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
3.23.21 4:30-6:30 pm
https://tinyurl.com/y93agvsj

Meeting ID: 870 2915 5233
Passcode: 377858
Dial by your location: 1-929-205-6099

Via Video Conference*

1. Call to Order

2. Approve Minutes of 2.15.21 and 3.10.21 – pg. 2

3. Review Existing Policies
   3.1. C2 Student Alcohol and Drugs – pg. 7
   3.2. C5 Weapons and Firearms – pg. 10
   3.3. Hearing Officer

4. Review Technology Policies
   4.1. F40 Change Management – pg.13
   4.2. F43 Backups – pg. 17
   4.3. D3 District Take Home Device and Personal Device Policy - pg. 19
   4.4. F44 Password Management Policy – pg. 22
   4.5. F45 Acceptable Use – pg. 25
   4.6. F47 Electronic Mail – pg. 28
   4.7. F48 Incident Response Policy and Plan – pg. 30
   4.8. B8 Electronic Communication Between Employees and Students – pg. 31

5. Future Agenda Items
   5.1. School Choice Policy

6. 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
2.15.21 4:30-6:00 pm

Present: Superintendent Bryan Olkowski, Jody Emerson, Michelle Ksepka, Jim Garrity, Jaiel Pulskamp, Chris McVeigh, Dorothy Naylor, Amy Molina, Kelly Bushey, Kevin Richards

1. **Call to Order:** Chris McVeigh called the meeting to order at 4:39 p.m.

2. **Approve Minutes of 1.26.21:** Dorothy Naylor moved to approve the minutes from January 26, 2021. Seconded by Chris McVeigh, this motion carried unanimously.

3. **Review Policies**
   - **3.1. C2 Student Alcohol and Drugs:** Superintendent Olkowski shared that he believes the implementation of this policy could create some confusion with administrators; he noted that both C2 and C5 appear to be "zero tolerance" policies and he believes that this could create legal challenges. He spoke about some students under special education regulations who are entitled to manifestation determination hearings. He asked whether the committee and the board would like to consider some amendments to these policies, given those issues. Chris McVeigh asked whether there has been difficulty administering this policy to date. Superintendent Olkowski indicated that, to date, there has not. Discussion followed around the procedures for this policy, which exist in the student handbook. Chris McVeigh suggested that the procedures be spelled out in the body of the policy. Superintendent Olkowski suggested having some type of "notice" that students have read and understand the policy. Jody Emerson reviewed that a variety of strategies have been in place over the years to review the handbook with students. The procedures for this policy are consistent, district-wide. Chris McVeigh suggested to add more specific language to the body of the policy, referring to possible penalties, versus including the entire procedure into the policy. The committee will reconsider this policy, as amended (as discussed) at the next meeting.)
   - **3.2. C5 Weapons and Firearms:** Superintendent Olkowski noted that this model policy in VSBA was updated in December 2020. He reviewed the current policy, especially Part A: With Regards to Students. He noted the issue of manifestation

determination (especially related to item #c in this section.) Discussion followed around the issue of manifestation determination for students with disabilities, and how this might apply to this policy as written. Specifically, the issue of whether the board can or should make disciplinary decisions when manifestation determination is in play. Kelly Bushey spoke about her experience at manifestation hearings. Chris McVeigh suggested that the policy be changed to indicate that a manifestation hearing happen before board action, and he discussed with those present how to change the verbiage to reflect how it applies to students with disabilities or students who are suspected of having disabilities.
Chris McVeigh suggested adding language to the policy to include "Student who has been referred for special education evaluation, is currently eligible for special education or has a 504 plan, or a student who the principal suspects might have a disability…"
Some discussion followed about whether it is necessary to include procedure in this policy, for example, after Part A paragraph that begins with "However, with the prior…" The committee agreed, after the sentence that begins with "However, with the prior written consent….." to add:
"For a student who has been referred for a special education evaluation, is currently eligible for special education or has a 504 plan, or a student who the principal suspects might have a disability, then a manifestation determination hearing (reference from special education regulations) must occur before any board hearing." Jody Emerson suggested also changing the language to: "The student is disabled, or may be disabled, and the misconduct is related to the disability, as determined during the manifestation meeting held prior to the hearing." under #C in the policy (Part A).
Chris McVeigh suggested amending the language in the policy and then taking it to the board to see what is their will. Jaiel Pulskamp indicated that she is in favor of whatever is less punitive, and she would like to dictate as little as possible what teachers and administrators *have* to do. Jody Emerson noted that in her tenure at U32, there have been no expulsions due to weapons violations.
Dorothy Naylor indicated that she feels having a manifestation hearing before board involvement seems like the most direct and sensible practice.
Chris McVeigh will edit the language in the policy as discussed; he also believes it should be highlighted when the board is considering, the difference between "dangerous weapon" and "firearm" as well as the different language of "may" or "shall."
Superintendent Olkowksi asked whether the board would like to consider hiring a hearing officer for board hearings. Chris McVeigh suggested bringing this to the full board as well.

3.3. F46 Flag Raising Policy: Superintendent Olkowski reviewed the policy which was adopted approximately a year ago. He asked how to ensure that the policy is likely to withstand a challenge. He asked whether there is an application procedure in place. He had provided a draft "WCUUSD Flag Request" form for discussion. Superintendent Olkowski indicated that the "Exclusionary Criteria" in the procedures may be unclear or leave room for inconsistencies. Some discussion followed around the registration process, for example, "registered as hate speech by a nationally recognized organization." Jaiel Pulskamp indicated that her understanding is that the board does have some discretion. Discussion followed around how student groups are formed at WCUUSD. Include language: "student groups, i.e., class, club, etc." Chris McVeigh suggested that Superintendent Olkowski share a memo sharing what counsel Bernie Lambek had provided, and then addressing this at the next Policy Committee meeting after considering the guidance. Chris McVeigh suggested inviting Bernie Lambeck to the next Policy Committee meeting for his input around the Flag Raising Policy.

