

**FERTILE-BELTRAMI PUBLIC SCHOOL DIST #599
2018-2019 K-9 INTERNET ACCOUNT AGREEMENT**

Personal information:

GRADE_____

Name_____

Address_____

City_____ State_____ Zip_____

2018-2019 SIGNATURE PAGE

STUDENT SECTION

I have read the school district’s Acceptable Use Policy. I agree to follow the rules contained in this policy. I understand that if I violate the rules my account can be terminated.

Student Signature_____ Date_____

PARENT OR GUARDIAN SECTION

I have read the school district’s Acceptable Use Policy. (If internet access is provided at home **I will supervise my child’s use of the system in accordance with the acceptable use policy**).

I hereby release the district, its personnel, and any institutions with which it is affiliated, from any and all claims and damages of any nature arising from my child’s use of, or inability to use, the district system, including, but not limited to claims that may arise from the unauthorized use of the system to purchase products or services.

I will instruct my child regarding any restrictions against accessing material that are in addition to the restrictions set forth in the District Acceptable Use Policy. I will emphasize to my child the importance of following the rules for personal safety.

I give permission to issue an account for my child and certify that the information contained in this form is correct.

Parent/Guardian Signature

Print Parent/Guardian Name

Address

City State Zip

Home Telephone Number

Work Telephone Number

**** 2018-2019 SCHOOL YEAR: TAKE HOME DEVICE PROGRAM ****

- **Fertile-Beltrami School has been awarded a grant for 20 Kajeet Take Home Devices. These are a wireless hot-spot, paired with an ipad device, intended to enhance internet accessibility to students that do not have it available to them at home, and/or to increase learning and completion of work/projects by the student as deemed necessary by their teacher. Please contact the technology department if you have any questions about this program.**
- **The authorized use of the take home device is designed for the Ipad to connect through the Kajeet device or the available school bus hotspots, and not to any other WiFi network. This allows for proper content filtering, consistent with the district policy.**
- **Parent permission is required before students are allowed access to the Take-Home Devices. By signing the below consent, you are authorizing your student to take home a backpack when deemed necessary or given permission by a teacher/staff member.**
- **Authorization includes making sure that all equipment brought home is returned intact and without damage. If a Kajeet unit or Ipad are returned damaged, the student/parent will be fiscally responsible for those damages, including any missing components. Authorization also includes conforming to the district use policy. Failure to do so results in a violation. The student will not be able to check out a system until either situation is remedied.**

