Microsoft

Digital Citizenship

Best Practices:

Safety and Privacy Online

Describe a good citizen

- Respect the laws of your country, state, and city
- Respect others
- Help others
- Take care of the environment

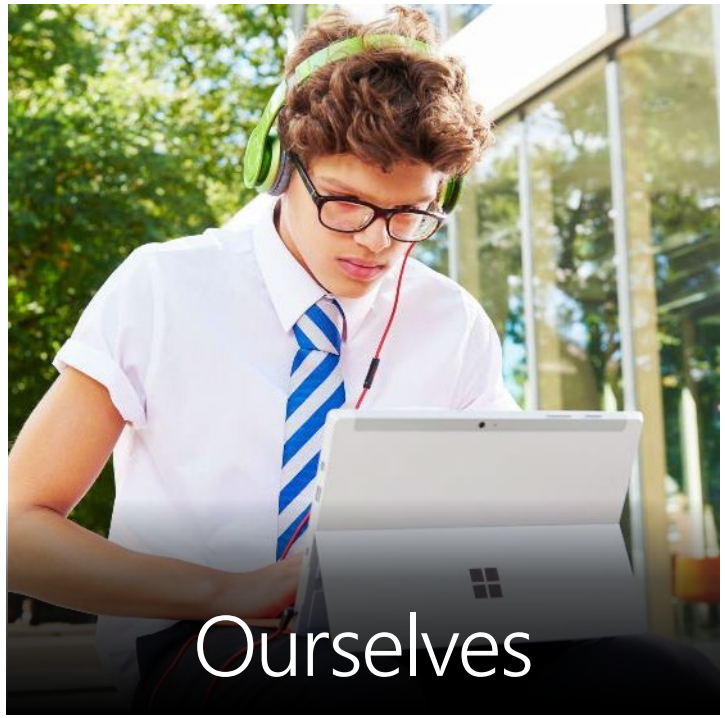
What is Digital Citizenship?

"the norms of behavior with regard to technology use"

What is Digital Citizenship?

???

How we treat…



How you treat yourself

- Your safety
- Your privacy
- Your reputation

Why do we lock our doors?

Protection (Safety)

