Torrington Public Schools

Packet for Policy Committee Meeting

September 4, 2019

Torrington Public Schools

SUSAN M. LUBOMSKI
SUPERINTENDENT

SUSAN B. FERGUSSON
ASSISTANT SUPERINTENDENT

Policy Committee
Wednesday, September 4, 2019, 7:00 P.M.
355 Migeon Ave.

Agenda

Comments may be solicited at any time during the meeting as recognized by the Chair.

1. Call to Order
2. Roll Call
3. Approval of Agenda
4. Approval of Minutes
5. Public Participation: *Members of the public and staff may bring to the committee's attention information, ideas, or matters of concern related to all the duties and responsibilities of this committee. This committee will not allow comments regarding specific staff members or personal grievances. The time for individual remarks will be apportioned according to the number of speakers and will be limited to five minutes per speaker unless extended by the chair.*
6. Discussion and Next Steps
    a. Acceptable Use for Employees
    b. Visitors (and Observations in Schools)
7. Comments for the Good of the Order
8. Topics for Future Meetings
9. Adjournment

Future Meetings:
October 2nd – Vogel Wetmore
November 4th – Torringford
December 2nd – Southwest
January 8th – Forbes
February 5th – TMS
March 4th – THS

April 1st – Migeon Avenue
May 6th – Migeon Avenue
June 3rd – Migeon Avenue

Torrington Public Schools

SUSAN M. LUBOMSKI
SUPERINTENDENT

SUSAN B. FERGUSSON
ASSISTANT SUPERINTENDENT

Policy Committee Meeting
Wednesday, August 7, 2019, 7:00PM
Migeon Ave

DRAFT Minutes

1. Call to Order: 7:00PM
2. Roll Call: Ms. Hoehne, Mr. Kissko, Ms.Todor
   Also Present: Ms. Lubomski, Ms. Fergusson, Ms. Schulte
3. Approval of Agenda: Mr. Kissko made a motion to amend the agenda to add 6d. Policy - Reports of Suspected Abuse or Neglect of Children or Sexual Assault of Students by School Employees, second by Ms. Hoehne. All in favor.
4. Approval of Minutes: Mr. Kissko made a motion to approve the minutes, second by Ms. Hoehne. All in favor.
5. Public Participation: None.
6. Discussion and Next Steps:
   a. Abuse/Neglect of Disabled Adults – Currently we do not have this policy. Bring to the Full Board
   b. Employment Check Policy – update our current policy - #4006 (per Shipman) Bring to Full Board
   c. Dress Code (Personnel) – Create an Employee Committee to draft a District Wide Dress Code Policy. Committee to be set by September 30, 2019.
   d. Reports of Suspected Abuse or Neglect of Children or Sexual Assault of Students by School Employees. Currently we do not have this Policy. Bring to the Full Board
7. Comments for the Good of the Order: None.
8. Topics for Future Meetings:
   a. Acceptable Use for Employees
   b. Bullying
   c. Nepotism
9. Adjournment: Mr. Kissko made a motion to adjourn the meeting, second by Ms. Hoehne. All in favor. Meeting adjourned at 7:56PM.

Future: September 4th – Migeon Avenue
October 2nd – Vogel Wetmore
November 4th – Torringford

December 2nd – Southwest
January 8th – Forbes
February 5th – TMS
March 4th – THS
April 1st – Migeon Avenue
May 6th – Migeon Avenue
June 3rd – Miegeon Avenue

THE SCHOOL DISTRICT OF TORRINGTON, CONNECTICUT

Acceptable Use Policy

Access to Electronic Networks

Electronic networks, including e-mail and the internet, are a part of the District's instructional program and are designed to promote educational excellence. These networks are a resource for sharing work, innovation, learning and communication. The district shall develop a technology plan that shall include, but is not limited to, the integration of the internet into the curriculum, staff training, software filters, connectivity, and safety issues. The district and city are not responsible for any information that may be lost, damaged, or unavailable when using the network.

