***Student Technology Use Guidelines*: Summary and Consequences**

Technology tools and the Internet are available to students and staff to enhance the curriculum and promote educational excellence. Use of school technology materials and Internet access will be provided to those who agree to act in a considerate and responsible manner. Information sent or received by e-mail, the Internet or other means over the computers available to students and staff is the property of the district and may be accessed at any time by the district for its review. In the event that a review reveals that this policy has been violated in any way or that the privilege of using the technology tools and the Internet is being abused in any way, appropriate action will be taken against the individual or individuals involved. The Internet user log shall be archived for a period of six months.

PRIVILEGES: The use of the district network services is a PRIVILEGE, not a right, and inappropriate use may result in a cancellation of those privileges. The Chief Technology Officer with the campus administrator will deem what is inappropriate use and may deny, revoke, or suspend access to specific users.

SECURITY: Security on any computer system is a high priority. If you can identify a security problem within the network, you must notify the teacher or principal. Do not demonstrate the problem to other users. Do not use another individual's account, forge messages or post anonymous messages. Attempts to login to any system as any other user may result in cancellation of user privileges. Attempts to login to the district networks as a system administrator or any other form of unauthorized access will result in immediate cancellation of user privileges. Any user identified as a security risk or having a history of problems in using other computer systems may be denied access to district network services.

NON-COMPLIANCE: Violations will be referred to a campus administrator for disciplinary or legal action. Consequences will be based on policies established in the Student Handbook, Code of Conduct, Federal and State law. In addition, failure to comply with this policy or directives may result, dependent on the severity of the breach, in withdrawal of your access privileges, exclusion from courses of study, placement in an alternative education program, or criminal prosecution. The individual is also subject to MISD Acceptable Use Policy. Faculty members will be notified of the student’s loss of privileges.

Level I	Level II	Level III
The following offenses are subject to Level 1 Code of Conduct consequences. If applicable, the individual will reimburse the District for any incurred expenses and the individual may lose the privilege of using any networked District technology tools for a period of time determined by the appropriate campus administrator.	The following offences are subject to Level II Code of Conduct consequences (minimum of fifteen days placement in our district BIC program). If applicable, the individual will reimburse the District for any incurred expenses and the individual may lose the privilege of using any networked District technology tools for a period of time determined by the appropriate campus administrator. Depending on the severity of the breach, the individual may be excluded from courses of study and criminal charges filed.	The following offences are subject to Level III Code of Conduct consequences (minimum of thirty days placement in our district BIC program). If applicable, the individual will reimburse the District for any incurred expenses and the individual may lose the privilege of using any networked District technology tools for a period of time determined by the appropriate campus administrator. Depending on the severity of the breach, the individual may be excluded from courses of study and criminal charges filed.

Offenses	Offenses	Offenses
*Intentionally wasting resources. *Using the school's hardware, software or network for commercial purposes. *Participating in any type of teleconferencing or chat without permission of instructional staff or using e-mail without instructional staff permission/supervision. *Using another's password. *Revealing passwords to others.	*Vandalizing any part of the computer hardware, software or the network. This includes theft of any hardware and or software. *Displaying or sending offensive messages or pictures on the network or while using any school owned computer. *Sending a threatening or harassing message. *Trespassing in another's files or misusing or deleting another's files. *Publishing inappropriate information on the district Web page. *Other unethical use of the school's network system or to interfere with or disrupt network users, services or equipment as determined by the Chief Technology Officer.	*Interfering with the integrity of a network system. *Interfering with the integrity of any e-mail system. *Illegal activities that violate either State, Federal laws or District Policies. *Intentional spreading of embedded messages or files. *Violating copyright laws. This includes making illegal copies of school owned software.