- For ourselves
- For our possessions

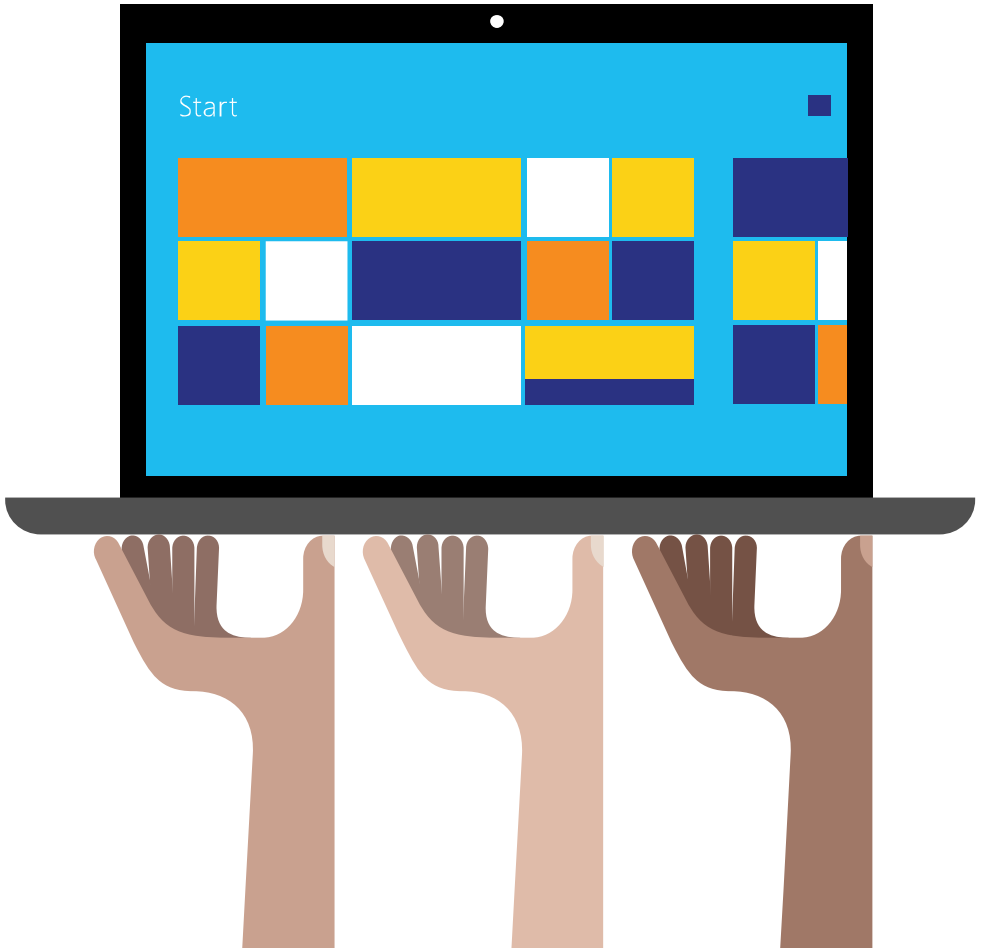
Privacy

- Of our information
- Of our activities

Treat your online safety like any other valuable

Your computer has valuables too

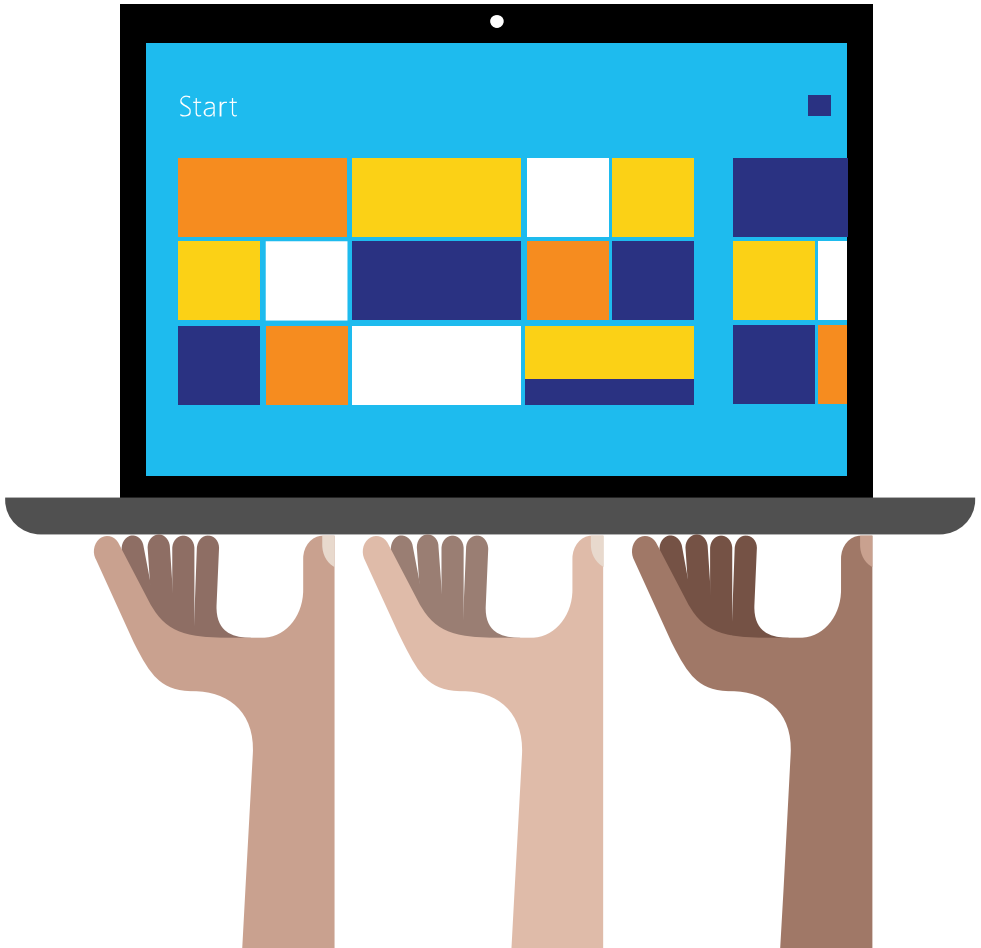
- Your parents' financial information
- Your personal information
  - Your age
  - Your address
  - Your pictures
- Your reputation
  - What people think of you



Treat your online safety like any other valuable

Your computer has valuables too

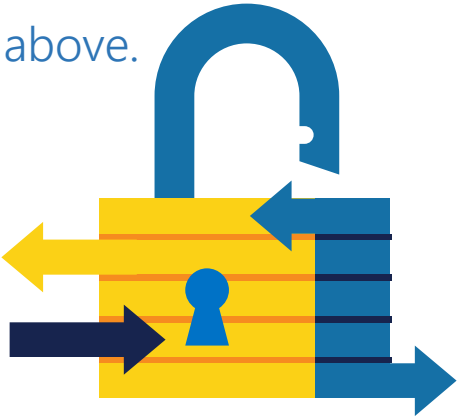
???