Purpose

This policy establishes the acceptable use of electronic network and computer tools provided by the City of Torrington, Torrington Public Schools, and Torrington Board of Education. It includes, but is not limited to computers, e-mail, and the internet.

Scope

This acceptable use policy applies to all BOE and TPS employees.

Acceptable Use Terms and Conditions

All use of the District's electronic network must be:

1) In support of education and be in furtherance of the Board of Education approved goals, or

2) For a legitimate school business purpose

The use of the network and equipment purchased by the district is a privilege and not a right. Students and staff have no expectation of privacy in any material that is stored, transmitted or received via the District's network or computers.

Usage Regulations and Procedures

1. Files, e-mail documents and other electronically stored material on the network and computers are not private. The employee must be aware that the district security systems are capable of recording (for each and every user) each World Wide Web site visit, each chat, news group, or e-mail message, and each file transfer into and out of our internal networks, and that TPS reserves the right to do so at any time. No employee should have any expectation of privacy in his or her internet or e-mail usage. The technology department will review internet and e-mail activity and analyze usage patterns, and TPS may choose to publicize this data to assure the internet and e-mail resources are devoted to maintaining the highest level of productivity.
2. TPS reserves the right to inspect any and all equipment, files(s), and e-mail stored in private areas of our network or on any computer in order to assure compliance with policy or in the normal course of business. Reason for inspection or review include, but are not limited

to: system, hardware or software problem, suspicion of crime or the need to perform work on equipment or provide service when an employee is not available.

3. TPS reserves the right to remove any files or software which are not approved by the district.
4. TPS network uses independently supplied software and data to identify inappropriate, obscene or sexually explicit internet sites. The District may block access from within our networks to all such sites of which we have knowledge. If you find yourself connected inadvertently to a site that contains sexually explicit or obscene material, you must disconnect from that site immediately, regardless of whether that site has been deemed acceptable by any screening or rating program. An employee who is denied access to any such site should contact a TPS technician if the information and data contained therein are required for work-related reasons.
5. TPS retains the copyright to any material posted to any forum, news group, and chat or World Wide Web page by any employee in the course of his or her duties.
6. TPS will comply with reasonable requests from law enforcement regulatory agencies for logs, diaries, and archives on an individual's internet e-mail activities.

Employees Responsibilities

TPS internet facilities, computing resources, and software shall not be used in an unacceptable manner. It is the employee's responsibility to familiarize himself/herself with this policy so as to ensure compliance.

1. All TPS facilities and computing resources, including all e-mail, must not be knowingly used to violate the laws and regulations of the United States or any other nation, or the laws and regulation of any state, city, province or other local jurisdiction in any material way. Use of resources for illegal activity is grounds for immediate dismissal, and we will cooperate with any legitimate law enforcement activity.
2. The display of any kind of obscene or sexually explicit image or document, as defined above, on a TPS system is a violation of our policy on sexual harassment. In addition, obscene or sexually explicit material may not be archived, stored, distributed, edited or recorded using our network or computing resources.
3. No employee may use TPS facilities to knowingly download or distribute pirated software or data.
4. No employee shall use TPS facilities to knowingly create, send, forward, download, print or store messages or graphic images which are harassing, threatening, intimidating, libelous, slanderous, discriminatory, or defamatory in nature.
5. No employee may use the TPS internet facilities to deliberately propagate any virus, worm, Trojan horse, or trap-door program code.
6. No employee may use the TPS internet facilities to disable or overload any computer system or network, or to circumvent any system intended to protect the privacy or security of another user.
7. Each employee using the internet facilities shall identify himself or herself honestly, accurately and completely (including one's TPS affiliation and function where requested). An employee, who releases their personal information, including personal identifying information, does so at their own risk.
8. Employees are reminded that chats and news groups are public forums where it is inappropriate to reveal confidential information, customer

data, trade secrets, and any other material covered by existing policies and procedures. Employees releasing protected information via news group or chat, whether or not the release is inadvertent, will be subject to all penalties under existing policies and procedures.