Parent/Guardian Signature _____

Date _____

APPROPRIATE USE OF THE NETWORK AND THE INTERNET

- a. The following rules guide the use of the network and the Internet
 - i. All uses of the network and the Internet must be in support of education and consistent with the purposes of the Fertile-Beltrami School District #599.
 - ii. **NO HANDHELD DEVICES WILL BE AUTHORIZED TO ACCESS THE F-B WIRELESS NETWORK. Unauthorized users will lose their unauthorized device (phone, Ipod, Ipad, and personal device) immediately and the parent will have to pick it up from the principal.**
 - iii. Network accounts are to be used only by the authorized owner of the account. **The sharing of passwords is ABSOLUTELY prohibited and will result in a violation.**
 - iv. Any violations of the use of the network and the Internet should be reported to the district's Technology Coordinator.
 - v. The teacher in charge must approve the use of personal USB drives or CD's on the network computers.
 - vi. Personal information about oneself SHOULD NOT be shared over the Internet. **The computer is NOT a social tool and violations will be enforced for chat rooms, blogging, game and music downloading (Itunes is acceptable). The school district blocks Facebook and Twitter, along with any other social media sites that we are made aware of. The school district strongly urges parents to prohibit their son/daughter from posting information on these sites.**
 - vii. Use of the network to access or process inappropriate materials or to download files dangerous to the integrity of the network is PROHIBITED. Transmission of material, information, or software in violation of any district policy or federal, state, or local law or regulation is prohibited. **This includes through chatting software and blogging.** A zero tolerance policy is in effect.
 - viii. Network users identifying a security problem on the district system must notify the teacher in charge. Do not demonstrate the problem to anyone.
 - ix. Network users may download materials for their own use. Copyrighted materials must be used in accordance with district policy and applicable law.
 - x. Vandalism will result in cancellation of system use privileges and loss of computer. Vandalism is defined as a malicious attempt to harm or destroy district equipment or material, that of another user of the district system or the Internet system. The authorities will be notified.
- b. It is illegal to use the school district's Internet resources/accounts:
 - i. To access, upload, download, or distribute violent, pornographic, obscene, or sexually explicit material. This includes any use of the computer that would be considered bullying. This includes inappropriate cartoons, jokes, and music titles. **Zero tolerance policy is in effect.**
 - ii. To transmit obscene, abusive, violent, or sexually explicit language. This includes music, music videos and song titles. **Zero tolerance policy is in effect.**
 - iii. To violate any local, state or federal statute. **Zero tolerance policy in effect and authorities WILL BE CONTACTED.**
 - iv. To access any software sites that allow user to bypass any firewalled or restricted school district sites. **Zero tolerance policy in effect.**
 - v. To vandalize, damage or disable the property of another person or organization. **Zero tolerance policy in effect and authorities WILL BE CONTACTED.**
 - vi. To access another person's materials, information or files without the implied or district permission of that persons. A violation will be enforced.
 - vii. To violate copyright laws, or otherwise use another person's intellectual property without their prior approval or proper citation, including the downloading or exchanging of

pirated software or copying software to or from any school computer. A violation will be enforced.

- viii. For unauthorized commercial use and/or financial gain of the user. A violation will be enforced.

II. Parent notification of student Internet use

- a. Outside of school, families bear responsibility for the same guidance of Internet use as they exercise with information sources such as television, telephone, radio, movies, and other possibly offensive media. Please instruct your children that chat rooms and blogging are not allowed on the school's computer. We discourage student access to Facebook or similar sites. We encourage parents to go to these sites periodically to monitor activity.
- b. Parents will be notified that their students will be using school district resources/accounts to access the Internet. The district will provide parents the option to request alternative activities NOT requiring Internet access.
- c. Student, teacher and parent or guardian must sign the "Internet Use Agreement" before a student will be permitted to access the Internet.
- d. It is possible for students to purchase goods and services via the Internet. These purchases could potentially result in unwanted financial obligations. It is the parents' responsibility to provide appropriate guidance in such use of the Internet.
- e. District Google accounts are setup for students to safely access other sites requiring login, as well as for creating & sharing school appropriate material. Elementary K-6 students have Google Docs access without email. Grades 7-9 are allowed email restricted within the district only, and grades 9-12 have outside email access as well. **Sharing of inappropriate material through the district account will result in a violation.**
- f. **Violations: I understand that a first violation may result in the loss of my computer for one month and my parents will be notified of the violation. I understand that a second violation may result in the loss of my computer for the remainder of the school year.**
- g. **ZERO TOLERANCE: Any student found in violation of Fertile-Beltrami Dist #599's Internet policy regarding student safety, inappropriate sites, any type of information considered to be sexually explicit, violent, or in any way harassing to minorities or bullying of other students will result in the loss of the laptop, loss of Internet access and loss of LAN access immediately and permanently for the rest of the school year. If the violation involved the breaking of any local, state, or federal law the authorities will also be notified.**

FERTILE-BELTRAMI PUBLIC SCHOOL DIST #599
As posted in the District Policy Manual

524 INTERNET ACCEPTABLE USE AND SAFETY POLICY**I. PURPOSE**

The purpose of this policy is to set forth policies and guidelines for access to the school district computer system and acceptable and safe use of the Internet, including electronic communications.