Use strong passwords and keep them secret

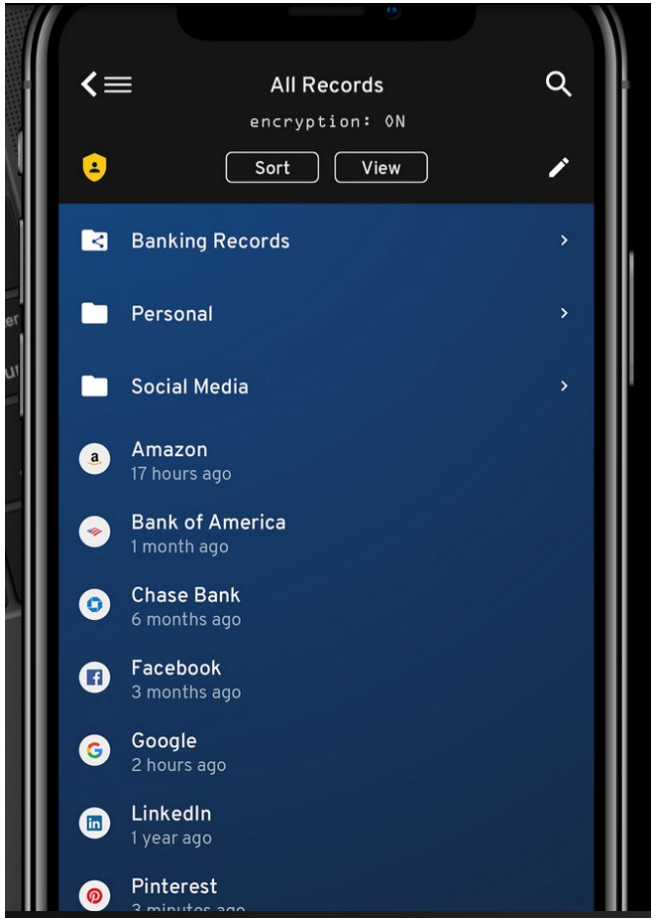
Strong passwords are:

- Long; mix capital and lowercase letters, numbers, and symbols
- Easy for you to remember; hard for others to guess: a PASS PHRASE!
  - Milo likes to play football – M!loLikes2PlayF00tball
  - Strong passwords are safer – Str0ngpassw0rdsRsafer!
  - I love popcorn – !L0veP0pc0rn
- Our IT department recommends *any* phrase of *15 characters* or more:
  - Milolikestoplayfootball works just as well as the more complicated example above.
- Use different passwords for different accounts
- Write your passwords down and keep them safe
- Turn on two-step verification when available



How do I remember all my passwords?

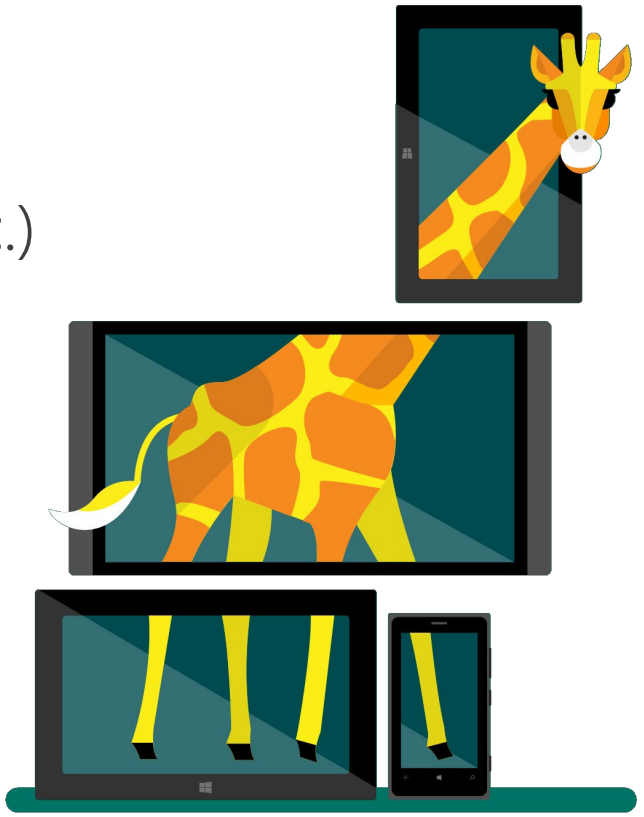
- **Write them down and keep them safe** Everyone can forget a password. Keep a list that's stored in a safe, secure place away from your computer.
- Ask your parents if they use a password manager and could help you set one up for yourself.
- Bear Creek does not recommend any one solution, however, here are some examples:
  - LastPass: https://lastpass.com/
  - Keeper: https://keepersecurity.com/
  - Dashlane: https://dashlane.com/



