Washington Central Unified Union School District

WCUUSD exists to nurture and inspire in all students the passion, creativity and power to contribute to their local and global communities.

1130 Gallison Hill Road
Montpelier, VT 05602
Phone (802) 229-0553
Fax (802) 229-2761

Bryan Olkowski.
Superintendent

Berlin East Montpelier Calais
U- 32
Middlesex Worcester

WCUUSD Policy Committee
Meeting Agenda
4.27.21 4:30-6:30 pm
https://tinyurl.com/zn4jzepj
Meeting ID: 828 3725 2616
Passcode: 370651
Dial by your location: 1-929-205-6099

Via Video Conference*

1. Call to Order

2. Approve Minutes of 4.12.21 – pg. 2

3. Review Technology Policies
   3.1. F44 Password Management Policy – pg. 5
   3.2. F45 Acceptable Use – pg. 8
   3.3. B8 Electronic Communication Between Employees and Students – pg. 11

4. Future Agenda Items
   4.1. School Choice Policy
   4.2. Memorials Policy
   4.3. Family Request to Remain in School at End of Year

5. Adjourn

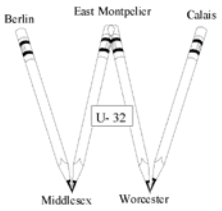
***Open Meeting Law temporary changes as of 3/30/20: Boards are not required to designate a physical meeting location. Board members and staff are not required to be present at a designated meeting location. Our building will not be open for meetings. All are welcome to attend virtually.**

Washington Central Unified Union School District

WCUUSD exists to nurture and inspire in all students the passion, creativity and power to contribute to their local and global communities.

1130 Gallison Hill Road
Montpelier, VT 05602
Phone (802) 229-0553
Fax (802) 229-2761

Bryan Olkowski
Superintendent



WCUUSD Policy Committee
Meeting Minutes Unapproved
4.12.21 5:15-7:15 pm

Present: Superintendent Bryan Olkowski, Michelle Ksepka, Jim Garrity, Chris McVeigh, Jody Emerson, Dorothy Naylor, Aaron Boynton, Christina Pollard

1. **Call to Order: Chris McVeigh called the meeting to order at 5:21 p.m.**

2. **Approve Minutes of 3.30.21: Christina Pollard moved to approve the minutes of March 30, 2021. This motion carried unanimously.**

3. **Review Technology Policies:**
   - **3.1. D3 District Take Home Device and Personal Device Policy**: Jim Garrity introduced this draft policy. Chris McVeigh asked for input around the language indicating "It is expected that…." is that strong enough? Jody Emerson indicated that students are required to sign an acceptable use agreement. She believes that the content of this policy is covered in the agreement. Some discussion followed around the language around replacement costs. Sentence on page 3 of the policy draft: "Physical damage…" Suggested: "replacement fee consistent with the acceptable use agreement" "replacement fee equal to the cost to replace the equipment" The committee agreed to edit that sentence to read: *"Physical damage or lost equipment may cost a student or employee a replacement fee."* Chris McVeigh asked whether we should consider putting language in the policy to differentiate between purposeful damage to equipment versus accidental. In the acceptable use policy, the school administrator determines the extent of damage. The committee agreed to leave the language in this policy vague and use the edited sentence as noted above. The committee recommended to bring this policy to the board. **Christina Pollard moved to bring this policy D3 to the school board, as edited tonight. Seconded by Chris McVeigh, this motion carried unanimously.**
   - **3.2. F44 Password Management Policy:** Jim Garrity introduced this policy. He had crafted it based on resources from National Institute of Standards and Technology. Jody Emerson stated that this policy seemed very procedural. She wondered if the policy itself could be more vague and the procedures around password management could be updated as needed and as explicit as needed. Chris McVeigh asked whether this policy will compel a change in behavior. Jim Garrity stated that, for example, "Shared Passwords" is an area that needs change. The committee

agreed to revisit this policy at the next meeting, and consider a draft policy that is brief, the Standard Operating Procedure is more explicit.

