

EMAIL ACCEPTABLE USE REGULATION

Email is a core internal and external communication tool. This Regulation contains key information regarding user responsibilities.

Email services are provided to all staff whose job functions and responsibilities require such services, as determined by their supervisor, the Human Resources Director, and the Technology Director. An email account is obtained as part of the request for general network access and is to be used to support District activities.

All users shall adhere to the following rules:

- Staff will use email to communicate with others in the District and outside the district so long as those communications are related to legitimate business activities.
- Staff will use email for legal, constructive, ethical, and professional activities and not for personal gain.
- Staff will refrain from sending confidential information in emails (such as protected information as defined by HIPAA or FERPA). Email sent to recipients outside the regional email system is unencrypted and unsecure and should not contain confidential information.
- In the event confidential information must be sent, it should occur via a third party account such as Zixmail or by using the current Barracuda Networks encryption service process.
- Staff who actively sync the district email system with a personal device (i.e., “smartphone”, tablet, etc.) must create and employ a manually entered PIN (numeric, non-swipe, personal identification number).

All users will understand the possible need for review of their email accounts for:

- A legitimate business purpose (e.g., the need to access information when an employee is absent for an extended period of time).
- Diagnoses and resolution of technical problems involving system hardware, software or communications.
- Possible misuse of email when a reasonable suspicion of abuse exists, or in conjunction with an approved investigation.

All users will understand that email created in the normal course of official business and retained as evidence of official policies, actions, decisions or transactions are records subject to records management requirements and need to be retained by the District for six (6) years. Examples include:

- Policies and directives.
- Correspondence or memoranda related to official business.
- Work schedules and assignments.
- Agendas and minutes of meetings.
- Drafts of documents that are circulated for comment or approval.
- Any document that initiates, authorizes, or completes a business transaction.
- Final reports or recommendations.

Examples of messages that typically do not constitute records are:

- Personal messages or announcements, social announcements, or phone messages.
- Copies or extracts of documents distributed for convenience or reference.

Approved: July 18, 2014

Revised and Approved: Nov. 13, 2014