4. **Review of Technology Policies**: (these policies were not addressed in light of the late hour.)
   4.1. F40 Change Management
   4.2. F43 Backups
   4.3. D3 District Take Home Device & Personal Device Policy
   4.4. F44 Password Management Policy
   4.5. F45 Acceptable Use
   4.6. F47 Electronic Mail
   4.7. F48 Incident Response Policy & Plan
   4.8. B8 Electronic Communication Between Employees and Students

5. **Future Agenda Items:** Next Policy Committee Meeting: Wednesday, March 10, 4:30 - 6:30.

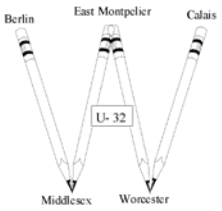
6. **Adjourn**: The committee adjourned at 6:36 p.m.

Respectfully submitted,

Lisa Stoudt, Committee Recording Secretary

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

Bryan Olkowski
Superintendent



WCUUSD Policy Committee
Meeting Minutes Unapproved
3.10.21 4:30-6:00 pm

Present: Superintendent Bryan Olkowski, Michelle Ksepka, Jim Garrity, Chris McVeigh, Kelly Bushey, Bernie Lambeck, Esq. (Legal Counsel), Christina Pollard, Jody Emerson, Aaron Boynton

1. **Call to Order: Chris McVeigh called the meeting to order at 4:33 p.m.**
2. **Elect Chair of the Committee: Chris McVeigh nominated himself as Chair. Christina Pollard seconded. This motion carried unanimously.**
3. **Approve Minutes of 2.15.21: Tabled**.
4. **Review Existing Policies:**
   - **4.1. F46 Flag Policy Updated**: Bernie Lambek had provided a confidential memo for consideration regarding this policy. He had provided an edited version of the policy, and had tracked suggested changes. He invited questions or comments. Mr. Lambek had explained that the flag is considered more a forum for "board" speech versus "student" speech. He explained that even though the request is initiated by students, it is considered endorsed by the board/ school (government entity).
     Jody Emerson explained that the U32 Board had first addressed this policy and had wanted the ability to decide how long a flag was to be flown. Some discussion followed around having a timeline included in the policy. Committee members agreed that having a time frame is needed. Mr. Lambek suggested that some language could be added to the time frame, e.g. "unless the board decides otherwise in this case."
     Mr. Lambek had provided a draft of very specific procedures.
     Jody Emerson suggested replacing "Vermont transferrable skills" with "Student Learning Outcomes" in the procedures, for consistency.
     Some discussion followed around the idea that a student group would require having a faculty advisor. Could read "faculty advisor or club advisor, if any" on the request form. If students do not have an advisor, and they have questions, they can be referred to the principal. Discussion followed around "hate symbols."
     For procedures #3, 4, 5, the group decided that "Administration" will be replaced with "Principal." Aaron Boynton brought up the topic of building principals having to decide whether a request aligns with the criteria as stated in the policy, where there is some level of judgement required. On Item #6 in procedures, clarify "appeal to…." would like to make this clearer –*appeal to the Superintendent.* It will ultimately go to the board.

Chris McVeigh invited questions/ comments. He recommends bringing this edited version to the board for a first reading.

Chris McVeigh moved to make a recommendation to the WCUUSD Board to adopt the Policy F46 as edited. Seconded by Christina Pollard, this motion carried.

Superintendent Olkowski would like to have the procedures as discussed tonight, be presented to the board for its consideration as well.

Bernie Lambek will update the documents and include some "red lined" edited versions as well as clean copies for the board to consider.

4.2. C2 Student Alcohol and Drugs Updated: Superintendent Olkowski had sought legal counsel from Scott Cameron and added some language to this policy, especially around manifestation determination and disciplinary action. Chris McVeigh suggested that the language around students on IEP or Section 504 be expanded to include "or may have a disability," similar to what had been discussed previously for Policy C5.

Jody Emerson asked, do we want the procedures to be included in the policy, as some of the edits tonight reflect moving procedures into the body of the policy?

Chris McVeigh indicated that, especially with the topic of manifestation, it is helpful to include the verbiage into the body of the policy. Superintendent Olkowski expressed his support to have the language around "manifestation" in the policy. Discussion followed around manifestation determination hearings.

Some discussion about whether the word "substantially" be struck from the language, as this is not language from special education law. Discussion followed around the language "prior to taking disciplinary action for violation…" Kelly Bushey and Jody Emerson indicated that this will tie the hands of the administration while a manifestation determination hearing is put together. Much discussion centered around manifestation hearing "trumping" discipline - is it critical that manifestation hearing happens before discipline is imposed? Is it feasible?

This discussion will be continued at the next meeting, as the committee ran out of time.

4.3. C5 Weapons and Firearms Updated: Not discussed

5. **Review Technology Policies:**
   - **5.1.** F40 Change Management
   - **5.2.** F43 Backups
   - **5.3.** D3 District Take Home Device and Personal Device Policy
   - **5.4.** F44 Password Management Policy
   - **5.5.** F45 Acceptable Use
   - **5.6.** F47 Electronic Mail
   - **5.7.** F48 Incident Response Policy and Plan
   - **5.8.** B8 Electronic Communication Between Employees and Students

6. **Future Agenda Items:**
   - **6.1.** School Choice Policy

Is this committee moving meetings to Wednesday evenings? (First Wed. of the month)
The group agreed to stay with the Tuesday meetings. Next meeting March 24, 4:30 - 6:30.

