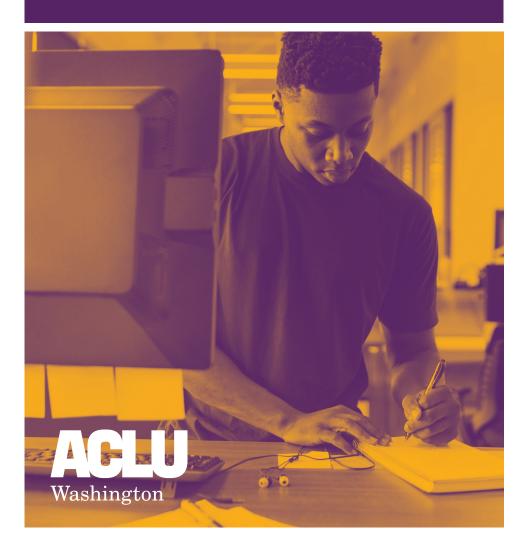
WASHINGTON STUDENT TECH GUIDE: RIGHTS & RESPONSIBILITIES IN THE

DIGITAL AGE



2

Washington Student Tech Guide: Rights & Responsibilties in the Digital Age

This guide addresses the rights of students in K-12 public schools in Washington. The rights of students in private schools or in college may differ.

You can find more general information on student rights, available in English and Spanish, in the Student Rights section of our website, www.aclu-wa.org.

Published November 2017 A project of the American Civil Liberties Union of Washington

INTRODUCTION

Communicating with electronic devices and on the Internet – whether through text message, chat, e-mail, Facebook, blogs, Twitter, Tumblr, image boards or countless others – raises both new and old questions about your legal rights.

Schools have an important duty to provide education for all students, and students are responsible for following reasonable school rules so school remains a safe, welcoming place where all students can learn. But students also have free speech and privacy rights that our schools must recognize and respect.

Can a school limit what students do online? Must students give administrators access to their private text messages, photos, e-mails, and contacts on their cell phones? Do students need permission to videotape other students or teachers at school?

This booklet provides information about legal rights online and the limits to those rights. It outlines your right to express yourself online and what kinds of speech can get you in trouble. It describes your privacy rights – and how you can respect the privacy rights of others.

I. TECHNOLOGY AND FREE SPEECH

You have the right to express yourself online, whether you are writing e-mails, posting to a blog, updating a homepage, or talking in a chatroom. Yet you also are responsible for your actions as they affect others.

A. The Basics on Freedom of Expression

Congress shall make no law...abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition the government for a redress of grievances.

 $U.S.\ Constitution, Amendment\ I$

Every person may freely speak, write and publish on all subjects, being responsible for the abuse of that right. Washington Constitution Article 1, Section 5 The U.S. Constitution and the Washington Constitution guarantee freedom of expression for everyone, including students. Students do not give up their constitutional rights when they walk onto school grounds. Whether you want to comment on a new school rule, gay rights, teen pregnancy, or the latest national news, you have the right to express your ideas, including those that are controversial. But there are limits.

In some situations, speech can be restricted at school, even if it would be protected in the community outside of school. To restrict your speech or impose discipline, the school must have a good reason to believe that your expression will disrupt school or infringe on the rights of others. Keep in mind that speech on controversial subjects may sometimes disrupt school if done at the wrong time or place — such as giving a sexually suggestive speech at a school assembly, or promoting illegal drug use at a school function. In other cases, schools can limit controversial subjects if the school is sponsoring the speech — such as when the school publishes a newspaper. But in most situations, school administrators and teachers cannot prevent you from saying something just because it is controversial.

When speech on sensitive topics stirs passionate feelings, the best response is usually more speech – not less.

There are also some limits on the freedom of expression that apply to everyone. The constitutional right to freedom of expression generally does not cover speech that is:

- A true threat
- A defamatory statement
- Obscene

Here is what each of these means.

True Threats

Whether you are in school or not, online or in-person, the right to free speech does not protect speech that a reasonable person would interpret as a serious expression of your desire and ability to harm him/her.

Defamatory Statements

The right to free speech also does not protect false personal attacks against another person that are untrue, that harm someone's reputation, and that you knew, or should have known, were untrue when you said or wrote it.

Obscene Speech

The right to free speech does not protect speech that deals with sex in a manner appealing to purely lustful interests in a patently offensive manner, and without serious literary, artistic, political, or scientific value.

