SUBJECT: TECHNOLOGY – SECURITY

Access to Services Policy
All networked district technology resources require authentication. Login accounts are generated by the technology department upon receipt of a users signed Acceptable Use Agreement. Expired accounts are deleted by the Technology Department at the request of a Building Principal or the District Office. At the end of each academic year the Technology Services Offices contact each Building Principal and the District Office to request confirmation of all expired accounts which are to be deleted.

Data privacy policy
Staff data files and electronic storage areas shall remain District property are subject to District control and inspection. The District Network Administrator may access all such files and communications to insure system integrity and compliance with requirements of this policy and accompanying regulations. Staff should NOT expect that information stored on district system will be private.

User Identification (User Name) and Password Policy
A new district wide default password is chosen on July 1 of each year. Users are notified (at point of login) to change their password every 60 days. All users are mandated to change their default password upon first use. The Technology Office recommends that users not maintain the same password beyond 60 days. Long term substitute and temporary employees are granted accounts with Building Principal or District Office approval. Staffs are not to share their user password with long term staff, temporary staff or visitors. Passwords are not to be written down or posted. The disclosing of passwords is prohibited. Staff should have no need to grant Technology Services access to their passwords. Users should not attempt to gain unauthorized access by attempting to log in through another person's account. All internal user accounts are standardized as first initial of first name and the first seven characters of the last name. Passwords must be no less than six characters.

Security Awareness Policy
The Technology Services department will store mobile technology resources during any long-term school closings such as extended weekends, holidays and the summer break. Building coordinators and Principals are asked to present monthly reminders to their staff concerning technology resource security. Teachers and staff are responsible for securing all smaller, mobile technology resources when not in use.

Network Security Policy
All network closets are too remained locked at all times. Access should only be granted to these areas with the knowledge and approval of the Technology Services Department. Main Office staff should notify and receive approval prior to allowing any service or support vendor access to any area of the district.

Network Attack Policy
Technology Services maintains a server client anti-virus security application, a top level firewall and SPAM filter. The Anti-Virus application, firewall and SPAM filter are updated under an annual maintenance agreement allowing for on-going support contract for services.

(Continued)

SUBJECT: TECHNOLOGY – SECURITY (cont.)

Visitor Network Access
Guests, visitors and vendors are not authorized to use non-district technology resources on the districts network without prior authorization from the District Office and the office of Technology Services.

Remote Network Administration Support Access Policy
For the purpose of remote support the Network Administrator is granted remote network access for diagnostics and repair of network systems. No other remote network administration is authorized by district staff or students.

Remote Staff Access Policy
For the purpose of remote communication and file storage, staff are granted remote access to all district e-mail services including e-mail, chat, conferences, file storage, web publishing, calendars and workspaces.

District E-Mail Communications Policy
All district staff shall make use of the district e-mail system for all internal and external digital communications. Staff is not authorized to use personal or third party e-mail systems for district communication.

Reviewed: 1/26/09
First Reading: 3/9/09
Adopted: 3/23/09