II. GENERAL STATEMENT OF POLICY

In making decisions regarding student and employee access to the school district computer system and the Internet, including electronic communications, the school district considers its own stated educational mission, goals, and objectives. Electronic information research skills are now fundamental to preparation of citizens and future employees. Access to the school district computer system and to the Internet enables students and employees to explore thousands of libraries, databases, bulletin boards, and other resources while exchanging messages with people around the world. The school district expects that faculty will blend thoughtful use of the school district computer system and the Internet throughout the curriculum and will provide guidance and instruction to students in their use.

III. LIMITED EDUCATIONAL PURPOSE

The school district is providing students and employees with access to the school district computer system, which includes Internet access. The purpose of the system is more specific than providing students and employees with general access to the Internet. The school district system has a limited educational purpose, which includes use of the system for classroom activities, educational research, and professional or career development activities. Users are expected to use Internet access through the district system to further educational and personal goals consistent with the mission of the school district and school policies. Uses which might be acceptable on a user's private personal account on another system may not be acceptable on this limited-purpose network.

IV. USE OF SYSTEM IS A PRIVILEGE

The use of the school district system and access to use of the Internet is a privilege, not a right. Depending on the nature and degree of the violation and the number of previous violations, unacceptable use of the school district system or the Internet may result in one or more of the following consequences: suspension or cancellation of use or access privileges; payments for damages and repairs; discipline under other appropriate school district policies, including suspension, expulsion, exclusion or termination of employment; or civil or criminal liability under other applicable laws.

V. UNACCEPTABLE USES

A. The following uses of the school district system and Internet resources or accounts are considered unacceptable:

1. Users will not use the school district system to access, review, upload, download, store, print, post, receive, transmit or distribute:

- a. pornographic, obscene or sexually explicit material or other visual depictions that are harmful to minors;
 - b. obscene, abusive, profane, lewd, vulgar, rude, inflammatory, threatening, disrespectful, or sexually explicit language;
 - c. materials that use language or images that are inappropriate in the education setting or disruptive to the educational process;
 - d. information or materials that could cause damage or danger of disruption to the educational process;
 - e. materials that use language or images that advocate violence or discrimination toward other people (hate literature) or that may constitute harassment or discrimination.
2. Users will not use the school district system to knowingly or recklessly post, transmit or distribute false or defamatory information about a person or organization, or to harass another person, or to engage in personal attacks, including prejudicial or discriminatory attacks.
 3. Users will not use the school district system to engage in any illegal act or violate any local, state or federal statute or law.
 4. Users will not use the school district system to vandalize, damage or disable the property of another person or organization, will not make deliberate attempts to degrade or disrupt equipment, software or system performance by spreading computer viruses or by any other means, will not tamper with, modify or change the school district system software, hardware or wiring or take any action to violate the school district's security system, and will not use the school district system in such a way as to disrupt the use of the system by other users.
 5. Users will not use the school district system to gain unauthorized access to information resources or to access another person's materials, information or files without the implied or direct permission of that person.
 6. Users will not use the school district system to post private information about another person, personal contact information about themselves or other persons, or other personally identifiable information, including, but not limited to, addresses, telephone numbers, school addresses, work addresses, identification numbers, account numbers, access codes or passwords, labeled photographs or other information that would make the individual's identity easily traceable, and will not repost a message that was sent to the user privately without permission of the person who sent the message.
 - a. This paragraph does not prohibit the posting of employee contact information on school district webpages or communications between employees and other individuals when such communications are made for education-related purposes (i.e., communications with parents or other staff members related to students).
 - b. Employees creating or posting school-related webpages may include personal contact information about themselves on a webpage. However, employees may not post personal contact information or other personally identifiable information about students unless:
 - (1) such information is classified by the school district as directory information, and verification is made that the school district has not

received notice from a parent/guardian or eligible student that such information is not to be designated as directory information in accordance with Policy 515; or

- (2) such information is not classified by the school district as directory information but written consent for release of the information to be posted has been obtained from a parent/guardian or eligible student in accordance with Policy 515.