9. Use of internet access facilities to commit infractions such as misuse of assets or resources, sexual harassment, discrimination, unauthorized public speaking, misappropriation, or theft of intellectual property are also prohibited by general policy, and violators will be sanctioned under the relevant provisions of the policy and any applicable state and federal laws.
10. Since a wide variety of materials may be deemed offensive by colleagues, customers or suppliers, it is a violation of policy to store, view, print, or redistribute any document or graphic file that is not directly related to the user's job or business activities.

11. Employees with internet access may not use TPS internet facilities to download entertainment software or games, or to play games against opponents over the internet. Employees should also avoid using their personal software to play games, create inappropriate screen savers, etc.

12. Employees with internet access may not upload any software licensed to TPS or licensed by TPS without explicit authorization from TPS Technology Department .

13. Employees may not intentionally intercept, record, alter or receive another employee's e-mail. In addition, employees shall not send e-mail messages using another employee's I.D. or access the internet at another employee's computer.

14. No employee shall use a TPS computer, network or facilities for advertisement or conducting of business for profit, to distribute or advertise not related to school business.

15. TPS employees shall not subscribe to non-business related e-mail such as jokes/pictures/horoscope/prayer of the day, etc. The distribution of chain letters is forbidden.

16. No software may be installed or downloaded unless pre-approved by TPS Technology staff.

Violations

Violations of this policy will be reviewed on a case-by-case basis and can result in disciplinary action, up to, and including, suspension and termination. Any known or suspended violation of this policy shall be reported to the employee's immediate supervisor and thoroughly investigated. If necessary, this violation may be turned over to the appropriate authorities.

Receipt of Document/Acknowledgement

I acknowledge the receipt of a written copy of the Torrington Public Schools Acceptable Usage Policy. I understand all terms provided in this policy and agree to abide by them. I realize that Torrington Public Schools software may record and store for management use the electronic e-mail messages I send and receive the internet address of any site that I visit, and any computer network activity. I understand that any violation of this policy could have significant repercussions in my professional standing that might include, but is not limited to, my dismissal from employment.

Principal's Name (Print)	Employee's Name (Print)
Principal's Signature	Employee's Signature
Date	Date

Series 4000
Personnel

POLICY REGARDING EMPLOYEE USE OF THE DISTRICT'S COMPUTER SYSTEMS AND ELECTRONIC COMMUNICATIONS

Computers, computer networks, electronic devices, Internet access, and e-mail are effective and important technological resources. The Board of Education provides computers, a computer network, including Internet access and an e-mail system, and other electronic devices that access the network such as wireless and/or portable electronic hand-held equipment that can be used for word processing, wireless Internet access, image capture and recording, sound recording, information transmitting and/or receiving, storing, etc. (including, but not limited to, personal laptops, Smartphones, network access devices, Kindles, Nooks, cellular telephones, radios, personal cassette players, CD players, iPads or other tablet computers, walkie-talkies, Blackberries, personal data assistants, iPhones, Androids and other electronic signaling devices) (referred to collectively as "the computer systems"), in order to enhance both the educational opportunities for our students and the business operations of the district.

These computer systems are business and educational tools. As such, they are made available to Board employees for business and education related uses. The Administration shall develop regulations setting forth procedures to be used by the Administration in an effort to ensure that such computer systems are used for appropriate business and education related purposes.