When speech is directed toward minors, the legal definition of obscenity is broader. Courts have said speech is obscene for minors if it appeals to their "prurient, shameful, or morbid interest in sex," is patently offensive with respect to what is suitable for minors, and is without redeeming social importance

DIFFERENCE BETWEEN A JOKE AND A THREAT

School authorities are understandably sensitive about provocative statements or jokes about violence. True threats are not protected inside of school or out. For speech to be considered a "true threat," it must be something that a reasonable person would interpret as a serious expression of an intention to harm him/her.

for minors. Swear words, by themselves, are not "obscene," in the legal definition of the term.

B. Using Electronic Communications at School

Technology Policies

Most schools have written policies on student computing and technology use. Perhaps you've had to sign a technology use agreement. These rules and policies might limit what you do on:

- School desktop computers and laptops
- · School-sponsored e-mail accounts and discussion groups
- · Any school Internet connection, including Wi-Fi

The rules must be reasonable and have educational purposes. Be sure to read and understand your school's technology or computing policies. Ask a teacher if you cannot find a copy.

$School ext{-}sponsored \ E ext{-}mail \ Accounts$

If the school provides students with an e-mail address, it can impose rules on its use. For example, it can require that the address be used only for school-related purposes and can prohibit using the account in a way that interferes with

Your school may limit your online activites at school for valid educational reasons.

It may also monitor what you view, send, or receive on school-provided computers or e-mail accounts.

another student's learning, such as sending flames or bullying messages.

But if your school does not have such a policy, it can discipline you only if what you write disrupts school activities or infringes on the rights of others.

School officials may not censor what is said in an e-mail simply because they disagree with the thoughts. For example, you may criticize a school policy or a school board action. You have the right to express your views on public issues, and doing so does not in itself interfere with the school's educational goals.

C. Using the Internet at School

Schools may place reasonable limits on Internet access in order to maintain a working educational environment.

Your school may prohibit all access to the Internet on any computer. Or your school may prohibit using school computers to access the Internet, including sites such as Facebook or YouTube, or using Hotmail or Gmail accounts, if school officials believe access is disruptive to the school. Or your school may just bar online activities in class if officials believe these activities disrupt school. Be sure to check your own school's policy for Internet use.

When you are using the school's computer and Internet access, school officials can see what you are sending and receiving online. To protect your privacy, stick to doing only academic work when using school computers. Check your personal e-mail or non-school-related websites outside of school, on your own time, with a computer that does not belong to the school.

Internet Filtering

School computers often are equipped with filtering software that prevents access to websites considered improper for a school setting or which contain harmful software, such as viruses or spyware.

Unfortunately, these filters sometimes block more websites than necessary, such as sites dealing with sexual health, sexual identity, political groups, or religion.

If you think your school is blocking academically useful information, here's what to do:

- Read your school's Internet use policy.
- Write down why the website would be useful to your education, including details about your related schoolwork and the website's address. Be sure to explain how your desire to access the website fits into your school's current policy on Internet use.
- Ask school staff to adjust the filter so you can see the site.
- Consider asking that your school filtering policy be updated to allow more access to academically useful materials.
- If your school continues to block academically useful information, please contact the ACLU. Be sure to keep notes about the actions you take, including a journal of whom you talk to on specific days.

D. Using the Internet Outside of School

Your right to express yourself from a computer outside of school is a different matter from what you do at school or with a school computer.

A school's authority to govern student speech generally does not extend to speech that takes place off campus or outside of a school activity. Your school may not enforce rules for what you read online when you are at home or other places away from school.

Discipline for Off-Campus Posting

The school does not have authority to impose discipline for writing or posting about a school-related topic, or posting an opinion that school officials don't like.

But merely because you are off campus, you are not free to say just anything. Remember, state and federal laws make it illegal to post threats of violence against a person or to advocate certain illegal actions. If, for example, something you post outside of school is considered a "true threat" or is false and harms someone's reputation, you may be subject to police investigation and punishment by the courts, and your school

may be notified. It does not matter whether the speech occurs in a chat room, text message, IM, video game, blog comment, website, or anywhere else in the virtual world.

Generally, your school cannot censor or discipline you for posting content or sending a message that is:

- sent during non-school hours;
- and sent using an off-campus Internet connection;
- and sent using a non-school computer;
- and sent using a non-school e-mail address.

