DAYTON PUBLIC SCHOOLS E-MAIL GUIDELINES

1. INTRODUCTION

The Dayton Public School District (DPSD) current E-mail/electronic office system is GroupWise (GW). Facilities available within GW include E-mail, spell check, calendars, scheduling, directories, listings, automatic reminders and distribution lists. Each user must complete and sign a DPS Novell Network New Hire Form – User Account form to obtain access to the E-mail/electronic office system.

2. ACCEPTABLE USE

Acceptable uses of the E-mail / electronic office system are activities that support the user's job assignment within the guidelines and policies of the Dayton Public Schools. Users are encouraged to make full use of these electronic facilities in the pursuit of their jobs and assignments, provided such use complies with Board Policy EDE. The remainder of this document concerns primarily the use of the E-mail portion of the district's electronic facilities.

3. UNACCEPTABLE USE

Consistent with the district's Computer & Internet Acceptable Use Policy, unacceptable uses of these electronic facilities include:

a) Using profanity, obscenity or other language that may be offensive to another user.
b) Copying commercial software or other copyright protected material in violation of copyright law.
c) using these electronic services for financial gain or for any commercial or illegal activity
d) Time-wasting activities that do not adhere to the district's mission.

4. E-MAIL MANAGEMENT AND PRIVACY

The E-mail/electronic office system is the property of the DPSD. All E-mail messages written using the system are also the property of the district. Never consider electronic communications to be private. Treat electronic communications the same as written hard copy communications with regard to propriety and openness. The district reserves the right to review all electronic correspondence that uses district systems and facilities.

5. ACCOUNT RESPONSIBILITIES

The person in whose name an account/user ID is issued is responsible at all times for proper usage. Users should change their passwords every 90 days and should never reveal their password to any other person, including help desk personnel or their manager or personal secretary/assistant. Passwords must be selected in a manner that avoids names, dates, and other combinations that would make guessing them possible. Good passwords are at least eight (8) characters long and include both letters and numbers.

6. EFFECTIVE USE OF E-MAIL

The following practices will increase the effectiveness of E-mail:

a) Make subject headings as descriptive as possible.

b) Restate the question or issue being addressed in a response unless the text of the original message(s) is included in the current message.

c) Include the most important fact/idea/issue first or very near the top of the message.

d) Avoid misunderstandings by keeping in mind that electronic text is devoid of any context clues that convey shades of irony, sarcasm or harmless humor.

e) Proofread/edit each message and use the system's spell check prior to sending a message.

f) Check the facts in your message before sending it; do not spread rumors via E-mail.

7. EXPECTED BEHAVIOR

Employees are expected to use these systems only for activities appropriate to the business and educational objectives of the DPSD. Your usage and communication should reflect well on yourself and on the school district. While your behavior represents the district, you must restrict your communication to within the bounds of the authority of your position. You may not, for example, commit the district to purchasing an item as a result of your communication when a Purchase Order is required for such activity. Just as with written correspondence, such a violation is subject to disciplinary action including dismissal from employment.

8. CAPACITY AND CONSERVATION OF RESOURCES

The storage of documents and other items uses system resources that are finite and limited; failure to use these resources wisely could result in system outages and thus deprive others from getting their work done. Users are expected to:

a) Open their E-mail on a regular basis (at least daily, if possible), delete unneeded items, and file items needed for future reference appropriately so as not to fill up their incoming mail file (in-basket). Failure to do so will result in that user ID being deleted from the system along with all associated files and records including all unopened E-mail.

b) Delete unneeded items from their mail logs on a regular basis and keep mail logs organized so that they can be easily maintained.

c) Send E-mail to concerned parties only.

d) Use the E-mail system's delegation or forwarding facilities (which ever is available and/or appropriate) whenever they are out for extended periods of time. Passwords are never to be shared with anyone.

9. SHARED ACCOUNTS

A single individual should log onto all accounts. Shared accounts, when approved, are specific to an educational or business purpose.