3.3. **F45 Acceptable Use:** Jim Garrity introduced this policy. Chris McVeigh asked whether this policy is consistent with what we already have in place. Jody Emerson stated that she believes it is probably consistent with the law; however this policy spells it out and makes it very clear to employees. Suggestion to eliminate "with or without consent" and simply state "without consent." Chris McVeigh indicated that the entire statement about "no expectation of privacy" should be highlighted so that staff knows this very explicitly. Chris McVeigh asked, does there need to be a trigger, for a search like this? He would like to have language in the policy that explains what might cause such a trigger. Language should read "All searches of this nature will only be conducted with the approval of the Superintendent or the Superintendent's designee." Jim Garrity suggested creating a new policy about electronic searches at the district, to spell out clarity around this issue. Chris McVeigh asked staff members how they are currently notified about the potential of this type of search. Jody Emerson indicated that she believes it is part of the staff handbook and is reviewed during new staff training, but it is not something that is regularly discussed. Chris McVeigh suggested, "WCUUSD reserves the right, through decision by Superintendent or Superintendent's designee, to turn over potentially illegal material to law enforcement for civil and or criminal action." The committee discussed requiring subpoena or the consent of the parent provided for any student under 18 years old. Chris McVeigh asked, once a student turns 18, can a parent still provide consent for a search, or does it need to come from the student? The committee will revisit this policy with updated language after consulting legal counsel.

3.4. **F47 Electronic Mail:** Jim Garrity explained that email is traditionally an unsecure platform. Bryan Olkowski spoke about the need to explain FERPA, HIPPA and FOIA within this policy. Chris McVeigh reminded him to change the language from "company" to "district." Jody Emerson asked whether some of the policies could be included into one, for example, passwords and this email policy. Superintendent Olkowski indicated that if it is going to include language around FERPA, HIPPA and FOIA then it might be better as a "stand alone" policy. Dorothy Naylor indicated that she believes it is important for staff to be aware of the FERPA, HIPPA and FOIA details. She would advocate for the simplest way to get this information across to people. Christina Pollard agreed with Dorothy's points. She suggested putting this information in more than one place as needed, to be sure that staff are aware: err on the side of providing more information/ protection. Chris McVeigh agreed with the idea of keeping this policy as a stand-alone policy, and to include the details around FERPA, HIPPA and FOIA as discussed, in other places of access. This policy will go, as edited, to the next board meeting, for board's consideration. **Dorothy Naylor moved to forward this policy, as amended, to the WCUUSD board for consideration. Seconded by Christina Pollard, this motion carried.**

3.5. **F48 Incident Response Policy and Plan:** Jim Garrity reviewed this policy. **Dorothy Naylor moved to forward this policy to the WCUUSD board for consideration. Seconded by Christina Pollard, this motion carried unanimously.**

3.6. **B8 Electronic Communication between Employees and Students**: The committee will discuss this policy at the next meeting.

4. **Future Agenda Items:**
   4.1. School Choice Policy
   4.2. Memorials Policy

   Superintendent Olkowski brought up the idea of having a policy to address enrollment in the middle of the school year. The committee will address this at a future meeting.
   Next Meeting: April 27, 4:30 - 6:30

5. **Adjourn:** The meeting adjourned by consensus at 7:13 p.m.

   Respectfully submitted,
   Lisa Stoudt, Committee Recording Secretary

Recommended

WASHINGTON CENTRAL UNIFIED UNION SCHOOL DISTRICT

Board of Directors' Policy

PASSWORD MANAGEMENT

POLICY: F44

WARNED: _____

ADOPTED: _____

EFFECTIVE: _____

Overview

Strong and consistent management of user IDs and passwords enables the WCUUSD to authenticate individual users, trace actions to users, and fully utilize the secure features of the network and system infrastructure of the organization and to protect sensitive information to the fullest extent practical. All employees and personnel that manage or have access to systems and networks must adhere to the password policies defined below in order to protect the security of sensitive information and data.

Purpose

This policy applies to any and all personnel who have any form of user or administrator account requiring a password on any network, system, or system component.

Scope

The scope of this policy includes all personnel who have or are responsible for an account (or any form of access that supports or requires a password) on any system that resides at any WCUUSD facility, has access to the WCUUSD network, or stores any non-public WCUUSD information.

User ID & Password

User-IDs and Passwords: WCUUSD requires that each service user accessing multi-user information systems have a unique user-ID and a private password. The unique user-ID and in some cases, the initial password will be issued by WCUUSD Information Technology Department. All issued passwords must be changed at first login and is enforced through group policy. These user-IDs must then be employed to restrict system privileges based on job duties, project responsibilities, and other business activities. Each service user is personally responsible for the usage of his or her user-ID and password. All activity logged under a user account is the responsibility of the user who owns the account.