In accordance with applicable laws and the Administrative Regulations associated with this Policy, the system administrator and others managing the computer systems may access email or monitor activity on the computer system or electronic devices accessing the computer systems at any time and for any reason or no reason. Typical examples include when there is reason to suspect inappropriate conduct or there is a problem with the computer systems needing correction. Further, the system administrator and others managing the computer systems can access or monitor activity on the systems despite the use of passwords by individual users, and can bypass such passwords. In addition, review of emails, messages or information stored on the computer systems, which can be forensically retrieved, includes those messages and/or electronic data sent, posted and/or retrieved using social networking sites, including, but not limited to, Twitter, Facebook, LinkedIn, YouTube, and MySpace.

All use of the District's computer systems/network must for a legitimate school business purpose.

Users should not have any expectation of personal privacy in the use of the computer system or other electronic devices that access the computer system. Use of the computer system represents an employee's acknowledgement that the employee has read and understands this policy and any applicable regulations in their entirety, including the provisions regarding monitoring and review of computer activity.

Legal References:

Conn. Gen. Stat. § 31-40x
Conn. Gen. Stat. § 31-48d
Conn. Gen. Stat. §§ 53a-182; 53a-183; 53a-250

Electronic Communication Privacy Act, 18 U.S.C. §§ 2510 through 2520

ADOPTED:_____
REVISED:_____

8/1/16

Series 4000
Personnel

ADMINISTRATIVE REGULATIONS REGARDING EMPLOYEE USE OF THE DISTRICT'S COMPUTER SYSTEMS AND ELECTRONIC COMMUNICATIONS

Introduction

Computers, computer networks, electronic devices, Internet access, and electronic mail are effective and important technological resources. The Board of Education has installed computers, a computer network, including Internet access and an e-mail system, and may provide electronic devices that access the system, such as personal laptops, Smartphones, I-Pads or other tablet computers, I-Phones, Androids or other mobile or handheld electronic devices, to enhance the educational and business operations of the district. In these regulations, the computers, computer network, electronic devices, Internet access and e-mail system are referred to collectively as "the computer systems."

These computer systems are business and educational tools. As such, they are being made available to employees of the district for district-related educational and business purposes. ***All users of the computer systems must restrict themselves to appropriate district-related educational and business purposes*.**

These computer systems are expensive to install, own and maintain. Unfortunately, these computer systems can be misused in a variety of ways, some of which are innocent and others deliberate. Therefore, in order to maximize the benefits of these technologies to the district, our employees and all our students, this regulation shall govern *all* use of these computer systems.

Monitoring

It is important for all users of these computer systems to understand that the Board of Education, as the owner of the computer systems, reserves the right to monitor the use of the computer systems to ensure that they are being used in accordance with these regulations. The Board of Education intends to monitor in a limited fashion, but will do so as needed to ensure that the systems are being used appropriately for district-related educational and business purposes and to maximize utilization of the systems for such business and educational purposes.

The system administrator and others managing the computer systems may access email or monitor activity on the computer system or electronic devices accessing the computer systems at any time and for any reason or no reason. Typical examples include when there is reason to suspect inappropriate conduct or there is a problem with the computer systems needing correction. Further, the system administrator and others managing the computer systems can access or monitor activity on the systems despite the use of passwords by individual users, and can bypass such passwords. In addition, review of emails, messages or information stored on the computer systems, which can be forensically retrieved, includes those messages and/or electronic data sent, posted and/or retrieved using social networking sites, including, but not limited to, Twitter, Facebook, LinkedIn, YouTube, and MySpace.

Notwithstanding the above and in accordance with state law, the Board may not: (1) request or require that an employee provide the Board with a user name and password, password or any other authentication means for accessing a personal online account; (2) request or require that an employee authenticate or access a personal online account in the presence of the Board; or (3) require that an employee invite a supervisor employed by the Board or accept an invitation from a supervisor employed by the Board to join a group affiliated with any personal online account of the employee. However, the Board may request or require that an employee provide the Board with a user name and password, password or any other authentication means for accessing (1) any account or service provided by Board or by virtue of the employee's employment relationship with the Board or that the employee uses for the Board's business purposes, or (2) any electronic communications device supplied or paid for, in whole or in part, by the Board.