10. ACCESSING ANOTHER USER’S E-MAIL

Where appropriate, primary users may provide proxy access to their incoming E-mail to other secondary/proxy E-mail users. This should only be done in situations where the same proxy users might also handle the primary user's paper mail. In all cases, this should be done by means of the E-mail system's proxy facilities, not by giving a person the ability to log onto the primary user's account ID. The same approach should be used for calendar access and for access to any other facilities belonging to the primary user.

11. GOVERNMENT-IN-THE SUNSHINE LAW ADHERENCE

Most E-mail messages, created or received in the transaction of official School District business, are public records, open to public inspection according to provisions in the Ohio Revised Code (ORC) 149.43. Depending on the content and topic of a particular message, it may or may not be exempt from public inspection under Public Records Law. Each user is individually responsible for maintaining the public accessibility of his/her own incoming and outgoing E-mail messages as required by the Public Records Law. Questions relating to whether or not the content of a particular E-mail message constitutes a public record should be directed to the district’s Legal Department. As a general rule, information that is known to be exempt from public inspection (for example, confidential student records/data and some personnel information) should not be included in any E-mail message.

12. RETENTION OF E-MAIL MESSAGES

The district’s E-mail system will delete all E-mail 365 days after the message is sent. District employees are encouraged to delete messages on a daily basis, immediately after reading, replying, or taking other action concerning a particular message. If, according to State mandated records retention schedules, the content of an E-mail message possesses long term business value, employees are required to print the message and place it in the proper paper file for further retention. Three record categories are described below to assist users in determining the retention requirement of E-mail messages. It is important to note that an estimated 90% of E-mail messages typically fall under the categories of non-record materials, notices with no business value, or transitory messages and therefore should be deleted by both the sender and receiver immediately after the administrative value is lost.

Category #1 – Transient Retention (consists of email messages)

- Do not set policy, establish guidelines or procedure, certify a transaction or become a receipt.
- Example: Telephone Messages
- Retention Period: Until no longer of administrative value, then destroy.

Category #2 – Intermediate Retention

- Have more significant administrative, legal and/or fiscal value but are not scheduled as transient or permanent.
- Examples: Internal and external correspondence, requests for information, documentation of ongoing projects and issues.
- Retention Period: 1 Year, then destroy.

Category #3 – Permanent Retention

- Have significant administrative, legal and/or fiscal value.
- Examples: Correspondence dealing with agency policies and programs, fiscal and personnel matters, department policies and procedures.
- Retention Period: 2 Years, then appraise for historical value or retain until superseded, obsolete or replaced.

13. BACKUP OF E-MAIL MESSAGES

For disaster recovery purposes, the Technology Department will backup E-mail to magnetic tape for offsite security storage. These "snapshot" security backup procedures are not designed to meet record retention requirements. See "Retention of E-mail Messages" for information on user responsibilities and compliance to E-mail retention requirements.

14. RESTORATION OF E-MAIL MESSAGES

Restoration of E-mail messages will be possible through the Technology Department, unless a message has been deleted by the user. See "Government in the Sunshine Law Adherence" for more information on public records law compliance.

15. E-MAIL DISTRIBUTION LISTS

Distribution lists are very useful tools when sending the same message to a group of users. The following rules should be adhered to when using distribution lists:

a) Maintenance of these distribution lists is the responsibility of the department that requests the creation of the list.
b) Think carefully before using a large distribution list. Ask yourself, "Do all E-mail users really need to know this information?"
c) When printing a message sent to a distribution list for retention in a paper file, print and file the distribution list along with the E-mail message.

16. USER ID TERMINATION

All user ID's will be revoked immediately upon a user's termination of employment with the district or upon the termination of whatever status gave the user access to the E-mail system. Within three months, the data associated with that user will be deleted including all files, records, notes, unopened mail, etc. The user's manager is responsible for: (1) notifying the Technology Department of the user's termination of relationship; and (2) requesting access to the former employee's stored E-mail to review for required retention of any official record material. Upon the termination of the user's relationship with the district, the user should no longer attempt to access the system.