system users; and 3) does not violate this policy and the accompanying rules or any other board policy, procedure, or school rules. "Incidental personal use" is defined as use by an individual for occasional personal communications.
6. Misuse of Passwords/Unauthorized Access – Users may not share passwords, use other users' passwords, access or use other users' accounts, or attempt to circumvent network security systems.
7. Malicious Use/Vandalism – Users may not engage in any malicious use, disruption, or harm to the school corporation's computers, electronic devices, or network and Internet services, including but not limited to hacking activities and the creation/uploading of computer viruses.
8. Avoiding School Filters – Users may not attempt to or use any software, utilities, or other means to access Internet sites or content blocked by the school filters. All users must use their own login credentials, and not those belonging to any other student or staff member.
9. Unauthorized Access to Blogs/Social Networking Sites, Etc. – Users may not access blogs, social networking sites, etc. prohibited by building administration or the RBBCSC Technology Department. Teachers and students using authorized social networking sites for educational projects or activities shall follow the age requirements and legal requirements that govern the use of social networking sites in addition to the guidelines established in this policy.
10. Wasting System Resources - Users shall not use the network in such a way that would waste system resources or disrupt the use of the network by others. This includes but is not limited to excessive printing, file storage, online games, and video/audio streaming not directly related to educational projects as determined by the supervising instructor or building administrator.
11. Unauthorized Equipment - Users may not attach unauthorized equipment, including personal laptops, tablets, and handheld devices, to the corporation network without permission from the RBBCSC Technology Department.

Compensation for Losses, Costs, and/or Damages

As technology has become more mobile many electronic devices owned by the Richland-Bean Blossom Community School Corporation (RBBCSC) and used by staff members are transported outside both the direct physical control and locations controlled by the RBBCSC. It is in this outside environment that responsibility is shared by both the RBBCSC and the individual staff member who chooses to take an electronic device off school grounds. In the event that an electronic device is lost, stolen, or

damaged, the individual student or staff member may be responsible for the total replacement cost per the market value of the device. In addition all users (students and staff) may be responsible for compensating the school corporation for any losses, costs, or damages incurred for violations of board policies/procedures and school rules. The school corporation assumes no responsibility for any unauthorized charges or costs incurred by users while using school corporation computers, devices, or the school network.

Employee Uses of Social Media or Social Networking Websites
The Richland-Bean Blossom Community School Corporation (RBBCSC) respects the right of employees to use social media networking sites, personal websites, blogs, tweets, and other forms of electronic communication. It is important that school employees' personal or professional use of these sites does not damage the reputation of the school, its staff, students, or their families. Employees should exercise care in setting appropriate boundaries between their personal and public online behavior, understanding what is private in the digital world. Such online behavior always has the possibility of becoming public, even without knowledge or consent.

The RBBCSC asks all employees to carefully review the privacy settings on any social media and networking sites they use (ie: Facebook, Twitter, Flickr, LinkedIn, etc.) and exercise care and good judgment when posting school content and information. In addition school employees should adhere to the following policies, which are consistent with the school's workplace standards on harassment, student relationships, conduct, professional communication, and confidentiality:

1. An employee should not make statements that would violate any of the school's policies, including its policies concerning discrimination, harassment, content, and confidentially.
2. All school employees must uphold the RBBCSC's value of respect for the individual and avoid making defamatory statements concerning the school, its employees, its students, or their families.
3. An employee may not disclose any confidential school information or confidential information obtained during the course of his/her employment concerning any individuals or organizations, including staff, students, and/or their families.
4. All sites established or maintained by RBBCSC employees that can be identified, or could reasonably be construed as a RBBCSC site, are deemed the property of the Richland-Bean Blossom Community School Corporation.
5. At no time may a student(s) name(s) or other identifying information be matched with a student's picture or likeness without express written permission of the parent or guardian.
6. When establishing a social networking site that represents The RBBCSC, all school employees must follow the school corporation's prescribed naming convention.