In addition, prior to posting any personal contact or personally identifiable information on a school-related webpage, employees shall obtain written approval of the content of the postings from the building administrator.

- c. These prohibitions specifically prohibit a user from utilizing the school district system to post personal information about a user or another individual on social networks, including, but not limited to, social networks such as “MySpace” and “Facebook.”
7. Users must keep all account information and passwords on file with the designated school district official. Users will not attempt to gain unauthorized access to the school district system or any other system through the school district system, attempt to log in through another person’s account, or use computer accounts, access codes or network identification other than those assigned to the user. Messages and records on the school district system may not be encrypted without the permission of appropriate school authorities.
 8. Users will not use the school district system to violate copyright laws or usage licensing agreements, or otherwise to use another person’s property without the person’s prior approval or proper citation, including the downloading or exchanging of pirated software or copying software to or from any school computer, and will not plagiarize works they find on the Internet.
 9. Users will not use the school district system for conducting business, for unauthorized commercial purposes or for financial gain unrelated to the mission of the school district. Users will not use the school district system to offer or provide goods or services or for product advertisement. Users will not use the school district system to purchase goods or services for personal use without authorization from the appropriate school district official.
- B. A student or employee engaging in the foregoing unacceptable uses of the Internet when off school district premises also may be in violation of this policy as well as other school district policies. Examples of such violations are, but are not limited to, situations where the school district system is compromised or if a school district employee or student is negatively impacted. If the school district receives a report of an unacceptable use originating from a non-school computer or resource, the school district may investigate such reports to the best of its ability. Students or employees may be subject to disciplinary action for such conduct, including, but not limited to, suspension or cancellation of the use or access to the school district computer system and the Internet and discipline under other appropriate school district policies, including suspension, expulsion, exclusion, or termination of employment.
 - C. If a user inadvertently accesses unacceptable materials or an unacceptable Internet site, the user shall immediately disclose the inadvertent access to an appropriate school district official. In the

case of a school district employee, the immediate disclosure shall be to the employee's immediate supervisor and/or the building administrator. This disclosure may serve as a defense against an allegation that the user has intentionally violated this policy. In certain rare instances, a user also may access otherwise unacceptable materials if necessary to complete an assignment and if done with the prior approval of and with appropriate guidance from the appropriate teacher or, in the case of a school district employee, the building administrator.

VI. FILTER.

- A. With respect to any of its computers with Internet access, the School District will monitor the online activities of minors and employ technology protection measures during any use of such computers by minors and adults. The technology protection measures utilized will block or filter Internet access to any visual depictions that are:
1. Obscene;
 2. Child pornography; or
 3. Harmful to minors.
- B. The term "harmful to minors" means any picture, image, graphic image file, or other visual depiction that:
1. Taken as a whole and with respect to minors, appeals to a prurient interest in nudity, sex, or excretion; or
 2. 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 simulated normal or perverted sexual acts, or a lewd exhibition of the genitals; and
 3. Taken as a whole, lacks serious literary, artistic, political, or scientific value as to minors.
- C. An administrator, supervisor or other person authorized by the Superintendent may disable the technology protection measure, during use by an adult, to enable access for bona fide research or other lawful purposes.

VII. CONSISTENCY WITH OTHER SCHOOL POLICIES

Use of the school district computer system and use of the Internet shall be consistent with school district policies and the mission of the school district.

VIII. LIMITED EXPECTATION OF PRIVACY

- A. By authorizing use of the school district system, the school district does not relinquish control over materials on the system or contained in files on the system. Users should expect only limited privacy in the contents of personal files on the school district system.
- B. Routine maintenance and monitoring of the school district system may lead to a discovery that a user has violated this policy, another school district policy, or the law.