Some administrators do try to discipline students for off-campus Internet speech that they believe has disruptive effects at school, such as allegedly interfering with classes or the ability of others to learn. Courts generally have said students cannot be disciplined for off-campus speech, though schools may respond to online speech that connects the school with violent imagery. In some situations, schools can punish students for online speech that is likely to disrupt school activities. These situations are very limited. If you are threatened with discipline for off-campus speech, please contact the ACLU.

If your online postings demonstrate that you broke school rules, the school can discipline you. For example, you could get in trouble if you post a video of yourself and friends skipping school. And if you post about doing something illegal, law enforcement may use it as evidence against you.

While it may be lawful to post something on a public website, doing so may not be wise. Keep in mind that school officials, college admissions officers, and potential employers are free to look at it. What's more, what you put on a public website may stay on the Internet forever. Other people could take your posting and copy

POSTING INFORMATION ON THE INTERNET

It can be like publishing it in the newspaper. If the website is public, anyone can look at it.

it to another website where you can't delete it. If the post includes your name, anyone "Googling" your name will find it, even many years down the road. Some people have been denied jobs because of material they posted on the Internet, so think carefully before you post.

Cyberbullying – Don't Do It!

School officials have a responsibility to ensure that the school is a welcoming place for all students. Bullying, in-person or through electronic means, is a form of aggression that can cause fear, shame, or worse, and interferes with another student's right to receive an education.

By law, schools must adopt rules to prevent on-campus bullying and are expected to swiftly respond to incidents of bullying. Under these rules, what you say and do electronically may not:

- have the effect of substantially interfering with another student's education;
- be so severe, persistent, or pervasive that it creates an intimidating or threatening educational environment; or
- Have the effect of substantially disrupting the orderly operation of school; or
- threaten physical harm to someone at school.

OUR WORK ON STUDENT INTERNET SPEECH

The ACLU has helped students stand up for their rights when schools tried to discipline them for off-campus Internet speech and when schools didn't act to stop bullying and harassment of students.

Learn more about the cases and how they turned out in the Youth section of our website: www.aclu-wa.org. A school's anti-bullying policy must be written carefully so that it does not punish opinions or beliefs in and of themselves, but instead punishes impermissible conduct.

Schools are authorized only to investigate harassment and bullying on campus. Evidence of off-campus bullying, however, puts the school on notice to ensure the student is not being harassed on campus.

II. RECORDING PEOPLE AT SCHOOL

A. Your Speech and Other People's Privacy

Whether you're recording a conversation or taking pictures with your cell phone, you have to respect other people's privacy rights.

Audio Recordings

In Washington, it is against the law to record a private conversation without the permission of all people being recorded. This includes conversations that you have over the phone or may overhear in the hall.

Ask for permission before you record a conversation. If the person agrees, then recording is okay. With a group of people, try to get their consent, if at all possible. At the very least, you should announce that you are recording so everybody knows and can ask you to stop. If someone asks you to stop, or the person you asked does not agree, recording the conversation is illegal. If you don't ask or announce, don't record.

Make sure you know your school's policy for taking photos or video at school.

It may be against the rules to bring a recording device, including a cell phone, to school.

Photographing or Videotaping

Photography, like other art forms, is considered a type of speech, so a school cannot punish you for the message conveyed by your photograph (presuming that it is not obscene.)

However, your school may have rules against taking pictures or video without the consent of the subject. And some schools simply forbid the use of electronic devices such as cell phones at school.

If such policies exist, you could get in trouble by breaking the rules against taking a photo or video. For example, if you use a cell phone secretly to capture a video of your teacher and post it on YouTube from home, you could face discipline.

Sexting

Taking, sending, viewing and even possessing nude, semi-nude or other sexually explicit images, videos, or other digital content, also known as "sexting," can get you into serious trouble both at school and with the law. Underage sexting, even when consensual and even if you took the pictures of yourself, is currently illegal under Washington child pornography laws. You could be charged with a felony and, if convicted, you might be forced to register as a convicted sex offender for the rest of your life. Forwarding images, videos, or other digitally sexted content you receive from another person could also run afoul of other criminal laws, including those prohibiting harassment and cyberstalking.

B. The School's Use of Technology to Monitor Students

Schools are permitted to use technology to promote safety on school grounds. In doing so, schools must respect student privacy.

