MADISON-GRANT UNITED SCHOOL CORPORATION
TECHNOLOGY ACCEPTABLE USE POLICY

Electronic Resources:
The Madison-Grant United School Corporation school board recognizes that an effective public education system develops students who are globally aware, civically engaged, and capable of managing their lives and careers. The board also believes that students need to be proficient users of information, media, and technology to succeed in a digital world.

Therefore, the Madison-Grant United School Corporation will use electronic resources as a powerful and compelling means for students to learn core subjects and applied skills in relevant and rigorous ways. It is the district's goal to provide students with rich and ample opportunities to use technology for important purposes in schools just as individuals in workplaces and other real-life settings. The district's technology will enable educators and students to communicate, learn, share, collaborate and create, to think and solve problems, to manage their work, and to take ownership of their lives.

The Board directs the Superintendent or designee to create strong electronic educational systems that support innovative teaching and learning, to provide appropriate staff development opportunities and to develop procedures to support this policy.

Electronic Resources:
Digital citizenship represents more than technology literacy: successful, technologically fluent digital citizens live safely and civilly in an increasingly digital world. They recognize that information posted on the Internet is public and permanent and can have a long-term impact on an individual's life and career. Expectations for student and staff behavior online are no different than face-to-face interactions.

Network
The district network includes wired and wireless computers and peripheral equipment, files and storage, e-mail and Internet content (blogs, web sites, web mail, groups, wikis, etc.). The district reserves the right to prioritize the use of, and access to, the network.

All use of the network must support education and research and be consistent with the mission of the district.

Acceptable network use by district students and staff includes:
- Creation of files, projects, videos, web pages and podcasts using network resources in support of educational research;
- Participation in blogs, wikis, bulletin boards, social networking sites and groups and the creation of content for podcasts, e-mail and web pages that support educational research;
- With parental permission, the online publication of original educational material, curriculum related materials and student work. Sources outside the classroom or school must be cited appropriately;
- Staff use of the network for incidental personal use in accordance with all district policies and guidelines;
- Use of staff or student personal devices on the district network *may* be authorized, upon approval of the Technology Director to confirm that the equipment meets district guidelines and the use supports the educational process. Connection of any personal electronic device is subject to all guidelines in this document.

Unacceptable network use by district students and staff includes but is not limited to:
- Personal gain, commercial solicitation and compensation of any kind;
- Liability or cost incurred by the district;
- Downloading, installation and use of games, audio files, video files or other applications (including shareware or freeware) without permission or approval from the Technology Director.
- Support or opposition for ballot measures, candidates and any other political activity;
- Hacking, cracking, vandalizing, the introduction of viruses, worms, Trojan horses, time bombs and changes to hardware, software, and monitoring tools;
- Unauthorized access to other district computers, networks and information systems;
- Cyberbullying, hate mail, defamation, harassment of any kind, discriminatory jokes and remarks;
- Information posted, sent or stored online that could endanger others (e.g., bomb construction, drug manufacture);
- Accessing, uploading, downloading, storage and distribution of obscene, pornographic or sexually explicit material; and
- Attaching unauthorized equipment to the district network. Any such equipment will be confiscated and destroyed.

The district will not be responsible for any damages suffered by any user, including but not limited to, loss of data resulting from delays, non-deliveries, mis-deliveries or service interruptions caused by its own negligence or any other errors or omissions. The district will not be responsible for unauthorized financial obligations resulting from the use of, or access to, the district's computer network or the Internet.

Internet Safety: Personal Information and Inappropriate Content
Students and staff should not reveal personal information, including a home address and phone number, on web sites, blogs, podcasts, videos, wikis, e-mail or as content on any other electronic medium.

Students and staff should not reveal personal information about another individual on any electronic medium.

No student pictures or names can be published on any class, school or district web site unless the appropriate permission has been verified according to district policy.

If students encounter dangerous or inappropriate information or messages, they should notify the appropriate school authority immediately.

Filtering and Monitoring
Filtering software is used to block or filter access to visual depictions that are obscene and all child pornography in accordance with the Children's Internet Protection Act (CIPA). Other objectionable material could be filtered. The determination of what constitutes "other objectionable" material is a local decision.

- Filtering software is not 100% effective. While filters make it more difficult for objectionable material to be received or accessed; filters are not a solution in themselves. Every user must take responsibility for his or her use of the network and Internet and avoid objectionable sites;
- Any attempts to defeat or bypass the district's Internet filter or conceal Internet activity are prohibited: proxies, https, special ports, modifications to district browser settings and any other techniques designed to evade filtering or enable the publication of inappropriate content;
- E-mail inconsistent with the educational and research mission of the district will be considered SPAM and blocked from entering district e-mail boxes;
- The district will provide appropriate adult supervision of Internet use. The first line of defense in controlling access by minors to inappropriate material on the Internet is deliberate and consistent monitoring of student access to district computers;
- Staff members who supervise students, control electronic equipment or have occasion to observe student use of said equipment online, must make a reasonable effort to monitor the use of this equipment to assure that student use conforms to the mission and goals of the district; and
- Staff must make a reasonable effort to become familiar with the Internet and to monitor, instruct and assist effectively.