- C. An individual investigation or search will be conducted if school authorities have a reasonable suspicion that the search will uncover a violation of law or school district policy.
- D. Parents have the right at any time to investigate or review the contents of their child's files and e-mail files. Parents have the right to request the termination of their child's individual account at any time.
- E. School district employees should be aware that the school district retains the right at any time to investigate or review the contents of their files and e-mail files. In addition, school district employees should be aware that data and other materials in files maintained on the school district system may be subject to review, disclosure or discovery under Minn. Stat. Ch. 13 (the Minnesota Government Data Practices Act).
- F. The school district will cooperate fully with local, state and federal authorities in any investigation concerning or related to any illegal activities or activities not in compliance with school district policies conducted through the school district system.

IX. INTERNET USE AGREEMENT

- A. The proper use of the Internet, and the educational value to be gained from proper Internet use, is the joint responsibility of students, parents and employees of the school district.
- B. This policy requires the permission of and supervision by the school's designated professional staff before a student may use a school account or resource to access the Internet.
- C. The Internet Use Agreement form for students must be read and signed by the user, the parent or guardian, and the supervising teacher. The Internet Use Agreement form for employees must be signed by the employee. The form must then be filed at the school office. As supervising teachers change, the agreement signed by the new teacher shall be attached to the original agreement.

X. LIMITATION ON SCHOOL DISTRICT LIABILITY

Use of the school district system is at the user's own risk. The system is provided on an "as is, as available" basis. The school district will not be responsible for any damage users may suffer, including, but not limited to, loss, damage or unavailability of data stored on school district diskettes, tapes, hard drives or servers, or for delays or changes in or interruptions of service or misdeliveries or nondeliveries of information or materials, regardless of the cause. The school district is not responsible for the accuracy or quality of any advice or information obtained through or stored on the school district system. The school district will not be responsible for financial obligations arising through unauthorized use of the school district system or the Internet.

XI. USER NOTIFICATION

- A. All users shall be notified of the school district policies relating to Internet use.
- B. This notification shall include the following:
 - 1. Notification that Internet use is subject to compliance with school district policies.
 - 2. Disclaimers limiting the school district's liability relative to:

- a. Information stored on school district diskettes, hard drives or servers.
 - b. Information retrieved through school district computers, networks or online resources.
 - c. Personal property used to access school district computers, networks or online resources.
 - d. Unauthorized financial obligations resulting from use of school district resources/accounts to access the Internet.
3. A description of the privacy rights and limitations of school sponsored/managed Internet accounts.
 4. Notification that, even though the school district may use technical means to limit student Internet access, these limits do not provide a foolproof means for enforcing the provisions of this acceptable use policy.
 5. Notification that goods and services can be purchased over the Internet that could potentially result in unwanted financial obligations and that any financial obligation incurred by a student through the Internet is the sole responsibility of the student and/or the student's parents.
 6. Notification that the collection, creation, reception, maintenance and dissemination of data via the Internet, including electronic communications, is governed by Policy 406, Public and Private Personnel Data, and Policy 515, Protection and Privacy of Pupil Records.
 7. Notification that, should the user violate the school district's acceptable use policy, the user's access privileges may be revoked, school disciplinary action may be taken and/or appropriate legal action may be taken.
 8. Notification that all provisions of the acceptable use policy are subordinate to local, state and federal laws.

XII. PARENTS' RESPONSIBILITY; NOTIFICATION OF STUDENT INTERNET USE

- A. Outside of school, parents bear responsibility for the same guidance of Internet use as they exercise with information sources such as television, telephones, radio, movies and other possibly offensive media. Parents are responsible for monitoring their student's use of the school district system and of the Internet if the student is accessing the school district system from home or a remote location.
- B. Parents will be notified that their students will be using school district resources/accounts to access the Internet and that the school district will provide parents the option to request alternative activities not requiring Internet access. This notification should include:
 1. A copy of the user notification form provided to the student user.
 2. A description of parent/guardian responsibilities.
 3. A notification that the parents have the option to request alternative educational activities not requiring Internet access and the material to exercise this option.
 4. A statement that the Internet Use Agreement must be signed by the user, the parent or guardian, and the supervising teacher prior to use by the student.
 5. A statement that the school district's acceptable use policy is available for parental review.