Role Accounts/Anonymous User-IDs: With the exception of electronic bulletin boards, Internet web sites, and other systems where all regular users are intended to be anonymous, users are prohibited from logging into any WCUUSD system or network anonymously. Anonymous access might, for example, involve use of "guest" user-IDs. When users employ system commands that allow them to change active user-IDs to gain certain privileges, they must have initially logged-in employing user-IDs that clearly indicated their identities. This might, for example, take place on UNIX systems with the SU command. Demonstration software and/or demonstration systems for customers are exempt in that a customer may access the system anonymously; however, all

administrative tasks performed by WCUUSD employees, representatives, contractors, or otherwise must not be anonymous.

Difficult-to-Guess Passwords: To ensure that password systems do the job they were intended to do; users must choose passwords that are difficult-to-guess. This means that passwords must NOT be related to one's job or personal life. For example, a car license plate number, a spouse's name, or fragments of an address must not be used. This also means passwords must not be a word found in the dictionary or some other part of speech. For example, proper names, places, technical terms, and slang must not be used. The password "WCUUSD" must never be used (regardless of upper or lower case) on network (public or private) connected systems, even for demonstration accounts or public access. The password length must be a minimum of eight alphanumeric characters with the maximum number of characters being system dependent. Creating passwords that are at least 15 characters or more can ensure a more secure environment. If words are used in your password, ensure that you are using non-compound words.

Random Characters Must Be Used: At least one special character and one numeric character should be used to increase the difficulty in guessing passwords. An example would be the numeric character '3' in place of the letter 'E'. Special and Numeric characters include numbers, punctuation marks, and delimiting characters such as the "@" symbol.

Passwords Change Frequency: Passwords should only be changed when there is a reason to believe that a password has been compromised. Changes should occur every year for privileged accounts. This must be enforced by software controls on multi-user systems and within the Active Directory domain. Additionally, passwords must not be re-used. All multi-user systems, which have the capability to prevent the re-use of passwords, will not allow a user to enter a password that has been recently used, within 5 uses. Additionally, software controls may be employed that prevent the repeated changing of passwords to facilitate the minimum number of changes within a short period of time.

Password Storage: Passwords must not be stored in readable form in batch files, automatic log-in scripts, software macros, terminal function keys, in computers without access control systems, or in other locations where unauthorized persons might discover them. Similarly, passwords must not be written down in some readily decipherable form and left in a place where unauthorized persons might discover them.

Sharing Passwords: If users need to share computer-resident data, they should use electronic mail, group-ware databases, public directories on local area network servers, and other similar mechanisms. Although user-IDs are shared for electronic mail and other purposes, passwords must never be shared with or revealed to others. Users should not disclose passwords to administrative staff or to managers, even when requested to do so – the password for a user account is not required for administrative purposes and any request for your password should be viewed as suspicious. The exception to this is the `Administrator' or `root' password, which is shared by users who require special access. Sharing a password (or any other access mechanism such as a dynamic password token) exposes the authorized user to responsibility for actions that the other party takes using the disclosed password. If a service user believes that someone else is using his or her user-ID and password, the service user must immediately notify the administrator for the information system in question. If a password is discovered written down in an easily accessible location (for example on a whiteboard, or written on a sticky note attached to the bottom of a keyboard) the account will be treated as if it had been disclosed and will be disabled.

Multi-Factor Authentication
The implementation of Multi-factor authentication is highly encouraged whenever applicable not only for work accounts but for personal accounts too.

Privileged User-IDS and Passwords: Certain privileged accesses on production systems require the use of the administrative or Super-User (root) accounts. Knowledge and use of such user-IDS shall be restricted to a need-to-know basis. All users granted such access shall have their names added to the authorized administrative user list and shall be removed when access is no longer required. If a privileged user-ID/password has been determined to be compromised, then the scope of the compromise must be assessed and all passwords relating to the compromised system must be changed as appropriate.

Password Policy Conformance Auditing: From time to time the Information Technology Department or the Security Team may audit the multi-user computer systems for password policy conformance. If a password is not long enough (16+ characters) or does not contain enough special characters or is based on a dictionary word and is easily guessed, the account related to the weak password will be required to choose a more secure password. Audits may also include checking the vicinity of one's workspace for passwords that have been written down (sticky note on keyboard) but will not include a search of personal effects or within desk drawers.