In accordance with applicable law, the Board maintains the right to require an employee to allow the Board to access his or her personal online account, without disclosing the user name and password, password or other authentication means for accessing such personal online account, for the purpose of:

(A) Conducting an investigation for the purpose of ensuring compliance with applicable state or federal laws, regulatory requirements or prohibitions against work-related employee misconduct based on the receipt of specific information about activity on an employee's personal online account; or

(B) Conducting an investigation based on the receipt of specific information about an employee's unauthorized transfer of the Board's proprietary information, confidential information or financial data to or from a personal online account operated by an employee or other source.

For purposes of these Administrative Regulations, "personal online account" means any online account that is used by an employee exclusively for personal purposes and unrelated to any business purpose of the Board, including, but not limited to, electronic mail, social media and retail-based Internet web sites. "Personal online account" does not include any account created, maintained, used or accessed by an employee for a business purpose of the Board.

Why Monitor?

The computer systems are expensive for the Board to install, operate and maintain. For that reason alone it is necessary to prevent misuse of the computer systems. However, there are other equally important reasons why the Board intends to monitor the use of these computer systems, reasons that support its efforts to maintain a comfortable and pleasant work environment for all employees.

These computer systems can be used for improper, and even illegal, purposes. Experience by other operators of such computer systems has shown that they can be used for such wrongful purposes as sexual harassment, intimidation of co-workers, threatening of co-workers, breaches of confidentiality, copyright infringement and the like.

Monitoring will also allow the Board to continually reassess the utility of the computer systems, and whenever appropriate, make such changes to the computer systems as it deems fit. Thus, the Board monitoring should serve to increase the value of the system to the district on an ongoing basis.

Privacy Issues

Employees must understand that the Board has reserved the right to conduct monitoring of these computer systems and can do so *despite* the assignment to individual employees 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 can be bypassed for monitoring purposes.

Therefore, *employees 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 and electronic devices that access same, including any incidental personal use permitted in accordance with these regulations.

Use of the computer system represents an employee's acknowledgement that the employee has read and understands these regulations and any applicable policy in their entirety, including the provisions regarding monitoring and review of computer activity.

Prohibited Uses

Inappropriate use of district computer systems is expressly prohibited, including, but not limited to, the following:

- Sending any form of solicitation not directly related to the business of the Board of Education;

- Sending any form of slanderous, harassing, threatening, or intimidating message, at any time, to any person (such communications *may* also be a *crime*);

- Gaining or seeking to gain unauthorized access to computer systems;

- Downloading or modifying computer software of the district in violation of the district's licensure agreement(s) and/or without authorization from supervisory personnel;

- Sending any message that breaches the Board of Education's confidentiality requirements, including the confidentiality rights of students;

- Sending any copyrighted material over the system;

- Sending messages for any purpose prohibited by law;

- Transmission or receipt of inappropriate e-mail communications or accessing inappropriate information on the Internet, including vulgar, lewd or obscene words or pictures;

- Using computer systems for any purposes, or in any manner, other than those permitted under these regulations;

- Using social networking sites such as Facebook, Twitter, MySpace and LinkedIn in a manner that violates the Board's Social Networking policy.

- Using social networking sites such as Facebook, Twitter, MySpace and LinkedIn in a manner that disrupts or undermines the effective operation of the school district; is used to engage in harassing, defamatory, obscene, abusive, discriminatory or threatening or similarly inappropriate communications; creates a hostile work environment; breaches confidentiality obligations of school district employees; or violates the law, Board policies and/or the other school rules and regulations.]

In addition, if a particular behavior or activity is generally prohibited by law and/or Board of Education policy, use of these computer systems for the purpose of carrying out such activity and/or behavior is also prohibited.

