No. 252A

BLOOMSBURG AREA SCHOOL DISTRICT
Policy Manual

Section:	PUPILS
Title:	DISTRICT-PROVIDED TECHNOLOGY RESOURCES: STUDENT USE, RIGHTS AND RESPONSIBILITIES: STUDENT E-MAIL ACCOUNTS AND WEB AND CLOUD-BASED STORAGE AND WEB AND CLOUD-BASED APPLICATIONS
Date Adopted:	16 March 2015
Date Last Revised:	

252A. DISTRICT-PROVIDED TECHNOLOGY RESOURCES: STUDENT USE, RIGHTS AND RESPONSIBILITIES: STUDENT E-MAIL ACCOUNTS AND WEB AND CLOUD-BASED STORAGE AND WEB AND CLOUD-BASED APPLICATIONS

A. Introduction

The Bloomsburg Area School District (herein after "District") provides students with District-hosted file storage. The District also may provide student users with electronic mail accounts, web and cloud-based storage and certain web and cloud-based applications to enhance the District's educational program and facilitate communication.

Prior to creating an account for a student, the District will send notice to the parents/guardians advising them of the District's intent and including the privacy statement of the provider that the District uses. For students age 13 or older, if a parent/guardian does not notify the District in writing of his or her desire not to have such an account issued, then the District will create the account. For students under the age of 13, the District will provide the notice and obtain verifiable parental consent before creating the account.

B. Definitions

District-Provided Technology Resources – refers to internet access, local (District-hosted) resources and non-local resources to which access is provided through the District. It includes, but is not necessarily limited to the following:

1. BASD-Net (as defined below);
2. Network shared resources, such as printers;

3. Network folder shares and backup folders; and
4. Electronic mail, web-based and cloud-based storage, and web-based and cloud- based applications provided by the District through a third party.

For purposes of this policy, this term does not include District-provided devices (covered by the Policy cross-referenced below) or other equipment or supplies other than Network accessible resources.

E-mail Client Mailbox Items - include but are not limited to, the following: Calendar, Contacts, E-mail, Notes and Tasks.

End User Licensing Agreements – refers to the agreements which establish the District's right to use software which the District in turn provides to students for student use.

BASD-Net – refers to the District's technology network. The BASD-Net is to be used to provide access to information beyond what is available in school district libraries, to expand the research capabilities of students, and to promote the exchange of educational ideas and information. The BASD-Net is accessible by students on school campus.

Network Administrator - an Information System Professional responsible for the day-to-day maintenance and upkeep of BASD-Net and other District-Provided Technology Resources.

System Integrity – refers to the maintenance of accurate and consistent information throughout the BASD-Net and other District-Provided Technology Resources.

C. General

Students may be required to use email, web-based and cloud-based storage and other web-based and cloud-based applications in accordance with the restrictions set forth in Board Policy 252, all other Board Policies, and the End User Licensing Agreements, as defined above, as well as any applicable law.

Student email, web-based and cloud-based storage and web-based and cloud-based applications will not be systematically backed up or archived by the District. Therefore, any District policy, regulation or practice concerning document retention will not apply to this information. Students are responsible for taking appropriate steps to safeguard their data. Student emails to and from District employee email accounts will be archived pursuant to the Board policy and administrative regulation cross-referenced at the end of this regulation.

Students are responsible for the appropriate use of their account. Students must maintain the security of their passwords. Students will be assigned an ID and a password. If a student believes that his or her password has been compromised or that someone has accessed his or her account or

otherwise finds inappropriate material in the student's email, web-based storage or other web based applications, the student must immediately notify the building Tech Center (Policy 815).

D. Searches

Searches Generally

While the District does not routinely monitor email communications, District-hosted web- based or cloud-based storage or District-hosted, web-based and cloud-based applications, those resources are provided by the District; therefore, students do not have any expectation of privacy in information created on, stored on, accessed through or transmitted through these resources.