Copyright
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 generally prohibited. However, the duplication and distribution of materials for educational purposes are permitted when such duplication and distribution fall within the Fair Use Doctrine of the United States Copyright Law (Title 17, USC) and content is cited appropriately.

All student work is copyrighted. Permission to publish any student work requires permission from the parent or guardian.

Network Security and Privacy
Passwords are the first level of security for a user account. System logins and accounts are to be used only by the authorized owner of the account, for authorized district purposes. Students and staff are responsible for all activity on their account and must not share their account password.

These procedures are designed to safeguard network user accounts:

- Change passwords according to district policy;
- Do not use another user's account;
- Do not insert passwords into e-mail or other communications;
- If you write down your account password, keep it out of sight;
- Do not store passwords in a file without encryption;
- Do not use the "remember password" feature of Internet browsers; and
- Lock the screen, or log off, if leaving the computer.

Student Data is Confidential
District staff must maintain the confidentiality of student data in accordance with the Family Education Rights and Privacy Act (FERPA).

No Expectation of Privacy
The district provides the network system, e-mail and Internet access as a tool for education and research in support of the district's mission. The district reserves the right to monitor, inspect, copy, review and store, without prior notice, information about the content and usage of:

- The network;
- User files and disk space utilization;
- User applications and bandwidth utilization;
- User document files, folders and electronic communications;
- E-mail;
- Internet access; and
- Any and all information transmitted or received in connection with network and e-mail use.

No student or staff user should have any expectation of privacy when using the district's network. The district reserves the right to disclose any electronic message to law enforcement officials or third parties as appropriate. All documents are subject to the public records disclosure laws of the State of Indiana.

Archive and Backup
Backup is made of all district e-mail correspondence for purposes of public disclosure and disaster recovery. Barring power outage or intermittent technical issues, staff and student files are backed up on district servers nightly – Monday through Friday.

Disciplinary Action
All users of the district's electronic resources are required to comply with the district's policy and procedures.

Violation of any of the conditions of use explained in this policy could be cause for disciplinary action, including suspension or expulsion from school and suspension or revocation of network and computer access privileges.

Madison-Grant United School Corporation
Technology Acceptable Use Policy Agreement Form

THIS USER IS A (CHECK ONE): STUDENT ☐ STAFF ☐ GUEST USER* ☐

*GUEST USERS: GIVE REASON FOR ACCOUNT REQUEST:_____

USERS'S NAME (Print): _____ _____ _____
Last First MI

USER'S ADDRESS: _____ _____ _____ _____
STREET **CITY** **STATE** **ZIP**

USER'S DATE OF BIRTH: ___/___/____ SCHOOL: _____GRADE ___

HOME PHONE: _____

Dear Parent/Guardian: At some time during the school year, school/district personnel may interview, audio tape, video tape, or photograph classroom activities or special events/projects that your child participates in during or after the school day. Such materials may be used for staff/student evaluations, educational or public awareness purposes, and my be viewed by other students and faculty/administrators and/or placed on the district or school Internet web sites. Please note that the media posed on these internet web sites are available to the general public. The school/district assumes no responsibility for video tapes, audio tapes or photographs, etc. ..that may been made by non-school personnel at public events. No personal video tapes, audio tapes, or photographs shall be allowed to be made by individual students.

If you choose not to allow your child to be interviewed, audio taped, video-taped, or photographed, you assume responsibility for teaching that child to inform/remind teachers that he/she is not to be included in such activities.

I agree to the following for my child (**ALL ITEMS *MUST* BE CHECKED "YES" OR "NO"):**

	Yes	**No**
Internet Access Account	☐	☐
Student Email Account	☐	☐
Network Account	☐	☐
Media Web page	☐	☐
Media Newspaper	☐	☐

NOTE: Federal Law requires the District to monitor electronic activities of minors.

ACCEPTABLE USE AGREEMENT
As a User of the Madison-Grant United School Corporation Technology Network, I have read the Acceptable Use Policy and agree to comply with the Internet Access and Email rules regulations as set forth in this document. I agree to communicate using the network in a responsible manner while abiding by all relevant laws and restricts. I further understand that violation of these regulations are unethical and may constitute a criminal offense. Should I commit any violation, my access privileges may be revoked and school disciplinary measure and/or legal action may be taken against me.

USER'S/STUDENT'S SIGNATURE: _____ DATE: _____

PARENTAL APPROVAL
As the parent or legal guardian of the student (under 18) signing above, I understand that all access is designed for educational purposes; however, I also recognize that some materials on the internet may be objectionable and I accept responsibility for guidance of Internet use by setting and conveying standards for my child to follow when selecting, sharing, researching, or exploring electronic information and media.

PARENT/GUARDIAN NAME (Printed**): _____**

PARENT/GUARDIAN SIGNATURE: _____ DATE: _____