XIII. IMPLEMENTATION; POLICY REVIEW

- A. The school district administration may develop appropriate user notification forms, guidelines and procedures necessary to implement this policy for submission to the school board for approval. Upon approval by the school board, such guidelines, forms and procedures shall be an addendum to this policy.
- B. The administration shall revise the user notifications, including student and parent notifications, if necessary, to reflect the adoption of these guidelines and procedures.
- C. The school district Internet policies and procedures are available for review by all parents, guardians, staff and members of the community.
- D. Because of the rapid changes in the development of the Internet, the school board shall conduct an annual review of this policy.

Legal References: 15 U.S.C. § 6501 *et seq.* (Children’s Online Privacy Protection Act)
 17 U.S.C. § 101 *et seq.* (Copyrights)
 20 U.S.C. § 6751 *et seq.* (Enhancing Education through Technology Act of 2001)
 47 U.S.C. § 254 (Children’s Internet Protection Act of 2000 (CIPA))
 47 C.F.R. § 54.520 (FCC rules implementing CIPA)
 Minn. Stat. § 125B.15 (Internet Access for Students)
 Minn. Stat. § 125B.26 (Telecommunications/Internet Access Equity Act)
Tinker v. Des Moines Indep. Cmty. Sch. Dist., 393 U.S. 503, 89 S.Ct. 733, 21 L.Ed.2d 731 (1969)
United States v. American Library Association, 539 U.S. 194, 123 S.Ct. 2297, 56 L.Ed.2d 221 (2003)
Layshock v. Hermitage Sch. Dist., 412 F.Supp. 2d 502 (2006)
J.S. v. Bethlehem Area Sch. Dist., 807 A.2d 847 (Pa. 2002)

Cross References: MSBA/MASA Model Policy 403 (Discipline, Suspension, and Dismissal of School District Employees)
 MSBA/MASA Model Policy 406 (Public and Private Personnel Data)
 MSBA/MASA Model Policy 505 (Distribution of Nonschool-Sponsored Materials on School Premises by Students and Employees)
 MSBA/MASA Model Policy 506 (Student Discipline)
 MSBA/MASA Model Policy 515 (Protection and Privacy of Pupil Records)
 MSBA/MASA Model Policy 519 (Interviews of Students by Outside Agencies)
 MSBA/MASA Model Policy 521 (Student Disability Nondiscrimination)
 MSBA/MASA Model Policy 522 (Student Sex Nondiscrimination)
 MSBA/MASA Model Policy 603 (Curriculum Development)
 MSBA/MASA Model Policy 604 (Instructional Curriculum)
 MSBA/MASA Model Policy 606 (Textbooks and Instructional Materials)
 MSBA/MASA Model Policy 806 (Crisis Management Policy)
 MSBA/MASA Model Policy 904 (Distribution of Materials on School District Property by Nonschool Persons)

- I. A student who is found in violation of any of the computer contract rules or the student account rules will lose his/her computer for a period of one month for the first violation. The parent will also receive a letter explaining the violation.
- II. A student who is found in violation for the second time will lose his/her computer for the remainder of the year. Parents will receive a letter and a copy of the inappropriate material notifying them that their student has his/her second violation.
- III. **ZERO TOLERANCE:** Any student found in violation of Fertile-Beltrami Dist #599's Internet policy regarding student safety, inappropriate sites, any type of information considered to be sexually explicit, violent, or in any way harassing to minorities or bullying of other students will result in the loss of the laptop, loss of Internet access and loss of LAN access immediately and permanently for the rest of the school year. If the violation involved the breaking of any local, state, or federal law the authorities will also be notified.