7. **Adjourn:** The meeting adjourned by consensus at 6:39 p.m.

Respectfully submitted, Lisa Stoudt, Committee Recording Secretary

Required

WASHINGTON CENTRAL UNIFIED UNION SCHOOL DISTRICT

Board of Directors' Policy

POLICY:	**C2**
WARNED:	~~**5.15.20**~~
ADOPTED:	~~**6.3.20**~~
EFFECTIVE:	~~**6.13.2020**~~

STUDENT ALCOHOL & DRUGS

It is the policy of the Washington Central Unified Union School District that no student shall knowingly possess, use, sell, give or otherwise transmit, or be under the influence of any illegal drug, regulated substance, or alcohol on any school property, **or on any school sponsored transportation** or at any school sponsored activity away from or within the school.[1] It is further the policy of the district to make appropriate referrals in cases of substance abuse.

Definitions

Substance Abuse is the ingestion of drugs and or alcohol in such a way that it interferes with a person's ability to perform physically, intellectually, emotionally, or socially.[2]

Drug means any narcotic drug, hallucinogenic drug, amphetamine, barbiturate, marijuana or any other controlled substance as defined by state or federal regulation or statute.[3]

Since education is an essential element to discourage inappropriate alcohol and drug use, the superintendent shall report to the board during its regularly scheduled June meeting, what efforts in the district fulfill this developmentally appropriate educational goal, at each of the district's schools.

Educational Program. The (superintendent, principal, other) shall work with appropriate staff members to develop and conduct an alcohol and drug abuse educational program.[4] The program shall be consistent with the Vermont Alcohol and Drug Education Curriculum Plan[5]. If the school district is a recipient of federal Safe and Drug-Free Schools and Communities Act funds, the Act will be considered in the development of the alcohol and drug abuse educational program.[6]

Support and Referral System. In each school the principal or ~~his or her~~their designee shall develop a support and referral system for screening students who refer themselves and students who are referred by staff for suspected drug and/or alcohol use and/or abuse problems.[7] The support and referral system will include processes to determine the need for further screening, education, counseling or referral for treatment in each referred case.[8] In addition, the principal shall establish procedures for administering emergency first aid related to alcohol and drug abuse.[9]

Students on IEP or Section 504 Plan or in pre-referral for IEP or Section 504 Plan : Prior to taking disciplinary action for violation of this policy against a student who is on an IEP or 504 Plan the superintendent or principal shall refer the student for a manifestation hearing to determine whether the conduct at issue is related to the student's disability. If it is determined that the conduct at issue is caused by or substantially related to the student's disability the superintendent or principal may elect not to impose disciplinary action but shall take appropriate measures to address the behaviors which protect the interests of the student and the school community and which comport with requirements of federal and state law.

Disciplinary Action: The superintendent or principal may take reasonable disciplinary and/or corrective action against students who violate this policy, up to and including a suspension not to exceed then (10) school days. Disciplinary and/or corrective action may include, but shall not be limited to in-school or out-of-school suspension, loss of privileges including ability to participate in extra-curricular activities, and referral to appropriate resources for screening, education, counseling or treatment, as appropriate.[1] If the superintendent believes that expulsion or a suspension in excess of ten (1) school days is warranted the matter shall be referred to the school board for hearing and a final determination. In its discretion the school board may designate a qualified hearing officer or a sub-committee of the board to conduct the hearing; in that case the hearing officer or sub-committee shall make written findings and recommendations to the school board, which shall make the final decision regarding suspension or expulsion. If after hearing, a student is found to have violated this policy the superintendent or principal may with the approval of the school board, expel the student for up to the remainder of the school year or up to 90 school days, whichever is longer. 16 V.S.A. §1162(a).

Cooperative Agreements.[10] The (superintendent, principal, other) shall annually designate an individual to be responsible for providing information to students and parents or guardians about outside agencies that provide substance abuse prevention services and to encourage the use of their services and programs when appropriate.

The Washington Central Unified Union School District has a Substance Abuse Prevention (SAP) Counselor. They will provide substance abuse treatment to students who are referred through the school's support and referral system, or who refer themselves for treatment.

Staff Training. The (superintendent, principal, other) will work with appropriate staff to provide training for teachers and health and guidance personnel who teach or provide other services in the school's alcohol and drug abuse prevention education program. The training provided will meet the requirements of State Board Rules related to staff training.[11]

Community Involvement. The (superintendent, principal, other) will work with school staff and community members to implement a program to inform the community about substance abuse issues in accord with State Board of Education rules.[12]

Annual Report. In a standard format provided by the Agency of Education, the (superintendent, principal, other) will submit an annual report to the Secretary of Education describing substance abuse education programs and their effectiveness.[13]

Notification. The (superintendent, principal, other) shall ensure that parents and students are given copies of the standards of conduct and disciplinary sanctions contained in the procedures related to this policy, and are notified that compliance with the standards of conduct is mandatory. Notice to students will, at a minimum, be provided through inclusion of these standards and sanctions in the student handbook distributed to all students at the beginning of each school year or when a student enrolls in the school.[14]

[1] 16 V.S.A. § 1165(a). See also 18 V.S.A. § 4237 making it unlawful for any person to sell or dispense any regulated drug to minors or to any other person on school property or property adjacent to a school.
[2] Vermont State Board of Education Manual of Rules and Practices, Rule 4211

[1] The cost associated with screening, education, counseling or treatment shall be the responsibility of the student unless otherwise approved by the school board or required by law.