Password management

Lock your phone with a PIN

- No sequential numbers (6789)
- Don’t repeat the same numbers (3333)
- Don’t use your own numbers (e.g. address, phone, etc.)



Don’t share your password or PIN

- WITH ANYONE
- Not even your best friend
- Never email, text, or put a password in a chat.

Use strong passwords and keep them secret

???

Phishing: Don’t be tricked

Sometimes emails that look genuine aren’t

- Treat all requests for personal information with caution

Friends’ emails can be hacked

Criminals can build fake websites

Never share your password in response to an email or phone request

Think, then click

- Before you click links
- Before you open attachments
- Even if you know the sender

How Do We Help Our Valuables Last?

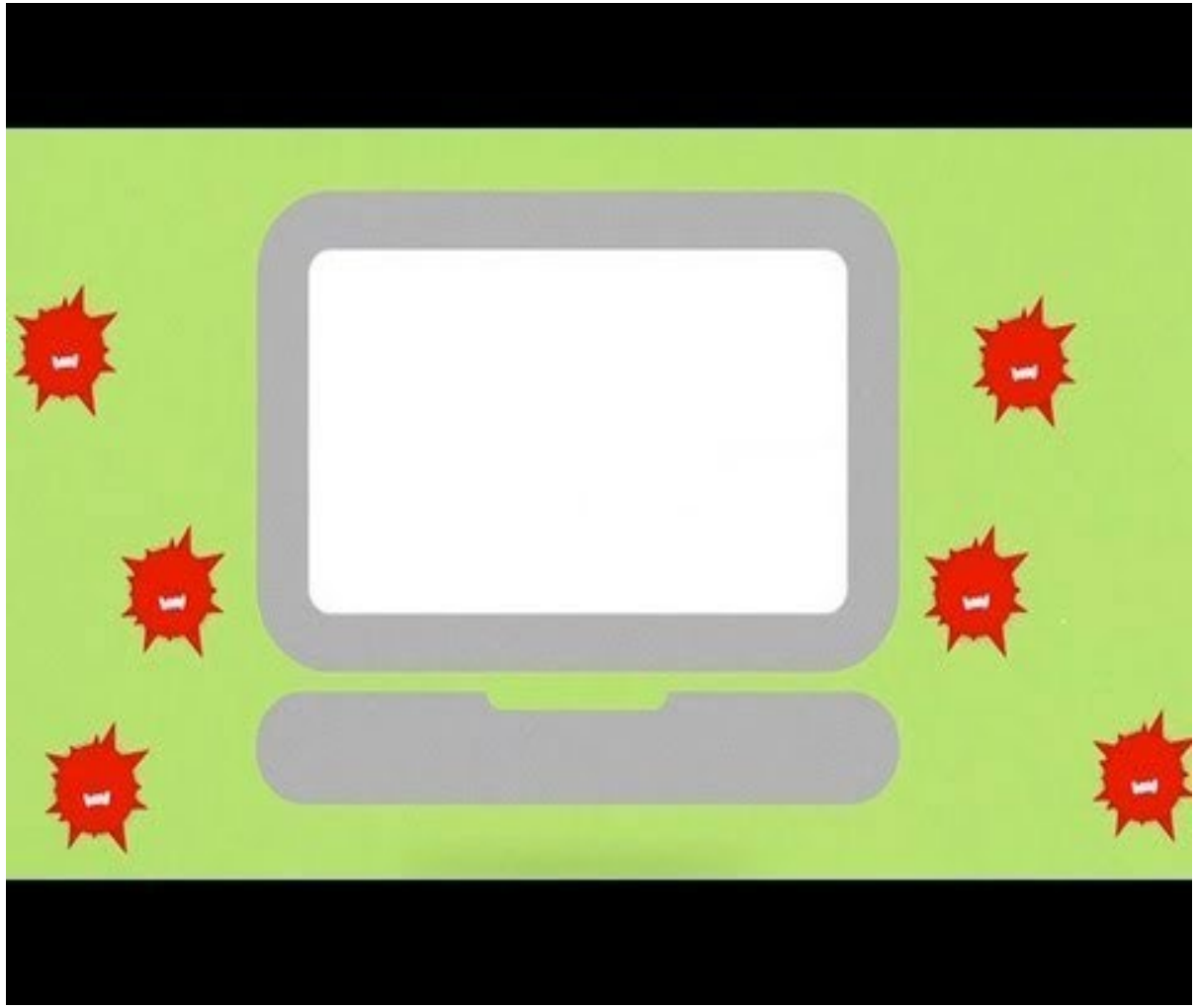
Maintenance for a car

- Change the oil