Electronic Communications

The Board expects that all employees will comply with all applicable Board policies and standards of professional conduct when engaging in any form of electronic communication, including texting, using the district's computer system, or through the use of any electronic device or mobile device owned, leased, or used by the Board. As with any form of communication, the Board expects district personnel to exercise caution and appropriate judgment when using electronic communications with students, colleagues and other individuals in the context of fulfilling an employee's job-related responsibilities.

Disciplinary Action

Misuse of these computer systems will not be tolerated and will result in disciplinary action up to and including termination of employment. Because no two situations are identical, the Board reserves the right to determine the appropriate discipline for any particular set of circumstances.

Complaints of Problems or Misuse

Anyone who is aware of problems with or misuse of these computer systems, or has a question regarding the appropriate use of the computer systems, should report this to his or her Administrator.

Most importantly, the Board urges *any* employee who receives *any* harassing, threatening, intimidating or other improper message through the computer systems to report this immediately. It is the Board's policy that no employee should be required to tolerate such treatment, regardless of the identity of the sender of the message. *Please report these events!*

Implementation

This regulation is effective as of __/__/__.

Legal References:

Conn. Gen. Stat. § 31-40x
Conn. Gen. Stat. § 31-48d
Conn. Gen. Stat. §§ 53a-182; 53a-183; 53a-250

Electronic Communication Privacy Act, 18 U.S.C. §§ 2510 through 2520

8/1/16

[Note: Although we have included this sample notice in our model policy documents for the convenience of our Board of Education clients, the notice does not need to be approved as a Board policy].

NOTICE REGARDING ELECTRONIC MONITORING

[To be posted in a conspicuous place readily available for viewing by employees]

In accordance with the provisions of Connecticut General Statutes Section 31-48d, the Board of Education hereby gives notice to all its employees of the potential use of electronic monitoring in its workplace. While the Board may not actually engage in the use of electronic monitoring, it reserves the right to do so as the Board and/or the Administration deem appropriate in their discretion, consistent with the provisions set forth in this Notice.

"Electronic monitoring," as defined by Connecticut General Statutes Section 31-48d, means the collection of information on the Board's premises concerning employees' activities or communications, by any means other than direct observation of the employees. Electronic monitoring includes the use of a computer, telephone, wire, radio, camera, electromagnetic, photoelectronic or photo-optical systems. The law does not cover the collection of information (A) for security purposes in any common areas of the Board's premises which are open to the public, or (B) which is prohibited under other state or federal law.

The following specific types of electronic monitoring may be used by the Board in its workplaces: **[modify as appropriate for the school district in question]**

- Monitoring of e-mail and other components of the Board's computer systems, including monitoring of electronic devices such as PDAs, Smartphones, and mobile or handheld devices that access the computer systems, for compliance with the Board's policies and regulations concerning use of such systems.

- Video and/or audio surveillance within school buildings (other than in restrooms, locker rooms, lounges and other areas designed for the health or personal comfort of employees or for the safeguarding of their possessions), on school grounds and on school buses and other vehicles providing transportation to students and/or employees of the school system.

- Monitoring of employee usage of the school district's telephone systems.

The law also provides that, where electronic monitoring may produce evidence of misconduct, the Board may use electronic monitoring without any prior notice when the Board has reasonable grounds to believe employees are engaged in conduct that (i)

violates the law, (ii) violates the legal rights of the Board or other employees, or (iii) creates a hostile work environment.

Questions about electronic monitoring in the workplace should be directed to the Superintendent.

Legal References:

Connecticut General Statutes:
Section 31-48b
Section 31-48d

8/1/16

Series 1000
Community/Board Operation

POLICY REGARDING VISITORS AND OBSERVATIONS IN SCHOOLS

The _____Board of Education (the "Board") encourages visits by citizens, taxpayers, and parents to all school buildings. In order to promote a safe and productive educational environment for all students and staff, the Board requires all visitors to receive prior approval from the school Principal or his/her designee before being permitted to visit any school building. The Board, through the administration, reserves the right to limit visits in accordance with administrative regulations.