[3] *See definitions of narcotic drugs and hallucinogenic drugs in* 18 V.S.A. §4201; *and controlled substance in* 41 U.S.C. §706(3) *and* 21 U.S.C. §812.
[4] 16 V.S.A. §131(9); SBE Rule 4213.1
[5] SBE Rule 4212.2 *requiring that education program be consistent with this Plan.*
[6] 20 U.S.C. §§7101 et seq.
[7] SBE Rule 4212.3
[8] SBE Rule 4212.3D.
[9] SBE Rule 4212.3B. SBE Rule 4212.3B requires that each "…school district policy…establish procedures for administering first aid related to alcohol and drug abuse. The procedures will define the roles of the personnel involved."
[10] SBE Rule 4212.3.
[11]SBE Rule 4213.2. See also SBE Rule 4212.3C.
[12] SBE Rule 4214 does not require that this paragraph be included in a school board policy. The rule does require that schools engage in community programs "…to inform the community about the school's alcohol and drug prevention education program, alcohol and drug abuse prevention issues, and community-wide responsibility for effective alcohol and drug abuse prevention.". This paragraph could be included in administrative procedures developed in conjunction with this policy.
[13] SBE Rule 4215 does not require that this paragraph be included in a school board policy. The rule does require that the school's annual report include information on substance abuse education programs. This paragraph could be included in administrative procedures developed in conjunction with this policy.
[14] This section is not required by law, but could be included in a school board policy to ensure that adequate notice of the school district's policy and procedures related to alcohol and drug abuse is given to students and parents.

Legal Reference(s): *20 U.S.C. §§7101 et seq. (Safe & Drug-Free Schools & Communities Act of 1994)*
16 V.S.A. §909 (Drug & Alcohol Abuse Prevention Education Curriculum)
16 V.S.A. 131(9) (Comprehensive Health Education)
16 V.S.A. §1045(b)(Driver Training Course)
16 V.S.A. §1165 (Alcohol and drug abuse)
18 V.S.A. §4226 (Drugs: minors, treatment, consent)
Vt. State Board of Education Manual of Rules and Practices §§4200 -4215)

Required

WASHINGTON CENTRAL UNIFIED UNION SCHOOL DISTRICT

Board of Directors' Policy

POLICY:	**C5**
WARNED:	~~**5.15.20**~~
ADOPTED:	~~**6.3.20**~~
EFFECTIVE:	~~**6.13.2020**~~

WEAPONS / FIREARMS

It is the intent of the board to comply with the federal Gun Free Schools Act of 1994, and the Vermont state laws (16 V.S.A. §1166 & §1162) requiring school districts to provide for the possible expulsion of students who bring or possess dangerous weapons or firearms at school. It is further the intent of the board to maintain a student discipline system consistent with the requirements of the federal Individuals with Disabilities Education Act, Section 504 of the Rehabilitation Act and the Vermont State Board of Education rules.

Definitions:

This policy shall define the terms *"dangerous weapons*", *"firearm"*, *"at school"* and *"expelled"*. However, the school board may augment the definitions, provided they remain consistent with definitions required by state and federal law.

a. The term "*dangerous weapon"* means a **firearm, knife or other** weapon, device, instrument, material, or substance, animate or inanimate, that is used for, designed for, or is readily capable of, causing death or serious bodily injury. This includes weapons that a student acquires at school or on the bus.

b. *"Firearm"* means **A)** any weapon **or device**, whether loaded or unloaded, which will expel a projectile by the action of an explosive and includes **but is not necessarily limited to** any weapon commonly referred to as a pistol, revolver, rifle, gun, machine gun or shotgun; **(B) the frame or receiver of any such weapon; (C) any firearm muffler or firearm silencer; or (D) any destructive device.**

c. **The term "destructive device" means—**
(A) any explosive, incendiary, or poison gas—
(i) bomb,
(ii) grenade,
(iii) rocket having a propellant charge of more than four ounces,
(iv) missile having an explosive or incendiary charge of more than one-quarter ounce,
(v) mine, or
(vi) device similar to any of the devices described in the preceding clauses;

d. *"At school"* means any setting that is under the control and supervision of the school district. It includes school grounds, facilities and vehicles used to transport students to and from school or school activities.

e. *"Expelled"* means the termination of educational services to a student for greater than 10 days, and is determined by the board.

Policy Statement

PART A: WITH REGARDS TO STUDENTS

Except as otherwise provided herein, any student who brings to school or possesses a dangerous weapon while at school shall be brought by the superintendent to the school board for consideration of ~~an expulsion hearing~~ **suspension or expulsion. In its discretion the school board may designate a qualified hearing officer or a sub-committee of the board to conduct the hearing; in that case the hearing officer or sub-committee shall make written findings and recommendations to the school board, which shall make the final decisions regarding suspension or expulsion.**

~~However,~~ **Exception:** with the prior written consent of the superintendent or their designee, a student may possess a device that might be considered a dangerous weapon for a predetermined educational purpose.

If after a hearing, a student is found ~~by the board~~ to have brought or possessed a dangerous weapon **other than a firearm** while at school, the superintendent or principal may suspend the student for up to 10 school days or, **with the approval of** the **school** board**,** may expel the student for up to the remainder of the school year or up to 90 school days, whichever is longer. 16 V.S.A. §1162(a).

~~Or,~~ **I**f after a hearing, a student is found ~~by the board~~ to have brought or possessed a firearm while at school, the **superintendent or principal shall expel the** student **from the school** ~~shall be expelled~~ for no**t** less than one calendar year. 16 V.S.A. §1166 (2). However, the school board may modify the expulsion on a case-by-case basis when it finds circumstances such as, but not limited to:

a. The student was unaware that they had brought a ~~weapon~~ **firearm** to school.
b. The student did not intend to use the ~~weapon~~ **firearm** or threaten or endanger others.
c. The student is disabled and the misconduct is related to **or impacted by** the disability.
d. The student does not present an ongoing threat to others and a lengthy expulsion would not serve the best interests of the student nor substantially further the goal of ensuring a safe and fear free environment.

