Retention of Electronic Records and Information

I. Policy

The Bethany Board of Education (Board) complies with all state and federal regulations regarding the retention, storage, and destruction of electronic information and records. The Superintendent or designee shall be responsible for developing and implementing administrative regulations concerning the retention, storage, and destruction of electronic information and the dissemination of such administrative regulations to all school officials, employees, and individuals granted access to the computer systems and/or networks of the Bethany Public School District (District) and/or who send electronic messages as part of their work for the District. Collectively, all individuals granted access to the District's computer systems are referred to as the "Users."

II. Use of Electronic Messages and Electronic Communications

The Board has installed computers and a computer network(s), including Internet access and electronic messaging systems, on Board premises and may provide other electronic devices that can access the network(s) and/or have the ability to send and receive messages with an operating system or network communication framework. Devices include but are not limited to, personal computing devices, cellular phones, Smartphones, network access devices, radios, personal cassette players, CD players, tablets, walkie-talkies, personal gaming systems, Bluetooth speakers, personal data assistants, and other electronic signaling devices. Electronic messaging systems include mobile, chat, and instant message; cloud collaboration platforms, including internal chat peer-to-peer messaging systems, and draft email message transfer; and other products that have the ability to create duration-based or subjective removal of content, such as Snapchat, and security focused platforms, such as Signal. The Board's computers, computer networks, electronic devices, Internet access, and electronic messaging systems are referred to collectively as "the computer systems" and are provided in order to enhance both the educational opportunities for our students and the business operations of the District.

Electronic messages sent by Users as part of their work and/or by using the District's computer systems and/or network(s) are not private communications and are potentially subject to disclosure, regardless of whether the messages are sent using personal devices or the District's computer systems. Users must understand that the Board has reserved the right to conduct monitoring of the District's computer systems and may do so *despite* the assignment to individual Users of passwords for system security. Any password systems implemented by the District are designed solely to provide system security from unauthorized users, not to provide privacy to the individual system User.

The system's security aspects, message delete function, and personal passwords may be bypassed for monitoring purposes. Therefore, **Users must be aware that they should not have any expectation of personal privacy in the use of these computer systems**. This provision applies to any and all uses of the District's computer systems, including any incidental personal use permitted in accordance with the Board's policy and regulations regarding computer use by Users.

Any retained messages may be retrieved as part of routine monitoring by the Board, an employee investigation, a search for documents pursuant to a Freedom of Information Act request, or a formal discovery process as part of litigation. Users should bear in mind that electronic messages may be retained at different locations within the computer network and that these messages are subject to retrieval, regardless of whether the User has deleted such messages from the User's accounts. Consequently, Users should use discretion when using computers or other electronic technology to send, record, or retain electronic messages and information.

III. Retention of Electronically Stored Information

Electronically stored information on District computers or electronic communication systems shall be retained only as long as necessary. The same record retention policy that applies to paper records applies to electronically stored information, including electronic messages. Therefore, like paper records, the content, and function of an electronic record, including electronic messages, determine the retention period for that document. The District will comply with all of the minimum standards set forth in the Municipal Records Retention Schedules, as issued by the Office of the Public Records Administrator for the State of Connecticut.

In addition to the retention guidelines established by the Board and used by District officials and employees, all District officials and employees have a duty to preserve all records and electronic information, including records and electronic information that might otherwise be deleted or destroyed, that relate to any matter that is currently in litigation or may be anticipated to involve future litigation.

Legal References: Connecticut General Statutes §§ 1-200(5), 1-211, 1-213(b)(3)

Connecticut General Statutes § 7-109

Connecticut General Statutes § 11-8 et seq.

General Letters 96-2 and 2009-2 of the Public Records Administrator

Record Retention Schedules Towns, Municipalities, and Boards of Education

Public Records Policy 01, Digital Imaging, of the Public Records Administrator (August 2014)

Connecticut State Library, Office of the Public Records Administrator, Authorization for Disposal of Original (Non-Permanent) Paper Records Stored as Digital Images, Form RC-075.1 (revised 12/2021)

Frequently Asked Questions about E-mail, CT Public Records Administrator, available at https://ctstatelibrary.org/wp-content/uploads/2015/05/EmailGuidelines.pdf.

Policy adopted: April 13, 2016
Policy revised: March 13, 2019
Policy revised: December 8, 2021
Policy revised: December 14, 2022

Source: Shipman