7. School employees who create sites to be used by students may not include any resources that students are forbidden to access at school.
8. All websites/social networking sites created or maintained by school employees are the direct responsibility of that employee and should be kept up-to-date and continually monitored and appropriately edited in a timely fashion by the sponsoring employee.
9. The RBBCSC will provide employees a set of guidelines designed to aid in the creation, appropriate use, monitoring, and interactions on social websites and when dealing with electronic communications.
10. Any RBBCSC employee upon departure from the school corporation must release access and control of any website/social networking site established as a RBBCSC site.

Student Social Media Guidelines

The Richland-Bean Blossom Community School Corporation works to provide all students with access to an education that prepares them to succeed in college and careers. Part of being a successful citizen is understanding that social media and digital communication are essential parts of our world today. It is important to recognize that access to information can result in tremendous advantages, but it can also create new responsibilities of which students should be aware.

Definition of Social Media

- Social media is any form of online publication or presence that allows interactive communication, including social networks, blogs, photo sharing platforms, Internet websites, Internet forums, and wikis. Examples of social media include, but are not limited to, Facebook, Twitter, Edmodo, Schoology, Instagram, YouTube, Google+, and Flickr.

- Some examples of social media uses include:
    - Blogging about movies, sports, or news events;
    - Posting updates or activities on your Facebook page;
    - Participating in a teacher-established Edmodo group; or
    - Using a Google Hangout to work on a class project.

Create the Digital Image You Want

- **Align your online image with your goals.** A digital footprint is the reputation you leave online and can include material posted on blogs, and mentions on websites and videos that are uploaded onto sharing sites. Online actions leave a permanent record and remain online, even if you click “delete.” Be thoughtful about what you share online and consider how it would appear to family, friends, colleges, and future employers.

  Because many colleges and employers search social media before making

admissions and hiring decisions, you might want to use social media as a tool to demonstrate your interests in positive ways. For example, social media allows you to show who you are as a student online by sharing what you think about and what matters to you. This can help as you get closer to graduation and begin considering post-secondary education and career options. Some examples of how you can use social media for academic advancement include:
    - Commenting on articles in a knowledgeable way; or
    - Starting a blog about current events.

- **Stand behind your words.** You should always take responsibility for the content you post in all social media environments. While you may think that using a fake name may prevent posts from becoming part of your footprint, there are still ways to link that information to the person who posted it (for example, through an Internet IP address or other distinguishing information linking posts). Be your best self online – post accurate information and be accountable for what you say.

- **Families can be helpful partners.** Share your digital footprint with your parents and consider their suggestions. Get your parents' input about what information they feel should remain private and what is fine to post publicly. Your parents are responsible for what you do online if you are a minor and may want your passwords and usernames to monitor your social media use. Additionally, because technology is constantly changing, you may know more about social media than your family, so you may also want to show your parents and other family members how to create an online presence themselves.

Post Responsibly – Be Mindful of Your Audience

- **Using social media academically is an extension of your classroom environment.** When you use social media for academic purposes, such as for a school assignment, treat the platform as a digital extension of your classroom – the same rules apply online as they do at school. For example, if you would not make fun of a classmate in English class, do not do it online either. For school-related social media, do not tag student posts, photos, or videos unless your teacher gives you permission, as this may expose the content to audiences for whom it was not intended.

- **Put your best foot forward.** People of all ages sometimes act differently on social media than they would "face-to-face," assuming that, because they are not communicating in person, they are not accountable for their actions. In fact, because of the nature of the digital world, you should be as responsible, if not more, when acting online. Since you never know who will ultimately be reading content online, always assume that anyone might have access. If you do not know who will be reading it, ask yourself if you would be okay with a parent or relative reviewing your content. If not, there might be a better way to get your point across.

- **Pause before you post.** Once a comment is posted online, you cannot later say, “never mind.” It may seem funny or harmless when you post it, but it could hurt or offend someone. As guidance, take a few extra minutes to think about whether a post will be hurtful or embarrassing or whether it could negatively affect a future opportunity. For example, if you post an aggressive or inflammatory comment online because you felt heated in the moment, this may end up making you a less attractive candidate in some employers’ minds. Because online posts can never be completely deleted, it is important to make sure that each post is something you want to live with.