At the discretion of the school board and administration, an expelled student may be afforded limited educational services at a site other than the school during the period of expulsion under this policy.

Policy Implementation

An expulsion hearing conducted under this policy shall afford due process as required by law, and as developed by the superintendent or their designee.

Nothing in this policy shall prevent a superintendent or principal, subject to subsequent due process procedures, from removing immediately from a school a student who brings a dangerous weapon to school in violation of this policy and who poses or may pose an immediate or continuing danger to persons or property, or an ongoing threat of disrupting the academic process of the school.

Students on IEP or Section 504 Plan: Prior to referring a student who is on an IEP or 504 Plan to the board for a hearing on suspension or expulsion the superintendent or principal shall refer the

student for a manifestation hearing to determine whether the conduct at issue is related to the student's disability. If it is determined that the conduct at issue is caused by or substantially related to the student's disability the superintendent or principal may elect not to refer the student to the board for suspension or expulsion, but shall take appropriate measures to address the behaviors which protect the interests of the school community and which comport with requirements of federal and state law.

The superintendent may refer to the appropriate law enforcement agency any student who possesses or brings a dangerous weapon to a school under the control and supervision of the school district. The superintendent shall refer to the appropriate law enforcement agency any student who possesses or brings a firearm to a school under the control and supervision of the school district. In addition, the superintendent may report any incident subject to this policy to the Department of Children & Families.

As required by state law, the superintendent shall annually provide the Secretary of Education with descriptions of the circumstances surrounding expulsions imposed under this policy, the number of students expelled, and the type of dangerous weapons involved.

PART B: WITH REGARD TO PERSONS OTHER THAN STUDENTS

No person shall enter onto school grounds while in possession of a dangerous weapon or firearm as described above unless:

a. The person has prior written approval from the superintendent or their designee to bring the weapon to school for authorized activities;
b. The person is a law enforcement officer.

Legal Reference(s): *16 V.S.A. §1162 (Suspension or expulsion of pupils)*
16 V.S.A. §1166 (State law pursuant to Federal law)
13 V.S.A. §§4004, 4016 (Criminal offenses)
20 U.S.C. §7151 (Gun Free Schools Act)
18 U.S.C. §921 (Gun Free Schools Act of 1990)
20 U.S.C. §§ 1400 et seq. (IDEA)
29 U.S.C. §794 (Section 504, Rehabilitation Act of 1973)
Vt. State Board of Education Manual of Rules & Practices, §§4311, 4312

Recommend

WASHINGTON CENTRAL UNIFIED UNION SCHOOL DISTRICT

Board of Directors' Policy

CHANGE MANAGEMENT

POLICY: F40

WARNED: _____

ADOPTED: _____

EFFECTIVE: _____

Overview

The objective of change management in this context is to ensure that standardized methods and procedures are used for efficient and prompt handling of all changes to control IT infrastructure, in order to minimize the number and impact of any related incidents upon service.

Purpose

To control all changes to equipment, software or procedures will be established and followed for change, integrating operational and application change control procedures, and logging all changes.

Change Advisory Board (CAB)

A CAB is a group of people who run formal CAB meetings to assess, prioritize, authorize, and schedule changes as part of the change control process.

There are two components of a best practice CAB: 1) The right people and 2) An effective CAB meeting structure.

The CAB should include at least one representative from all groups affected by the changes on the agenda (including non-IT groups if applicable) and can include managers or non-managers, such as a network engineer or teacher or administrator. It is likely to include groups from functional and technical disciplines such as the IT Helpdesk, application support, server support, etc.

The CAB owner acts as a chairperson and should be a CAB member. This person is typically a change manager or on the change management team.

The responsibilities of the CAB members include the following:

- Review changes prior to the meeting.
- Assess and recommend the approval or rejection of proposed changes in a timely manner. If a CAB member doesn't approve a change, make sure they explain why.
- Attend scheduled CAB meeting(s) or send a qualified representative.
- Act as a liaison between the CAB and its team regarding change management policies, procedures, questions, or enhancements.

The responsibilities of the CAB owner include the following:

- Develop the vision and strategy for CAB meetings.
- Lead CAB meetings and make sure the required representatives attend (representatives from all groups affected by changes).
- Define and communicate the CAB members' roles and responsibilities.
- Document and communicate the CAB meeting agenda before CAB meetings and decisions after the meeting.

Regular CAB meetings should take place at least monthly; however, a weekly or biweekly schedule is recommended.

All teams affected by a change should be represented in the CAB meeting.

The CAB Meeting Agenda should include the following:

- All high-risk changes and changes marked as required by the CAB
- A review of all failed and backed out changes
- Change management process updates
- Reviews for each change that include:
    - A risk/impact assessment (on the district)
    - The effects on the infrastructure and customer service as defined in the Service Level Agreement (SLA) as well as on capacity and performance, reliability and resilience, contingency plans, and security
    - The impact on other services that run on the same infrastructure (or on software that is in the cloud)
    - A resource assessment, including the IT, district, and other resources required to implement and validate the change
    - The effect, risk, and/or impact of not implementing the change
    - Other changes being implemented on the schedule of change
    - Technical capability and technical approval required

A change that goes into production can impact many teams, including central office, parents, administrators, students, IT, and other groups. If you don't consider all technical impacts of a change, there is a higher risk of a system outage or malfunction. This makes an effective CAB essential because it provides awareness of the changes for impacted teams and makes sure all technical aspects of a change are considered.

