

**MURFREESBORO CITY SCHOOLS
ADMINISTRATIVE DIRECTIVES**

Descriptor Term: E-mail Accounts and Individual Users' Data	Descriptor No: AD SS7	Effective Date: January 1999
Revised: 2/14; 7/14; 9/18; 3/24		

1 **E-mail Standards**

2 Murfreesboro City Schools (MCS) provides all full-time employees with a dedicated e-mail address
3 (ending in “cityschools.net”) to conduct business on behalf of the school district. Full-time employees
4 include interim teachers, and service provider interns. Exceptions to grant employees e-mail access may
5 be made on a case-by-case basis with their supervisor’s referral and approval from the Director of
6 Technology. This e-mail account should only be used for educational purposes, which include actions
7 directly promoting the educational, instructional, administrative, business, and/or support services of the
8 school district and are related to any instruction, project, job, work assignment, task, or function for which
9 the employee is responsible.

10 Employees may not use MCS e-mail to send any communication that is disruptive, obscene, pornographic,
11 profane, vulgar, threatening, or otherwise prohibited by law. Employees should refrain from including
12 political, religious, or commercial statements in their MCS e-mail unless its primary purpose is to support
13 the work of the school district. Employees may not use MCS e-mail to promote commercial or for-profit
14 entities or solicit business or compensation of any kind.

15 Employees may not use a personal e-mail address when communicating on behalf of MCS. If employees
16 receive a message in their personal e-mail account that is related to MCS business, that e-mail should be
17 forwarded to their MCS e-mail address and deleted from their personal e-mail.

18 Any e-mails, text messages, or other written communications made or received in connection with the
19 transaction of business involving MCS may be considered a public record pursuant to Board Policy 1.407
20 and TCA 10-7-503, or education record pursuant to Board Policy 6.600 and the Family Education Rights
21 and Privacy Act (FERPA), regardless of whether it was sent from a personal or MCS account.

22 MCS reserves the right to monitor, inspect, copy, review, and store, without prior notice, information
23 about the content and usage of e-mail accounts and any and all information transmitted or received in
24 connection with e-mail use. No employee has an expectation of privacy when using district e-mail. MCS
25 reserves the right to disclose any e-mail use to local law enforcement, Department of Children’s Services,
26 or other third party as appropriate or required by law.

27 All users of the district’s electronic resources are required to comply with Board policies and
28 administrative directives. Violation of any of the conditions of use may be cause for disciplinary action.

29 **E-mail Signatures**

30 In order to maintain consistency and professionalism, and decrease the data associated with individual e-
31 mails, the following guidelines apply to e-mail signatures used on MCS e-mail accounts. All e-mail
32 signatures are limited to the following information:

33 Employee Name, Job Title
34 School or Office Address
35 School or Office Phone Number
36 E-mail
37 District or school websites and/or social media accounts

38 MCS employees may use special stationery (electronic business card, V-Card, JPG, GIF, etc.) however
39 the special stationery must be limited to the above information and district- or school-related logos.
40 Quotations, sayings, religious, commercial or political statements should not be included as part of or
41 following an employee's e-mail signature.

42 Employees may add a confidentiality or legal disclaimer to their signature if frequently using e-mail to
43 communicate sensitive, legal, or otherwise confidential information.

44 **E-mail Security**

45 Employees are required to keep their MCS e-mail login credentials secure. Employees may not allow
46 other individuals use their MCS e-mail address, account, or password. Employees may be held
47 accountable for any action taken by or with their account.

48 MCS employees should report suspected phishing, as well as other suspicious or inappropriate use of data,
49 computer system abuse, or possible breaches of security. Each employee will be required to complete an
50 annual e-mail safety course. The Technology Department will conduct regular security audits with
51 simulated cyberattacks. In an effort to address vulnerabilities, employees who reply to or otherwise engage
52 in simulated phishing tests or other probes will be required to participate in additional security awareness
53 trainings. Failure to successfully complete these required trainings, will be considered insubordination
54 and the employee may be subject to discipline. Repeated failures will result in a referral to the Assistant
55 Superintendent of Operations.

56 Multi-factor authentication is a method of system access control in which a user is granted access only
57 after successfully providing at least two pieces of authentication. MCS uses DUO as its multi-factor
58 authentication application. MFA is required to be used by all employees who have a district-provided e-
59 mail address.

60 Access to e-mail or e-mail platforms will be terminated upon separation of the employee from MCS.
61 Access to e-mail or e-mail platforms will be suspended for employees on disciplinary suspension pending
62 the outcome of an investigation; the employee's access to their e-mail account will be re-instated following
63 the suspension.

64 **E-mail Retention**

65 E-mail sent or received using MCS Microsoft Outlook Mail accounts will be retained for a period of three
66 (3) years. Any e-mail messages over three (3) years old will be automatically deleted. Any e-mail that is
67 deleted will remain in the "Deleted Items" folder for ninety (90) days and will then be unrecoverable. For
68 supervisory staff, deleted e-mails will remain in the "Deleted Items" folder for one (1) year.

69 An e-mail message, including attachments, which requires retention beyond the scheduled deletion date
70 may be retained in Outlook Archive, which is not subject to automatic deletion rules. Employees are
71 responsible for identifying and saving documents that must be retained to comply with federal, state, or
72 local laws, and/or Board policies, or other legal obligations or pursuant to [record retention requirements](#)

73 of State or federal law or regulations. E-mail records appraised as “permanent” will be converted to paper,
74 microfilm, or another acceptable medium that meets State standards for permanent retention. E-mail
75 created or received by employees who resign, transfer, or are terminated will be subject to disposition on
76 a case-by-case basis as determined by the Director of Human Resources. Employees who are transferred
77 within the district as an administrative action may be assigned a new e-mail address.

78 The City Attorney’s office may also instruct employees not to delete electronically stored information, or
79 discard paper documents that must be preserved because they are relevant to potential or ongoing
80 litigation.