- Rotate the tires

Take Care of Our Clothes

- Wash them
- Hang them up

Protect your devices



Protect your devices

- Keep all software (including your web browser) current with automatic updates
- Install legitimate antivirus and antispyware software
- Never turn off your firewall
- Protect your wireless router with a password
- Use flash drives cautiously
- Only download reputable apps
- Use secure webpages (https://) when entering sensitive data

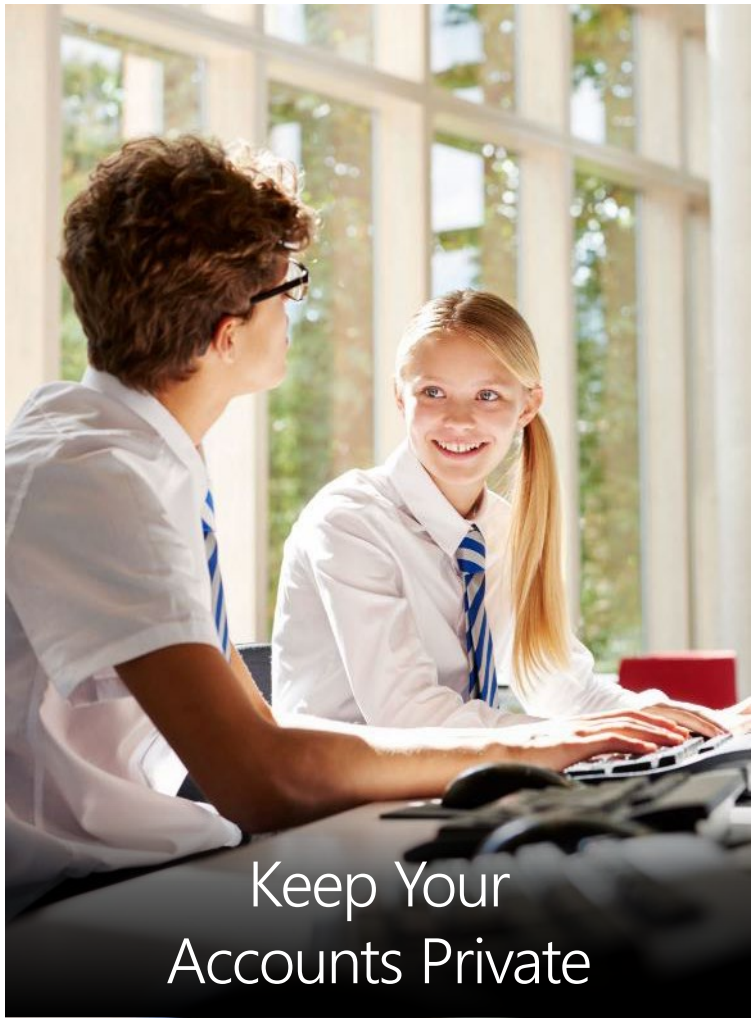
How would you feel…

…if you were at a restaurant with a friend and someone you have never met walked up to your table, sat down, and joined in your conversation?

…if you were shopping for some jeans with your friends (or your parents) and when you walked out of the dressing room someone you did not know shared her opinion about how you look in the jeans?