Consider the Consequences to Your Online Actions

- **Personal use of social media may have an effect at school.** While at times, it is easy to tell whether a social media use is school-related or personal, at other times, it may be difficult to distinguish fully between different uses. Sometimes, personal social media use, including off-hours use, may result in disruption at school and the school may need to get involved. This could include disciplinary action such as a parent conference or suspension. It is important to remember that infractions outlined in the Discipline Code prohibiting certain types of communication also apply to electronic communication. To be safe, be in control of what you do online, even if it is during personal time. For example, if your classmate is tagging you in rude Tweets, do not reciprocate in a similar way. Instead, stay positive, do what you know is right, and consider blocking or reporting this person if you feel it is warranted.

- **Protect yourself.** There are many ways to protect yourself online. For example, only accept friend requests from people you know. You may interact online with people you have never met in person. Use caution, find out as much as you can about the person, and tell a parent if you are considering meeting one of these people face to face. Additionally, while it is important to be yourself online, it is also important to remember not to post too many identifying details (such as where you live or your social security number) because revealing that information can be potentially dangerous or compromise your identity in some way. Do not share passwords with friends and be sure that the computers do not automatically save passwords. Always log off when you have finished using a site – do not just click out of the browser.

- **Adjust your privacy settings appropriately.** Privacy settings are automatically set by social media providers governing who can see your posts, how information is linked, and what data is available to the public. Each social media platform has different privacy setting defaults and some change those settings without making it obvious to you. As a user of social media, you should determine whether to change the default settings to make access to postings more or less private. For example, if you are creating a personal site to promote a social or political issue, you likely want to make that site open to everyone. However, if you want to discuss a project you are doing in class, it may be better to limit access only to a

small group of classmates.

Take Threats of Cyberbullying Seriously

- **Cyberbullying takes many forms.** Cyberbullying is the use of electronic technologies to hurt or harm other people. Examples include:
    - Sending offensive text messages or emails;
    - Posting statements that are not true and create rumors; or
    - Circulating embarrassing photos of a classmate online.

- **Report the behavior and get help.** If you are being cyberbullied or hear about/observe someone else being cyberbullied, report the behavior and get help. You can tell a parent, school staff, another adult family member, or a trusted adult. If no adult is available and you or someone else is in danger, call 911. Students who violate the student code of conduct may be subject to discipline per the RBBCSC Ownership in Education handbook.

- **Know what to do.** It is important not to respond to, retaliate to, or forward any harassing, intimidating, or bullying content. “De-friend,” block, or remove people who send inappropriate content. It may also be a good idea to save harassing messages, as this evidence could be important to show an adult if the behavior continues. If the behavior is school-related, print out the messages and provide them to the school when you report the incident (do not email them to anyone). If you have questions about reporting incidents, speak with your teacher, school principal or contact the Superintendent’s Office.

Understand the Fine Print and Other Rules

- There is no right to privacy when using school-related social media. If you are using the school’s device or network, the school may review what you post. The “Internet-Don’t List” related to online communication includes the following:
    - Causing harm to others or damaging technology-related property;
    - Gaining or attempting to gain unauthorized access to school systems;
    - Using school technology and/or systems for financial gain or business activities; or
    - Engaging in criminal or unlawful activities online.

Student Security

Users may not reveal personal information, including a home address and phone number, about themselves or another individual on any unsecured electronic medium, such as websites, blogs, podcasts, videos, wikis, or social networking sites. If users encounter dangerous or inappropriate information or messages, they shall notify the school administration immediately.

Staff may post student pictures on corporation/school/newspaper/classroom “public” websites, unless opted out by parents/guardians. Students’ grades, test results, or identifying pictures may be stored only on corporation-approved secure sites that

require a username and password for authorized individuals to access.

RBBCSC staff must maintain the confidentiality of student data in accordance with the Family Education Rights and Privacy Act (FERPA).

All RBBCSC schools are closed campuses. RBBCSC retains all rights concerning any recording and/or publishing of any student's or staff member's work(s) or image(s). Students must obtain permission from a RBBCSC staff member to publish a photograph or video of any school-related activity. It is best practice and common courtesy to ask permission before recording an individual or groups.