Surveillance Cameras

Generally, schools are allowed to watch and record students with video cameras while they are in common areas at school or on the bus. Schools cannot, however, record the audio of your private conversation without your consent.

And video cameras cannot be put everywhere. Students have a right to more privacy in certain areas of school, such as a locker room or nurse's office, where someone could be undressing. It is not okay for a school to videotape you in such places.

Remember, a school is not required to obtain your permission before videotaping you if the video does not include the sounds of private conversations.

The video captured from school surveillance cameras is considered a "public record." It does not have to be kept private, and under the state's Public Disclosure Act, the school must provide the tapes to anyone who requests them.

Location Tracking Devices

A number of new technologies are being developed which enable school officials to monitor the movements and location of their students.

Some of these tracking devices have capabilities that could go far beyond the school's authority to monitor students. Some parents and students have been successful in asking their school boards and school officials not to use such technology.

For example, a California elementary school introduced a program to track students through high-tech chips, called "RFID tags," in the school ID cards students wore around their necks. The ACLU helped parents who objected that RFID tracking was a demeaning practice that violated the privacy of students and jeopardized their safety by broadcasting location information to anyone with a chip reader. The school ended the program.

If your school requires you to carry a tracking device, talk to your parents and contact the ACLU.

Is your school monitoring your location?

- Gather information about when and where you have to use the tracking device.
- · Read your school's policy.
- Talk to your parents about the program.
- Identify what you want to do such as talking to other students, writing a letter to the newspaper about it, or asking school officials or the school board to make a change.

Be sure to keep notes about the actions you take, including whom you talk to and when.

III. SEARCHES AT SCHOOL

The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated...

U.S. Constitution Amendment IV

No person shall be disturbed in his private affairs, or his home invaded, without authority of law. Washington State Constitution, Article I, Section 7

The U.S. Constitution and the Washington State Constitution protect your privacy by prohibiting unreasonable searches and seizures. These rights extend to personal possessions and the information you store on items like cell phones, personal computers, and e-mail.

A. The Basics on Searches in School

When you are at school, the law specifies how you and your belongings can be searched; however, the standard differs depending on who is doing the searching – school officials or law enforcement officers. Here is some basic information about your privacy rights at school, plus information on how those rights apply to particular technologies.

Searches by School Officials

Before searching through your personal items, school officials need to have both reasonable and individualized suspicion.

Reasonable Suspicion

The U.S. Supreme Court has said that school officials may search a student or a student's property if they have a reasonable suspicion that the search might uncover evidence that the student violated a school rule.

Reasonable suspicion might be based on a school official overhearing, seeing, or smelling something first-hand, or on a tip from a reliable source. School officials also must be reasonable in the way they search you, based on your age and what they are searching for. However, if you voluntarily consent to a search,

the school does not need even reasonable suspicion to conduct the search. School officials cannot insist that you consent to a search. You can say "no" to a search of you or your property, and you can ask to contact your parents.

Individualized Suspicion

If, for example, the teacher or the principal has a reasonable suspicion that someone has been selling drugs or alcohol via text messages, it does not mean he or she can search everyone's cell phone.

School officials must have a reasonable suspicion that a search of a particular student will uncover evidence of a violation of a school rule. For example, if a school official has information that some students in an online group are bullying

VOLUNTARY SEARCHES

- If a school official asks you to voluntarily consent to a search, you have the right to say No.
- When you say No, the official can search you only with reasonable suspicion that you have broken a school rule.
- You can ask to contact your parents.

another student via text messages, that does not justify a search of all students in the group.

Being Searched by Law Enforcement?

If any officer, including a School Resource Officer, wants to search you or your belongings – including your personal technology (cell phone, PDA, laptop) – you can:

- Ask if they have a warrant.
- If they insist on searching without a warrant, tell them that you do not consent to the search.
- Ask if you are free to leave.
- Tell the officer you want to talk to your parent or a lawyer before answering any questions.

Remember, you never have to say you agree to a search, and you have the right to remain silent.

Searches by Law Enforcement Officers

The rules are different when law enforcement officials search students. To conduct a search at school, they generally must follow the same restrictions that apply outside of school – which usually means getting a warrant. These rules also apply to police officers working in schools as "School Resource Officers."

Be polite but firm when talking with law enforcement, and never physically resist an officer.