Types of Significant Change

There are three types of significant change that should be considered:

Standard Change – Standard Change is a consistent or routine change that takes place on a regular interval (weekly, monthly, quarterly, yearly) that should be formally reviewed and approved before being implemented. These changes have fairly common steps and guidelines and are generally low risk to the environment and seldomly require modification.

Once approved, this change does not need to go back to a change advisory board (CAB) or administration team for regular approval.

However, the schedule for change must be published and communicated on a regular basis. Additionally, if a standard change causes an issue or outage, it must be brought back to the CAB for review and discussion.

Examples of Standard Change:

- Lifecycle replacement of hardware
- Routine Software Patching and Updates
- Firewall Changes not requiring a service outage
- DNS entries

Normal Change – Normal Change is a change that may be common, but may also be unique in its construct. A normal change should be reviewed (and approved/scheduled or denied) by the CAB or administration as it may contain risk to the environment such as system downtime, data loss, security risk, enumeration or dissemination of PII, PHI, or other types of information.

Examples of Normal Change:

- Storage or Virtualization Platform replacement
- Application upgrade that impacts functionality or the data model of a system
- Telephone system enhancement or upgrade work that may cause an outage

Emergency Change – Emergency Change is a Normal Change that must be introduced and implemented as soon as possible, even before the CAB or administration team needs to approve or deny the change. The CAB owner will quickly determine if emergency change is warranted for a particular circumstance. These changes typically represent a crisis or opportunity that must be addressed without undue risk to the district. While the change may need to be implemented before a CAB meeting, the change MUST still go through the CAB or administration team AFTER implementation so they can review the efficacy of the change and the emergency nature of it and provide their approval or dissent to the change. YOU MAY NOT SKIP THIS PART OF THE PROCESS.

Examples of Emergency Change:

- Implementing a security patch to a zero-day exploit
- Isolating the network from a large-scale Distributed Denial of Service (DDOS) Attack

Change Management Requirements

There shall be a formal approval for proposed changes that could potentially impact the operational environment. Prior to any operational change there shall be a risk assessment that:

- Identifies significant changes.
- Records significant changes.
- Assesses the potential impact of such changes.
- Procedures and responsibilities for aborting and recovering from unsuccessful changes

- All changes shall be reviewed in advance and requires the written approval of the or designee.
- All changes shall be communicated to all relevant individuals.

Change Policies Computers/Workstations

There shall be a formal approval for proposed Local Administrator Access: WCUUSD service users will not have the right to change the local administrator passwords on WCUUSD provided desktop computers. Service Users may request access to the local administrators group from the Information Technology Department, however, this will void the computer and the service user from being supported by the Information Technology Department. Systems that have been modified and require the assistance of the Information Technology Department will be re-loaded with the original software configuration that the Information Technology Department supplies to service users when issued a new system.

Network Configuration Changes: The standard configuration on WCUUSD laptops is configured so that in most cases the computer can be transferred from network to network without any configuration changes.

Changes to Hardware: Computer equipment supplied by WCUUSD must not be altered or added to in any way (e.g., upgraded processor, expanded memory, or extra circuit boards) without prior knowledge and authorization from the Information Technology Department.

Changes NOT Related: Any changes that are not related to the changes listed above must adhere to and comply with the District Change Management Policy.

Recommended

WASHINGTON CENTRAL UNIFIED UNION SCHOOL DISTRICT

Board of Directors' Policy

BACKUPS

POLICY: F43

WARNED: _____

ADOPTED: _____

EFFECTIVE: _____

Individual User Responsibility: WCUUSD service users must ensure that information that represents any part of a business plan, system design, or that relates to the management of customer accounts are adequately protected from loss. Company file servers are frequently archived; this is the suggested method for ensuring that information loss is prevented. If a user is unable to ensure adequate loss protection, they should contact the WCUUSD Information Technology Helpdesk (ithelp@u32.org) for assistance in resolution of this problem.

Not Responsible for Backups of Personal Data: WCUUSD information systems are for official company use. WCUUSD will not backup user's personal data files or programs that are not WCUUSD property or have no relevance to WCUUSD business. Examples include but are not limited to encoded music files, digital images and games. The Information Technology Department may remove such items from WCUUSD systems at their discretion without prior warning to individuals.

General Storage Rules

- Maintain records in an appropriate storage form (i.e. paper, magnetic tape, microfilm, flash drive, optical disk) for the recommended length of time indicated by this policy.
- All records being prepared for storage should be described and include the following information on a label in order to facilitate their reference, review, and destruction:
    - The inclusive dates
    - Originating department name
    - Type of media
    - Date of destruction
    - Contact name and telephone number.
- Ensure the appropriate forms of records are complete and copies of such records can be reproduced in a complete and readable form upon request.
- Store all records in a manner that permits the efficient retrieval of stored records and the efficient return of records borrowed from storage.
- Restrict access to stored records to those individuals who have an appropriate need and permission to retrieve the records.
- Ensure all records are stored in a climate-controlled location with protection from hazards (i.e., theft, water, fire).

- Confirm that records copied onto an alternative storage medium (microfiche, diskette, tape) are complete and readable before the original paper record is destroyed. All records stored in an alternate format must be available for reading and/or duplicating within a reasonable timeframe. Once records have been transferred, the original version can be destroyed according to this policy.
- Protect computerized data with password, code or card system.
- The Uniform Preservation of Business Records Act requires retention of general business records for three years from the creation of such records if no retention period is specified by regulation.
- Credit card transaction data should be stored only as long as required for financial tracking and auditing purposes. The specific credit card holder information such as the account number, expiration date, or other magnetic stripe information should never be stored in electronic format unless specific approval is received from the IT Department and the WCUUSD Policy Committee.

