Employee Technology Agreement

Every Bonneville Academy employee will be required to sign this Technology Agreement each school year.

Computer and network use are necessary components of an employee's work at Bonneville Academy. In addition, varying work responsibilities result in access to information sources such as software, programs, the internet, school network, etc. Although employees may have access to these information sources, their use must be specially authorized.

Access and authorization to information and equipment carry a corresponding responsibility for their appropriate use. School equipment and access are intended to be used for educational and professional/career development activities.

Expectations of employees include, but are not limited to, the following (see *[policy number TBD ELECTRONIC INFORMATION RESOURCES AND ACCEPTABLE USE]* for a full listing of acceptable and unacceptable activities):

1. Student Personal Safety
a. Employees who supervise students with access to technology equipment shall be familiar with the Bonneville Academy Student Technology Use Agreement and enforce its provisions.

b. All student technology use must be supervised by a teacher who has signed this agreement.

2. Student Information and Records
a. Student data on the SIS, other databases, or simply gathered by educators are educational records for the purposes of FERPA and are protected as are other educational records.

b. Employees are responsible to meet the requirements of FERPA prior to the release or dissemination of any educational records, including student data, whether aggregated or disaggregated.

c. Employees are responsible to prevent disclosure of information or data in their control. This includes removable media and portable devices (e.g.: laptops, flash drives, etc.).

3. Illegal or Destructive Activities
a. Employees shall not go beyond their authorized access to the school network or other computer equipment or software including the files or accounts of others.

b. Employees shall not disrupt or attempt to damage or disrupt technology equipment or systems, including activities that would affect data or system performance.

c. Employees shall not use School equipment to engage in illegal acts.

4. System Security
a. Employees are responsible for the security of their technology equipment, files and passwords.

b. Employees shall promptly notify the School of security problems.

c. Employees with access to student records may not use, release, or share these records except as

authorized by Federal and State law.

d. Students may not have access to technology equipment other than workstations.

e. Staff will not leave their workstations unlocked or devices unattended while logged into the network.

f. Passwords are to be protected and not shared with anyone. This applies to students who are teacher aides and family members of staff.

5. Inappropriate Conduct—the following are prohibited in public, private or posted messages or files:
a. Obscene, profane, lewd, vulgar, rude, inflammatory, threatening or disrespectful language;

b. Potentially damaging, dangerous or disruptive material;

c. Personal or generalized attacks or harassment; and

d. False or defamatory information.

6. Plagiarism and Copyright Infringement
a. Works may not be plagiarized.

b. The rights of copyright owners are to be respected. Copyright infringement occurs when an individual inappropriately reproduces a work that is protected by copyright. If a work contains language that is protected by copyright, the expressed requirements should be followed. If an employee is unsure whether or not a work can be used, the copyright owner should be contacted for permission.

c. Software copyrights must be strictly respected.

7. Inappropriate Access to Material
a. School equipment shall not be used with material that is profane, obscene (pornographic) or advocates illegal acts, violence or discrimination. This restriction applies regardless of the physical location of equipment and regardless of network being used.

b. The non-educational use of multi-player computer games on school equipment is not allowed. This restriction applies to family members of staff.

c. Inadvertent inappropriate access shall be reported immediately to the principal or supervisor.

8. Expectation of Privacy
a. Employees have no expectation of privacy in files, disks, documents, etc., which have been created in, entered in, stored in, downloaded from, or used on School equipment.

9. Services and Assumption of Risks
a. The School makes no warranties of any kind, whether express or implied, for services provided and is not responsible for any damages suffered while on the system to include loss of data and inaccurate or poor quality information obtained from the system.

10. All acceptable and unacceptable activities as listed in *[policy number TBD ELECTRONIC INFORMATION RESOURCES AND ACCEPTABLE USE]*

11. Due Process

a. In the event there is an allegation that an employee has violated this agreement, the employee will receive notice of the alleged violation and an opportunity to present an explanation.

b. Disciplinary actions in harmony with Corrective Discipline procedures will be tailored to meet the specific concerns related to the violation. Deliberate violations of this agreement (e.g. malicious acts or omissions; searching for, viewing or otherwise visiting pornographic or sexually explicit sites) are cause for immediate termination.

I have read and understand this document and the **Electronic Information Resources and Acceptable Use policy** and its provisions.

Employee Computer Use Agreement and its provisions. I understand that violation of this Agreement are grounds for discipline and may be cause for immediate termination.

Name_____ (last, first, middle)

Grade/Subject/Department_____School/Location_____

_____

Signature_____Date_____

_____