B. Searches of Online Information

Just as anybody can read a letter to the editor that is printed in the newspaper, anybody can read what is written on a public webpage. If you post information online, comment on a friend's public profile, or post to YouTube, your comments are visible to anybody. This includes school officials, future employers, and law enforcement, who can look at it just as anyone else can.

Social Networks and Personal Postings

Some content on the Internet is not publicly available, but requires a login and password to be seen. For some web pages or e-mail accounts, you might be the only person with the password. Other websites like MySpace and Facebook allow you to change your privacy settings so that instead of your information being public, the information is only available to people to whom you give your access code (and to whomever those people give the info). Some e-mail lists also work this way, requiring the permission of the list's moderator before people can join and read messages.

Even with passwords and a small group of people seeing your content, your online information is not guaranteed to be "private."

Your online friends could:

- Show your pictures and comments to school officials or others from their account.
- Copy your text or photographs from your page and paste it into e-mail or onto another public website, where anybody could see it.
- Print out what is on their computer screen to pass around at school or work.
- If someone provides school officials with information, school officials are allowed to look at it and may act on it.

Online companies such as Google or Facebook, among countless others, can see, use, distribute, and sometimes sell your private computer activity. When you type a search request into Google, it records the IP address (the address given to you by the company that provides your Internet service), the query, the date and time, and the links you go to. Companies can also share your information with other companies or the government without you knowing about it. So keep your privacy in mind when posting.

Security and Anonymity Online

Putting your real name, address, or phone number on a public website is like putting the information up on a billboard – anybody can read and use the information for any purpose, without you ever knowing.

To protect your personal information from being used without your permission, you should not give out this information when posting or communicating online. Use a screen name, username, or e-mail address that does not provide personal info when communicating online. However, whoever provides your Internet connection still may be able to identify you through your computer's Internet Protocol (IP) address. All of the content you send, even under a pseudonym (fake name), will be tagged by an IP address. Plus, to get your anonymous online account, you probably had to provide an e-mail address or other personal info that links to your real-world identity.

In the U.S., we have the right to speak anonymously, including online. If someone seeks a court order for an Internet service provider (ISP) to disclose a student's real-life name that is linked to a screen-name, avatar, or other online persona, the student can go to court and seek to have the request denied. Your ISP may have a privacy policy that says that if it gets a request for your identity, it must inform you before providing the information, so that you can challenge the request. Check your ISP's privacy policy to see what it says about providing personal information about its users.

Everything done online likely can be connected back to a specific IP address. So even though your activities may appear anonymous, all of your actions online probably can be traced. That means everything from what you ask of search engines to what you post on Wikipedia or You-Tube. Some businesses even keep records of the multiple IP addresses you use to access a certain online account.

While you do not have the right to engage in illegal conduct online, such as harassing others or downloading copyrighted music without paying for it, your right to make online comments anonymously is an important First Amendment right. If you learn that your school is seeking to force your ISP to disclose your identity because of anonymous comments you have made online and you believe your identity should be protected, you should contact the ACLU. We may help you oppose the school's efforts if we feel that your First Amendment right to speak anonymously online will be violated if you are identified.

C. Searches of Communications Devices

The devices you carry contain all kinds of information about you. Think about all the information stored on your phone: phone numbers you call, friends you contact, your text or e-mail conversations, photos, videos, websites visited, location, and more! You have a right to keep this information private to a large extent, but there are limits.

This section provides info about when and how school officials may search the technology that you (or your family) own and bring onto school grounds.

Cell Phones

If school policy forbids having cell phones at school, then the school can take your cell phone until the end of the school day. But even if the phone is confiscated, your school does not have a right to read, copy, or search its contents.

IF A SCHOOL OFFICIAL
ASKS FOR PERMISSION TO
SEARCH YOUR PHONE, YOU
DO NOT HAVE TO CONSENT.

A school can search a cell phone only if it has reasonable, individualized suspicion that you personally broke a specific school rule. The search must be reasonable and must be limited to content that is reasonably necessary to confirm or dis-

pel the suspicion of wrongdoing. The search must stop once the suspicion has been dispelled.

In California, a teacher took a high school student's cell phone away after he was caught talking on it despite a school rule forbidding cell phone use at school. However, school officials went too far when they read the text messages stored on the student's phone, even though they had no reason to believe the student was violating any other school rule. After the ACLU explained the law to school officials on behalf of the stu-

dent, the school district agreed to change its policy and to instruct school staff so that the problem would not occur again.