Password Account Blocking: After six consecutive login failures an account will be blocked from further access for a minimum of 30 minutes (not including Network Infrastructure). If a user has had an account disabled in such a manner, they must contact the Information Technology Helpdesk following the IT Support Request Process to have the account re-enabled if it is necessary for the account to be accessible within the lockout time frame.

Violations of Password Policy: In the event that a password has been disclosed, either by accident or by the negligence of a user, the account in question must be disabled. In order for a service user to regain access to computing resources, an internal ticket request must be submitted by the user's manager before the account may be re-enabled for their use. Repeated violations or disclosure of access control information to an outside party will result in disciplinary action up to and including termination of employment. If your account has been disabled or you suspect that it has been disclosed, please immediately contact the Help Desk (ithelp@u32.org)

Recommended

WASHINGTON CENTRAL UNIFIED UNION SCHOOL DISTRICT

Board of Directors' Policy

ACCEPTABLE USE POLICY

POLICY: F45

WARNED: _____

ADOPTED: _____

EFFECTIVE: _____

Overview

WCUUSD's intentions for publishing an Acceptable Use Policy are not to impose restrictions that are contrary to WCUUSD's established culture of openness, trust and integrity. IT is committed to protecting WCUUSD's employees, partners and the company from illegal or damaging actions by individuals, either knowingly or unknowingly.

The question of Internet safety includes issues regarding the use of the Internet, Internet-capable computing devices, and other electronic devices in a manner that promotes safe online activity for children, protects children from cybercrimes, including crimes by online predators and cyberbullying, and helps parents shield their children from materials that are inappropriate for minors. To promote the safe and appropriate online behavior of students and staff as they access material from the Internet, the district will use the following four-part approach. However, given the ever-changing nature of the Internet, the district cannot guarantee that a student will never be able to access objectionable material.

Internet/Intranet/Extranet-related systems, including but not limited to computer equipment, software, operating systems, storage media, network accounts providing electronic mail, WWW browsing, and FTP, are the property of WCUUSD. These systems are to be used for business purposes in serving the interests of the company, and of our clients and customers in the course of normal operations. Please review Human Resources policies for further details.

Effective security is a team effort involving the participation and support of every WCUUSD employee and affiliate who deals with information and/or information systems. It is the responsibility of every computer user to know these guidelines, and to conduct their activities accordingly.

It is the responsibility of every computer user to know these guidelines, and to conduct their activities accordingly.

Purpose

This policy applies to employees, contractors, consultants, temporary and other workers, including all personnel affiliated with third parties. This policy applies to all equipment that is owned and/or leased by WCUUSD.

Scope

This policy applies to the use of information, electronic and computing devices, and network resources to conduct WCUUSD business or interact with internal networks and business systems, whether owned or leased by WCUUSD, the employee, or a third party. All employees, contractors, consultants, temporary, and other workers at WCUUSD and its subsidiaries are responsible for exercising good judgment regarding appropriate use of information, electronic devices, and network resources in accordance with WCUUSD policies and standards, and local laws and regulation. This policy applies to employees, contractors, consultants, temporaries, and other workers at WCUUSD, including all personnel affiliated with third parties. This policy applies to all equipment that is owned or leased by WCUUSD.

Right to Search and Monitor – No Expectation of Privacy

To ensure compliance with WCUUSD internal policies as well as applicable laws and regulations, and to ensure service user safety, WCUUSD administration reserves the right to monitor, inspect, and/or search at any time all WCUUSD information systems. This examination may take place with or without the consent, presence, or knowledge of the involved service users. The information systems subject to such examination include, but are not limited to, electronic mail system files, personal computer hard drive files, voicemail files, printer spool files, fax machine output, desk drawers, and storage areas. All searches of this nature will be conducted after the approval of the Legal and Human Resources Departments.

All district-owned and personally owned Internet-capable devices in all district facilities accessing the Internet through district network resources will be filtered and monitored to prevent access to obscene, racist, hateful, violent, or other objectionable material as specified in the FCC Children's Internet Protection Act or district policies.

Since WCUUSD's computers and networks are provided for business purposes only, service users should have no expectation of privacy associated with the information they store in or send through these information systems. WCUUSD administration additionally retains the right to remove from its information systems any material it views as offensive or potentially illegal. WCUUSD reserves the right to turn over potentially illegal material to law enforcement for civil and or criminal prosecution.