The use of cameras on any type of electronic device is strictly prohibited in locker rooms and restrooms.

Students may be issued a school email address to improve student communication and collaboration on school projects. Email shall be used only for educational purposes that directly relates to a school project or assignment.

Technology Privacy
All computers, telephone systems, voicemail systems, electronic mail, and electronic communication systems are the corporation's property. The corporation retains the right to access and review all electronic and voice mail, computer files, databases, and any other electronic transmissions contained in or used in conjunction with the corporation's computer system, telephone system, electronic mail system, and voice mail system. Students and staff should have no expectation that any information contained on such systems is confidential or private.

System Security
Any user who identifies a security problem must notify his/her teacher or building administrator immediately. The user shall not demonstrate the problem to others or access unauthorized material. Staff shall immediately report any potential security breaches to the RBBCSC Technology Department.

Staff shall change their passwords to all systems at the beginning of every school year.

Personal Devices
All users are prohibited from using privately-owned electronic devices in school settings unless explicitly authorized by the building principal or RBBCSC corporation administration. BYOD will no longer be permitted effective after the 2015-2016 school year.

Additional Rules for Laptops, iPads, or other Electronic Devices Issued to Students or Staff

1. Electronic devices loaned or leased to students or staff shall be used only for educational purposes that directly relate to a school project or assignment,

unless otherwise explicitly authorized by building administration.

2. Users are responsible for the proper care of electronic devices at all times, whether on or off school property, including costs associated with repairing or replacing the device.
3. Users must report a lost or stolen device to the building administration immediately. If a device is stolen, a report also should be made immediately with the school safety officer and/or local police.
4. The policy and rules apply to the use of the electronic device at any time or place, on or off school property. Students are responsible for obeying any additional rules concerning care of devices issued by school staff.
5. Violation of policies or rules governing the use of electronic devices or any careless use of the device may result in a student's device being confiscated and/or a student only being allowed to use the device under the direct supervision of school staff. The student will also be subject to disciplinary action for any violations of Board policies/procedures or school rules.
6. Parents are responsible for supervising their child's use of the device when not in school.
7. The device configuration shall not be altered in any way by users; this includes software, hardware and accessories such as cases. No software applications shall be installed, removed, or altered on the device unless permission is explicitly given by the teacher or building administrator.
8. The device is to be used only by the student or staff member to whom it is issued. The person to whom the device is issued will be responsible for any activity or action performed on the device.
9. Devices issued to staff are linked to the position of the staff member. If a staff member is unable to be present for his/her job duties for more than 6 weeks; the device must be turned into administration so the staff member fulfilling that position may employ the technology.
10. Interns and student teachers will not be issued a school device. It is the responsibility of the university to provide the intern or student teacher with the necessary technology for their placement.
11. The device must be returned in acceptable working order by the last day of each school year, upon withdrawal or exit date from the school corporation, and whenever requested by school staff.

Terms of Use

RBBCSC reserves the right to deny, revoke, or suspend specific user privileges and/or take other disciplinary action, including suspension or expulsion from school, for violations of this policy. Additionally, all handbook regulations apply to the use of the RBBCSC network, Internet, and electronic resources.

Students have no expectation of confidentiality or privacy with respect to any usage of a school-issued electronic device, regardless of whether that use is for school or personal purposes. RBBCSC may, without notice or consent, supervise access, view, monitor,

and record use of these devices at any time or any reason related to the operation of the school. By use of these devices, students agree and consent to such access, monitoring, and recording of their use.

Disclaimer – RBBCSC, its employees and agents, make no warranties of any kind, neither expressed nor implied, concerning the network, Internet access, and electronic resources it is providing. Furthermore, RBBCSC is not responsible for:

1. The accuracy, nature, quality, or privacy of information stored on local servers or devices or information gathered through Internet access.
2. Any damages suffered by a user (whether the cause is accidental or not) including but not limited to, loss of data, delays or interruptions in service, and the infection of viruses or other malware on personal computers or other devices.
3. Unauthorized financial obligations resulting from the use of RBBCSC electronic resources.