Remember, you do not have to consent to a search of your phone. A school official may go into your closed bag or purse to find your cell phone only if he or she has a reasonable suspicion that the search might uncover evidence you violated a school rule or the law. If your school seizes your phone and does not give it back at the end of the day, ask your parents to contact the school.

Lockers are a different story. Washington state law says these are school property that can be searched at any time, with or without reasonable suspicion. But this does not mean that the information on your cell phone inside your locker can be searched without reasonable, individualized suspicion.

Even if school officials temporarily seize your cell phone because you have violated a "no cell phones on campus" rule, they may not search the phone to investigate you or other students for other possible misconduct unless you consent to such a search. A school official may not text-message, IM, or call your fellow students using your phone without your consent.

In Colorado, high school officials suspected a student had violated school rules by smoking on campus. After a search did not find any cigarettes on the student, the assistant principal seized his phone, and read and sent text messages to other students, posing as the student. The school repeated this activity with at least a dozen other students: seizing and searching their cell phones, going through their text messages, and transcribing "incriminating" text messages. The ACLU worked with students and their parents to convince the school district that searches of students' cell phones without their consent violated Colorado state privacy law as well as the state and federal constitutions. As a result, school officials now must obtain the student's or parent's consent and comply with constitutional standards before searching a student's cell phone unless there is an imminent threat to public safety.

Laptops

Whether school officials can seize and search a laptop depends on who owns it – you or the school.

- If you are allowed to bring a personally owned laptop to school, school officials may confiscate and search your laptop only if there is reasonable suspicion that it contains evidence you violated school rules. The officials must return your laptop once they have the evidence they need, or have dispelled the suspicion of wrongdoing.
- If the school has a policy that you can't bring your own laptop
 to school and you do so anyway, school staff can take it away
 until the end of the school day. The ACLU believes it would
 be illegal for them to search it without reasonable suspicion
 that it contains evidence you violated school rules; however,
 the courts have not yet ruled on this.
- If the laptop you're using belongs to the school, school
 officials can take it back from you at any time. The school
 may be able to search the laptop for files even if there is no
 suspicion of wrongdoing, but the courts have not ruled on
 this yet.

Just as with cell phone searches, a search of your personally owned laptop must be reasonable and limited to confirming or dispelling the school's suspicion. If school officials reasonably believe that you violated a school rule and that there is evidence of that violation on your personal laptop, they may search your laptop to look for and copy only the files related to that violation. Officials must stop searching and copying your files once they have found what they are looking for, and they should return your laptop. They may not copy files that have nothing to do with the violation of school rules.

For example, if the school has a specific reason to suspect you sent a threatening e-mail to another student, the school could look for evidence of that on your laptop; but it could not look through your personal digital photos because those are not necessary to investigate the e-mail threat. When the search is complete, the school should give the computer back.

Passwords.

Again, what school officials can do depends on whether your password is for a school-affiliated or for a personal account or device.

If the password is to an account (such as e-mail) or a device (such as a laptop) that belongs to you and not to the school, then your teacher generally cannot make you give up your password. However, it is different if the school wants access to a school-sponsored e-mail account or school-owned computer. In that case, since you are using the school's property, school officials may require you to give your password to them. If you want to refuse to turn over the password, please discuss your situation with your parents and/or a lawyer.

Keep in mind the important difference between personal property and school property when you are using technology. If you want to send e-mail you would rather your teacher not see, do it outside of school on a non-school computer using your personal account. The same goes for computer files: if you want to keep something private, do not put it on a school computer.

IV. WHAT TO DO IF YOU THINK THE SCHOOL HAS VIOLATED YOUR RIGHTS

When you go to school, you have to obey your school's written rules. The school rules must be reasonable and have a logical relationship to the school's educational purpose.

If you are in a meeting with school officials and think something is wrong, ask to call a parent or guardian. If you are being accused of wrongdoing, it is best for an adult who is responsible for you to be with you during the meeting. If you are not permitted to call your parents, tell them as soon as possible about what happened.

If you think the school has violated your rights, write down what and when it happened, who was involved, what they said and did, and what they asked you to do.

If you have questions about your rights at school or want help in protecting them, call the ACLU to see if we can assist you.

www.aclu-wa.org or (206) 624-2180