Internet Access / Acceptable Use for Personal Activity

Service users are generally provided with Internet access to perform their job duties, but this access may be terminated at any time at the discretion of a service user's supervisor. Service users must take special care to ensure that they do not represent WCUUSD in an official capacity on Internet discussion groups and in other public forums, unless they have previously received administration authorization to act in this capacity. All information received from the Internet should be considered

to be suspect until confirmed by reliable sources; there is a great deal of inaccurate and deliberately misleading information available on the Internet. Separately, service users must not place WCUUSD material (software, internal memos, press releases, databases, etc.) on any publicly accessible computer system such as the Internet, unless both the information Owner and the Information Technology Department have first approved the posting. On a related note, sensitive information must not be sent across the Internet unless it is in encrypted form.

Supervision

When students and staff access the Internet from any district facility, district staff will make a reasonable effort to supervise student access and use of the Internet. If material is accessed that violates district policies, procedures and/or the network use agreement, then district staff may instruct the person to cease using that material and/or implement sanctions contained in district policies, procedures and/or the network use agreement.

Unbecoming Conduct

Prohibited Activities: Users must not test or attempt to compromise computer or communication system security measures unless specifically approved in advance and in writing by the WCUUSD IT Team or is specifically a part of their job duties. Incidents involving unapproved system cracking (hacking), password cracking (guessing), file decryption, bootleg software copying, or similar unauthorized attempts to compromise security measures may be unlawful and will be considered serious violations of WCUUSD internal policy. Likewise, short-cuts bypassing systems security measures, as well as pranks and practical jokes involving the compromise of systems security measures are absolutely prohibited.

Harassing or Offensive Materials: WCUUSD computer and communications systems are not intended to be used for and must not be used for the exercise of the service users' right to free speech. Sexual, ethnic, and racial harassment --including unwanted telephone calls, electronic mail, and internal mail -- is strictly prohibited and is cause for disciplinary action up to and including termination of employment. Service users are encouraged to promptly report the communications to their manager and the Human Resources Department. WCUUSD retains the right to remove from its information systems any material it views as offensive or potentially illegal.

Appropriate Behavior: To avoid legal problems, whenever any affiliation with WCUUSD is included with an Internet message or posting, "flaming" or similar written attacks are strictly prohibited. Likewise, service users must not make threats against another user or organization over the Internet. All Internet messages intended to harass, annoy, or alarm another person are similarly prohibited.

Business Activities not Related to WCUUSD: It will be a violation of policy for any user to conduct business other than that of Washington Central Unified Union School District on WCUUSD Information Systems.

Required

WASHINGTON CENTRAL UNIFIED UNION SCHOOL DISTRICT

Board of Directors' Policy

ELECTRONIC COMMUNICATION BETWEEN EMPLOYEES AND STUDENTS

POLICY: B8

WARNED: _____

ADOPTED: _____

EFFECTIVE: _____

I. Statement of Policy

The Washington Central Unified Union School District (WCUUSD) recognizes electronic communications, and the use of social media outlets create new options for extending and enhancing the educational program of the school district. Electronic communications and the use of social media can help students and employees communicate regarding: questions during non-school hours regarding homework or other assignments; scheduling issues for school-related co-curricular and interscholastic athletic activities; school work to be completed during a student's extended absence; distance learning opportunities; and other professional communications that can enhance teaching and learning opportunities between employees and students. However, the WCUUSD recognizes employees and students can be vulnerable in electronic communications.

In accordance with Act 5 of 2018 this model policy is adopted to provide guidance and direction to WCUUSD employees to prevent improper electronic communications between employees and students.

II. Definitions. For purposes of this policy, the following definitions apply:

A. **Electronic communication**. Electronic communication is any computer-mediated communication in which individuals exchange messages with others, either individually or in groups. Examples of electronic communication include, but are not limited to, email, text messages, instant messaging, voicemail, and image sharing and communications made by means of an internet site, including social media and social networking websites.

B. **Social media**. Social media is any form of online publication or presence that allows interactive communication, including, but not limited to, social networks, blogs, websites and internet forums. Examples of social media include, but are not limited to, Facebook, Twitter, Instagram, YouTube, and Google+.

C. **Employee**. Employee includes any person employed directly by or retained through a contract of employment the district, an agent of the school, a school board member, and including supervisory union employees.

D. **Student.** Student means any person who attends school in any of the grades Prekindergarten through 12 operated by the district.

III. Policy on Electronic Communication Between Students and Employees.

All communication between employees and students shall be professional and appropriate. The use of electronic communication that is inappropriate in content is prohibited.