If the District has a reasonable suspicion that a student is violating District rules or policies, authorized District administrators shall search a student's District-provided electronic mail accounts, District-hosted or web-based or cloud-based storage and other web-based and cloud-based applications. "Reasonable suspicion" means that reasonable grounds exist that the search will uncover evidence that the student violated the law, school rules or District policies. The scope of the search must be reasonably related to the suspected violation which justified the search. Typically, the District will request that the student provide access to the account and perform or assist the District in performing the search. If reasonable suspicion exists and either (a) the student refuses to provide the District with access to his or her account to perform the search or (b) the circumstances are such that the search must be performed before the student is consulted, then the District may use its administrative access to force a change of the password to facilitate the access. The District may disable access to an account to prevent relevant information from being deleted from the account while a particular matter is being reviewed.

Searches Involving Suspected Sexually Explicit Visual Depictions of Students or Minors

Where the suspected violation of the School Disciplinary Code may in any way involve sexually explicit visual depictions of a student or students, no search shall be performed by District personnel of such student account unless: (1) in the event the student assigned to the account is 18 years of age or older, such student is notified; (2) in the event the student assigned to the account is less than 18 years of age, such student's parent(s) or guardian(s) is notified of the search. Furthermore, the following shall apply when a search is conducted:

1. After notice is provided, the student, parent(s) and/or guardian(s) may be present while the student account is being searched by the Principal or Technology Systems Administrator or their designee.

2. Where the student account is believed to contain depictions of a student who is not the student assigned to the account, then the student believed to be depicted, and the student's parent(s) or guardian(s) if the student is under 18 years of age, shall be notified and be provided the opportunity to be present during the search

of the student account. The parents of the student assigned to the account shall not be permitted to view the depictions without the consent of the student believed to be depicted as well as their parent(s) or guardian(s) if the student believed to be depicted is under 18 years of age.

Absent the above requests, such search shall only be performed by the Principal or Technology Systems Administrator or their designee when District personnel reasonably suspect that the Student's safety or the safety or privacy of another student or students is threatened. Any material or information obtained from the search of a student account may be provided to the appropriate authorities.

Records of Searches

The Technology Department will maintain a written record of District searches of student accounts, including, at a minimum, the following:

1. the date and time the account was accessed,
2. the name of the student whose account was accessed,
3. the individual requesting the access,
4. the reason that access was requested,
5. the signature of the student in the event that consent was given for the access,
6. the scope of the search,
7. the results of the search,
8. the person conducting the search.

In addition to periodically reviewing the written record of District searches of student accounts, and to the extent technologically practical, the Technology Systems Administrator will audit searches, no less than annually, to include the accounts that have been searched, the persons conducting the searches, and the date/time of the searches. The Technology Systems Administrator will report any significant findings to the Superintendent.

E. Searches for and Deletions of E-mail Client Mailbox Items Improperly Sent by Employees to Students

a. Any requests by any District employee for deletion of any E-mail Client Mailbox Items sent by a requesting employee to a student shall be directed to the Technology Systems Administrator.

i. The request shall state the basis upon which the employee requests deletion.

ii. Acceptable bases for deletion are:

1. E-mail Client Mailbox Item inadvertently sent to incorrect recipient; or
2. E-mail Client Mailbox Item sent to correct recipient but with an inadvertent, or otherwise unintended, attachment or attachments,

particularly if one or more of the attachments does or could compromise student or employee privacy or adversely affect District operations

iii. A log shall be maintained of each time an E-mail Client Mailbox Item is deleted pursuant to this section. The log shall contain the name of the individual requesting the deletion, the bases for the deletion, the name of the individual authorizing the deletion and the date and time of the deletion. The log shall be maintained for a period of at least seven years from the date of the deletion.

iv. The search for the E-mail Client Mailbox Item requested to be deleted shall be reasonably related in scope to the circumstances that formed the basis of the search.

v. If applicable, an E-mail Client Mailbox Item deleted pursuant to this section may be maintained in the sending employee's personnel file or other investigative file as evidence of employee or student misconduct.

Policy No. 252B, District-Issued Devices: Student Use, Rights, and Responsibilities

Policy No. 800, Records Management