Required

WASHINGTON CENTRAL UNIFIED UNION SCHOOL DISTRICT

Board of Directors' Policy

DISTRICT TAKE HOME DEVICE & PERSONAL DEVICE POLICY

POLICY: **D3 Possibly**

WARNED: _____

ADOPTED: _____

EFFECTIVE: _____

Overview

The mission of the District Take Home Device & Personal Device Policy in WCUUSD is to create a collaborative learning environment for all learners. This environment will support students and teachers in the use of technology to enhance student learning and engagement in the classroom. It will create equity and level the playing field for all learners by providing every student with a device to use both in school and at home.

In 2019 the District expanded the use of Chromebooks and the ability for students to take home the devices to support their schoolwork. Students at all WCUUSD schools will have the opportunity to check out a district-owned Chromebook (Grades 3-12) or Tablets (Grades PreK-2) for the school year. This device will allow filtered access via the district network to educational resources and materials needed for students to be successful. It will also allow all student access to G Suite for Education, online textbooks, educational web-based tools, and many other useful websites.

Education and Access

G Suite for Education is a closed system whereby only students and staff have access. It includes applications that enable students to:

- Create projects
- Collaborate with their classmates
- Send emails to students and teachers
- Submit assignments

As a G Suite for Education District, we are able to monitor student Chromebook activity through web-based management tools.

Before each Chromebook device connects to the Internet, it must pass through district network firewalls and filters. This happens whether the device is browsing at school or home using another WiFi router that is providing the Internet connection. We are currently using Content Keeper for Chromebook and other background tools.

Daily Care and Maintenance

Students are responsible for the general care of the Chromebook they have been issued by the school. Chromebooks that are broken, or fail to work properly, must be submitted to IT or designated staff. Do not take District owned Chromebooks to an outside computer service for any type of repairs or maintenance. Do not attempt to repair the device yourself. We understand accidents happen. Report them immediately so that the district can fix the device.

- Students are responsible for bringing fully charged Chromebooks for use each school day.

- Chromebooks must have a District asset tag on them at all times and this tag must not be removed or altered in any way. If removed there may be disciplinary action.
- No food or drink is allowed next to your Chromebook while it is in use.
- Cords, cables, and removable storage devices must be inserted carefully into the Chromebook. Plug-in connectors are **fragile** and must be handled with care.
- Never transport your Chromebook with the power cord plugged in. Never store your Chromebook in your carry case or backpack while plugged in.
- Clean the screen with a soft, dry microfiber cloth or anti-static cloth. No liquids.
- Student should never leave a Chromebook unattended, such as in a vehicle or any unsupervised area.
- Transport Chromebooks with care, Chromebook lids should always be closed and tightly secured when moving.
- Never move a Chromebook by lifting from the screen. Always support a Chromebook from its base with the lid closed and open or close it using two hands.

Chromebook screens can be easily damaged! The screens are particularly sensitive to damage from excessive pressure on the screen.

- Do not store the Chromebook with the screen in the open position or tablet mode.
- Do not place anything on the Chromebook that could put pressure on the top or screen.
- Do not poke the screen with anything that will mark or scratch the screen surface.
- Do not place anything on the keyboard before closing the lid (e.g., pens or pencils)
- Do not place the device near magnets or anything with high electric current.
- Do not place anything in the sleeve or backpack that will press against the cover.

Digital Citizenship and Internet Safety

WCCUSD asks that all computing equipment is used for educational purposes or to support those employees who provide educational services. We expect device holders to use electronic resources safely and responsibly. We ask that students engage a trusted adult if you are unsure about something related to the use of your computer or electronic resources. We expect that you will not share your account information or the account information of others. Never post or share pictures of yourself or others unless you have school permission. Please tell a trusted adult if you come across something that is dangerous or disturbing. All school rules for how you behave and how you treat others apply for in-person and for electronic communications.

Security, Filtering, and Monitoring

The school district is required by law to provide certain levels of filtering and monitoring of the use of all district owned technology and electronic resources. All students are expected to support these efforts to provide a safe and legal electronic learning environment. It is expected that parents/guardians will monitor the student's use of the Internet at home so that the district-owned device is not used to access illegal or inappropriate websites or download any material from those sites. Please be aware of these cautions.

- Do not use district equipment or electronic resources for commercial or personal gain.
- Do not use district resources for political purposes, like trying to influence elections.
- Do not use district resources for anything illegal or indecent such as bullying, posting inappropriate images or text, or passing along information that is harmful or inappropriate.
- Do not participate in any activity to alter, bypass or attempt to bypass the school district network, security settings, filters, safety settings, or user roles.
- Do not install or download personal software or applications (apps), games, or operating systems.

Lost or Damaged Equipment

Students and parents will be responsible for district-owned technology that is issued to them, just as they are for other district-owned items such as textbooks, athletic equipment, or library books. The district will repair or replace the device, but students and parents may be responsible for the cost of those repairs or replaced devices. Please remind your student to report a missing Chromebook to the library staff or classroom teacher (in-person or via email) as **soon** as it's misplaced. We can help them locate. After 24 hours we will disable the device.

The WCUUSD Transportation Staff have been asked to return any found devices to the U-32 Technology Office.

Submit Chromebooks that need repair, with the sleeve and power cord to the Building Technology Specialist, teacher-librarian, or classroom teacher depending on your school. If we are able to fix the device, we will do so and return it. If we are unable to fix the problem, we will issue a new device. Physical damage or lost equipment may cost a student or employee the replacement fee of $400.