A. Inappropriate content of an electronic communication. Inappropriate content of an electronic communication between an Employee and a Student includes, but is not limited to:

1. Communications of a sexual nature, sexual oriented humor or language, sexual advances, or content with a sexual overtone;
2. Communications involving the use, encouraging the use, or promoting or advocating the use of alcohol or tobacco, the illegal use of prescription drugs or controlled dangerous substances, illegal gambling, or other illegal activities;
3. Communications regarding the employees' or student's past or current romantic relationships;
4. Communications which include the use of profanities, obscene language, lewd comments, or pornography;
5. Communications that are harassing, intimidating, or demeaning;
6. Communications requesting or trying to establish a personal relationship with a student beyond the employees' professional responsibilities;
7. Communications related to personal or confidential information regarding employee or student that isn't academically focused; and
8. Communications between an employee and a student between the hours of 10 p.m. and 6 a.m. An Employee may, however, make public posts to a social network site, blog or similar application at any time.

B. Procedures. The superintendent shall develop procedures for both the receipt and handling of reports filed under this policy (see IV.A. and B. below).

IV. Enforcement Responsibilities

A. **Student communications violation of this policy.** In the event a student sends an electronic communication, that is inappropriate as defined in this policy or that violates the procedures governing inappropriate forms of electronic communication to an employee, the employee shall submit a written report of the inappropriate communication ("Report") to the principal or designee by the end of the next school day following actual receipt by the Employee of such communication. The principal or designee will take appropriate action to have the student discontinue such improper electronic communications.

While the school district will seek to use such improper electronic communications by a student as a teaching and learning opportunity, student communications violation of this policy may subject a student to discipline. Any discipline imposed shall take into account the relevant surrounding facts and circumstances.

B. **Employee communications violation of this policy.** In the event an employee sends an electronic communication that is inappropriate as defined in this policy or that violates the procedures governing inappropriate forms of electronic communication to a student, the student shall or the student's parent or guardian may submit a written report of the inappropriate communication ("Report") to the principal and/or the person designated by the principal to receive complaints under this policy promptly. The report shall specify what type

of inappropriate communication was sent by the employee with a copy of the communication, if possible.

Inappropriate electronic communications by an employee may result in appropriate disciplinary action.

C. **Applicability.** The provisions of this policy shall be applicable at all times while the employee is employed by the district and at all times the student is enrolled in the school district, including holiday and summer breaks. An employee is not subject to these provisions to the extent the employee has a family relationship with a student (i.e. parent/child, nieces, nephews, grandchildren, etc.).

D. **Other district policies.** Improper electronic communications that may also constitute violations of other policies of the district, i.e. unwelcome sexual conduct may also constitute a violation of the school's separate policy on the Prevention of Harassment, Hazing and Bullying of Students. Complaints regarding such behavior should be directed as set forth in the school's Procedures on the Prevention of Harassment, Hazing and Bullying of Students.

V. Reporting to Other Agencies

A. **Reports to Department of Children and Families [DCF]**. When behaviors violative of this policy include allegations of child abuse, any person responsible for reporting suspected child abuse under 33 V.S.A. §4911, et seq., must report the allegations to the Commissioner of DCF. If the victim is over the age of 18 and a report of abuse is warranted, the report shall be made to Adult Protective Services in accordance with 33 V.S.A. §6901 et seq.

B. **Reports to Vermont Agency of Education [AOE]**. Accordingly, if behaviors violative of this policy in a public school involve conduct by a licensed educator that might be grounds under Vermont law for licensing action, the principal shall report the alleged conduct to the superintendent and the superintendent shall report the alleged conduct to the AOE.

C. **Reporting Incidents to the Police**. Nothing in this policy shall preclude persons from reporting to law enforcement any incidents and/or conduct that may be a criminal act.

D. **Continuing Obligation to Investigate**. Reports made to either DCF or law enforcement shall not be considered to absolve the school administrators of their obligations under this or any other policy, such as the Policy on the Prevention of Harassment, Hazing and Bullying, to pursue and complete an investigation upon receipt of notice of conduct which may constitute a policy violation.

Legal Reference(s):	2018 Acts and Resolves No. 5 (located at https://legislature.vermont.gov/Documents/2018.1/Docs/ACTS/ACT005/ACT005%20As%20Enacted.pdf)
	16 V.S.A. § 1698
	16 V.S.A. § 570