…if someone you did not know entered your home, entered your bedroom, and started reading through your journal (or looking through the pictures on your phone)?

Why would you treat your online world differently?



If you wouldn't want a stranger hanging out with you at dinner, shopping with you, or hanging out in your room, don't invite a stranger into your online world.

Make your social network pages private. Look for the **Settings** or **Options** area on your social media sites to manage who can see your profile, who can find you, who can tag you in photos, and who can make comments.

Be a good friend…

Stand up for your friends. Cyberbullies are less likely to target someone who has a strong group of friends, and usually stop when a victim's friends rally around him or her. (Cyberbullies may be surprised to learn that their actions may be crimes.)

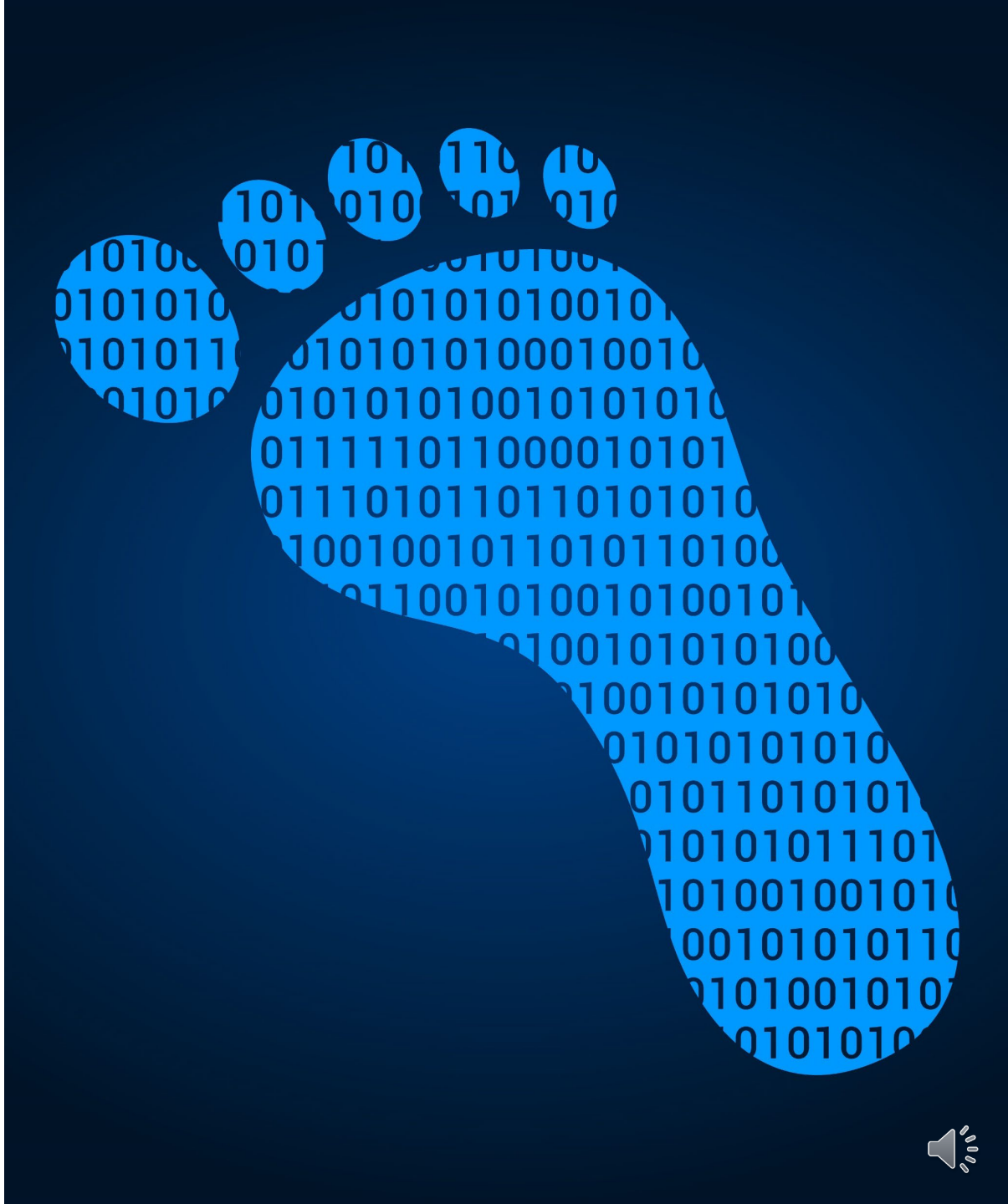
Don't share online personal details of friends and family members without their permission. You should ask permission before posting photos or videos.