Upon arrival, all visitors and observers must comply with any and all applicable building security procedures, including but not limited to utilizing security buzzers for access, complying with requests for photo identification, reporting directly to and signing in and out at the visitors' reception area of the school office, prominently displaying visitors' badges or other identification required for visitors to the school buildings, limiting access to those areas of the buildings and grounds for which the visitors/observers have authorized access, and complying with directives of school officials at all times.

ADOPTED: _____
REVISED: _____

8/12/18

SHIPMAN & GOODWIN LLP®
COUNSELORS AT LAW

Series 1000
Community/Board Operation

ADMINISTRATIVE REGULATIONS REGARDING VISITORS AND OBSERVATIONS IN SCHOOLS

1. Any person wishing to visit a school building, and/or observe any student program, must obtain prior approval from the building Principal or responsible administrator of the respective school building or program.

2. A visitor to any school building or program must be able to articulate a legitimate reason for his/her proposed visit and/or observation. Where the visitation involves direct contact with district students, or observation of an identified student or student program, the visitor must have a sufficient educational nexus with the district, its educational programs or the student to support such request.

3. All visits must be reasonable in length and conducted in a manner designed to minimize disruption to the district's educational programs.

4. When a parent/guardian makes a request to observe an identified student or student program, the request will be reviewed with the student's parent/guardian to determine the purpose of the observation, specific questions being addressed, the location(s) of the observation, and the date, time and length of the observation.

5. When determining whether to approve a request to visit and/or observe individual students or student programs, the building Principal or responsible administrator shall consider the following factors:

    a. the frequency of visits;

    b. the duration of the visit;

    c. the number of visitors involved;

    d. the effect of the visit on a particular class or activity;

    e. the age of the students;

    f. the nature of the class or program;

g. the potential for disclosure of confidential personally identifiable student information;

h. whether the visitor/observer has a legitimate educational interest in visiting the school;

i. whether the visitor/observer has professional ethical obligations not to disclose any personally identifiable student information;

j. any safety risk to students and school staff; and

6. The building Principal or responsible administrator has the discretion to limit, or refuse, requests for visits and/or observations of student programs in light of the above criteria. When a requested observation is refused, the building Principal or responsible administrator will provide the parent/guardian with the reason for the decision and will work to develop alternative ways for the parent/guardian to obtain the information the parent/guardian seeks.

7. If a building Principal or responsible administrator approves a request to visit a school building and/or observe a student program, arrangements must be made in advance to ensure that the visit will not disrupt educational programs. The length and scope of any visit shall be determined by the building Principal or responsible administrator in accordance with these regulations and accompanying Board policy. The building Principal or responsible administrator shall determine a reasonable amount of time for observations of individual students or student programs.

8. Upon arrival, all visitors must comply with any and all applicable building security procedures, including but not limited to utilizing security buzzers for access, complying with requests for photo identification, reporting directly to and signing in and out at the visitors' reception area of the school office, prominently displaying visitors' badges or other identification required for visitors to the school buildings, limiting access to those areas of the buildings and grounds for which the visitors have authorized access, and complying with directives of school officials at all times.

9. The district has an obligation to maintain the confidentiality of personally identifiable student information. All visitors and observers must restrict their visits and observations to the purpose identified in the request to visit or observe and are strictly prohibited from observing or collecting information on other students within the school. If the visitor/observer views, accesses or otherwise obtains personally identifiable student information concerning another student, the visitor/observer must notify the building Principal or responsible administrator as soon as possible.

10. A refusal to comply with any of the Board's policy provisions and/or regulations concerning visitors shall constitute grounds for denial of the visitor's privileges, as determined appropriate by the building Principal or designee. Such refusal may also result in a referral to law enforcement personnel, as determined appropriate by the building Principal or designee.

ADOPTED: _____
REVISED: _____

8/12/18