Use of Personal Electronic Devices

In accordance with all district policies and procedures, students and staff may use personal electronic devices such as, but not limited to, laptops, mobile devices, cell phones, and e-readers to promote student learning and to further the educational and research mission of the district. The use of personally owned devices at school by staff and students is voluntary and a privilege, and subject to all school district policies and procedures. School staff will retain the final authority in deciding when and how students may use personal electronic devices on school grounds and during any school-related activity.

The district assumes no liability or responsibility for any act of a staff, student or guest user that is inconsistent with school district policies and procedures. Any individual who brings personally owned devices onto school property is solely responsible for that equipment.

If the District has reasonable cause to believe a staff member or student has violated school district policies or procedures authorized personnel may confiscate and search a staff, student's or guest user's mobile device in accordance with school district policies and procedures for privacy, and search and seizure.

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.

Recommended

WASHINGTON CENTRAL UNIFIED UNION SCHOOL DISTRICT

Board of Directors' Policy

ELECTRONIC MAIL

POLICY: F47

WARNED: _____

ADOPTED: _____

EFFECTIVE: _____

Overview
Electronic email is pervasively used in almost all industry verticals and is often the primary communication and awareness method within an organization. At the same time, misuse of email can post many legal, privacy and security risks, thus it's important for users to understand the appropriate use of electronic communications.

Purpose
The purpose of this email policy is to ensure the proper use of WCUUSD email system and make users aware of what WCUUSD deems as acceptable and unacceptable use of its email system. This policy outlines the minimum requirements for use of email within WCUUSD Network.

Scope
This policy covers appropriate use of any email sent from a WCUUSD email address and applies to all employees, vendors, and agents operating on behalf of WCUUSD.

Policy

- All use of email must be consistent with WCUUSD policies and procedures of ethical conduct, safety, compliance with applicable laws and proper business practices.
- WCUUSD email account should be used primarily for WCUUSD business-related purposes; personal communication is permitted on a limited basis, but non-WCUUSD related commercial uses are prohibited.
- All WCUUSD data contained within an email message or an attachment must be secured according to the Data Protection Standard.
- Email should be retained only if it qualifies as a WCUUSD business record. Email is a WCUUSD business record if there exists a legitimate and ongoing business reason to preserve the information contained in the email.
- Email that is identified as a WCUUSD business record shall be retained according to WCUUSD Record Retention Schedule.
- The WCUUSD email system shall not to be used for the creation or distribution of any disruptive or offensive messages, including offensive comments about race, gender, hair color, disabilities, age, sexual orientation, pornography, religious beliefs and practice, political beliefs, or national origin. Employees who receive any emails with this content from any WCUUSD employee should report the matter to their supervisor immediately.
- Users are prohibited from automatically forwarding WCUUSD email to a third-party email system. Individual messages which are forwarded by the user must not contain WCUUSD confidential or above information.

- Users are prohibited from using third-party email systems and storage servers such as Google, Yahoo, and MSN Hotmail etc. to conduct WCUUSD business, to create or memorialize any binding transactions, or to store or retain email on behalf of WCUUSD. Such communications and transactions should be conducted through proper channels using WCUUSD-approved documentation.
- Using a reasonable amount of WCUUSD resources for personal emails is acceptable, but non-*work-related* email shall be saved in a separate folder from work related email. Sending chain letters or joke emails from a WCUUSD email account is prohibited.
- WCUUSD employees shall have no expectation of privacy in anything they store, send or receive on the company's email system.
- WCUUSD may monitor messages without prior notice. WCUUSD is not obliged to monitor email messages.

The Internet has been plagued with hoaxes alleging various security problems. Many of these hoaxes take the form of phishing attacks or chain letters, which request that the receiving party send the message to other people. Service users in receipt of information about system vulnerabilities should forward it to the WCUUSD Information Technology Helpdesk (ithelp@u32.org), who will then determine what if any action is appropriate. Service users must not personally redistribute system vulnerability information.

Distribution of Unsolicited WCUUSD Marketing: Service users must not use facsimile (fax) machines, electronic mail, instant messenger, auto-dialer robot voice systems, or any other electronic communications systems for the distribution of unsolicited advertising material.

Recommended

WASHINGTON CENTRAL UNIFIED UNION SCHOOL DISTRICT

Board of Directors' Policy

INCIDENT RESPONSE POLICY AND PLAN

POLICY: F48

WARNED: _____

ADOPTED: _____

EFFECTIVE: _____

Overview

In accordance with security best practices, all security incidents will be formally documented and responded to. This policy provides some general guidelines and procedures for dealing with computer security incidents.

Purpose

The WCUUSD is committed to maintaining the security of electronic information. Formal practices of tracking and mitigating security incidents will aid in assessing potential risks and vulnerabilities to data. As such, WCUUSD will continually assess risks and improve security measures.

Incident Examples

Some examples of possible incident categories include:

- Compromise of system or data integrity
- Denial of system resources.
- Illegal access to a system (either a penetration or an intrusion).
- Malicious use of system resources
- Inadvertent damage to a system.
- Malware or virus detection.

Some possible scenarios for security incidents are:

- Loss of a laptop or device containing, HIPAA, PII and/or other WCUUSD – data.
- Suspicious activities or anomalies that are identified through intrusion detection, firewall or other network device logs. You have discovered a major virus has infected multiple systems.
- Damage, intentional or accidental, to equipment or system affecting its ability to perform its job.
- Unauthorized wireless access points.

Incident Reporting

All suspected policy violations, system intrusions, virus infestations, and other conditions which might jeopardize WCUUSD information or WCUUSD information systems must be immediately reported to the WCUUSD Information Technology Helpdesk (ithelp@u32.org), who will coordinate with the WCUUSD Director of Technology and/or Superintendent.

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