Be a good friend…

???

What is your Digital Footprint?

ALL of your activity on the Internet



What is your Digital Footprint?

Examples:

Comments on a blog

Pictures shared on Instagram or Snapchat

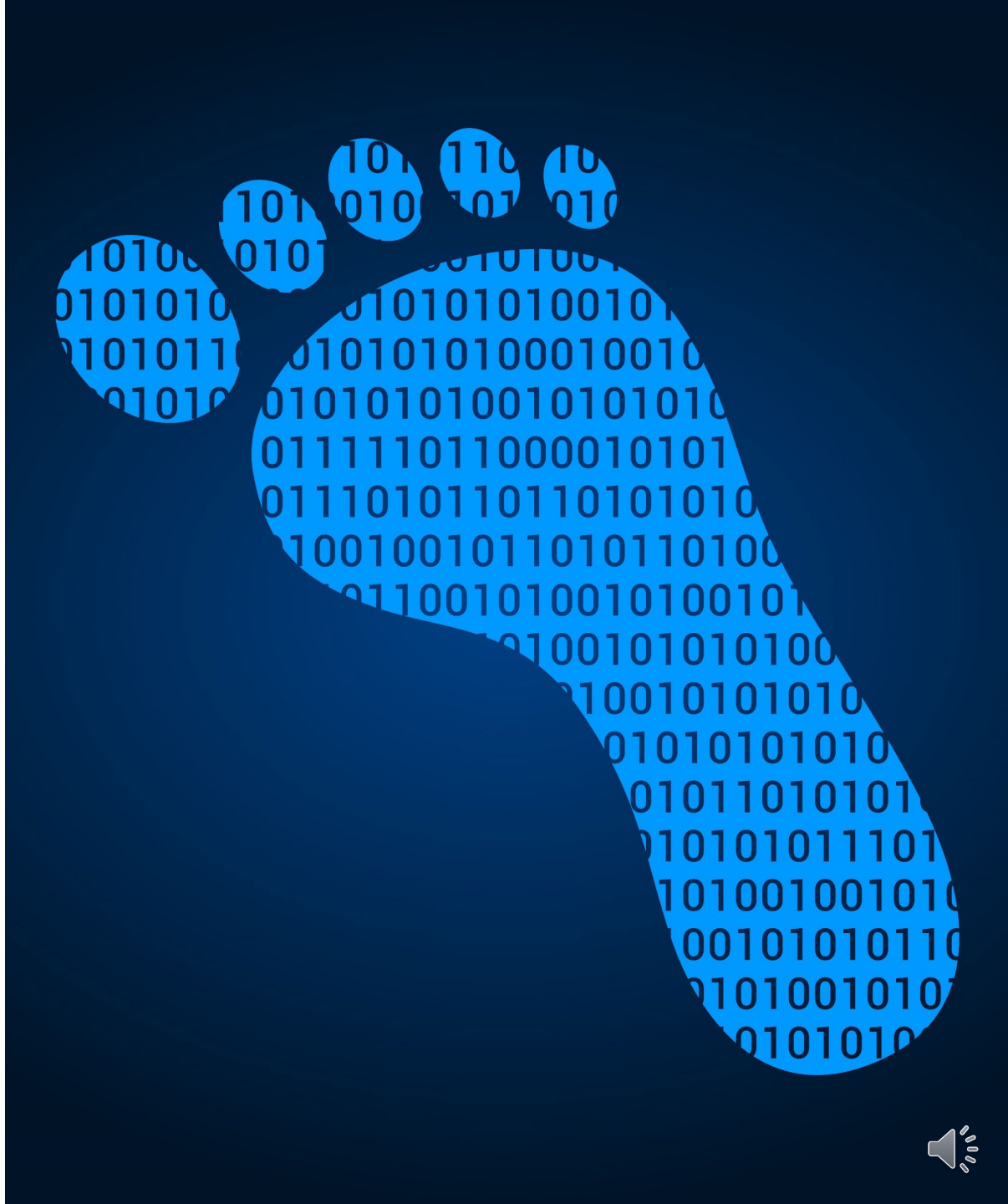
TikTok videos

Facebook posts

Email

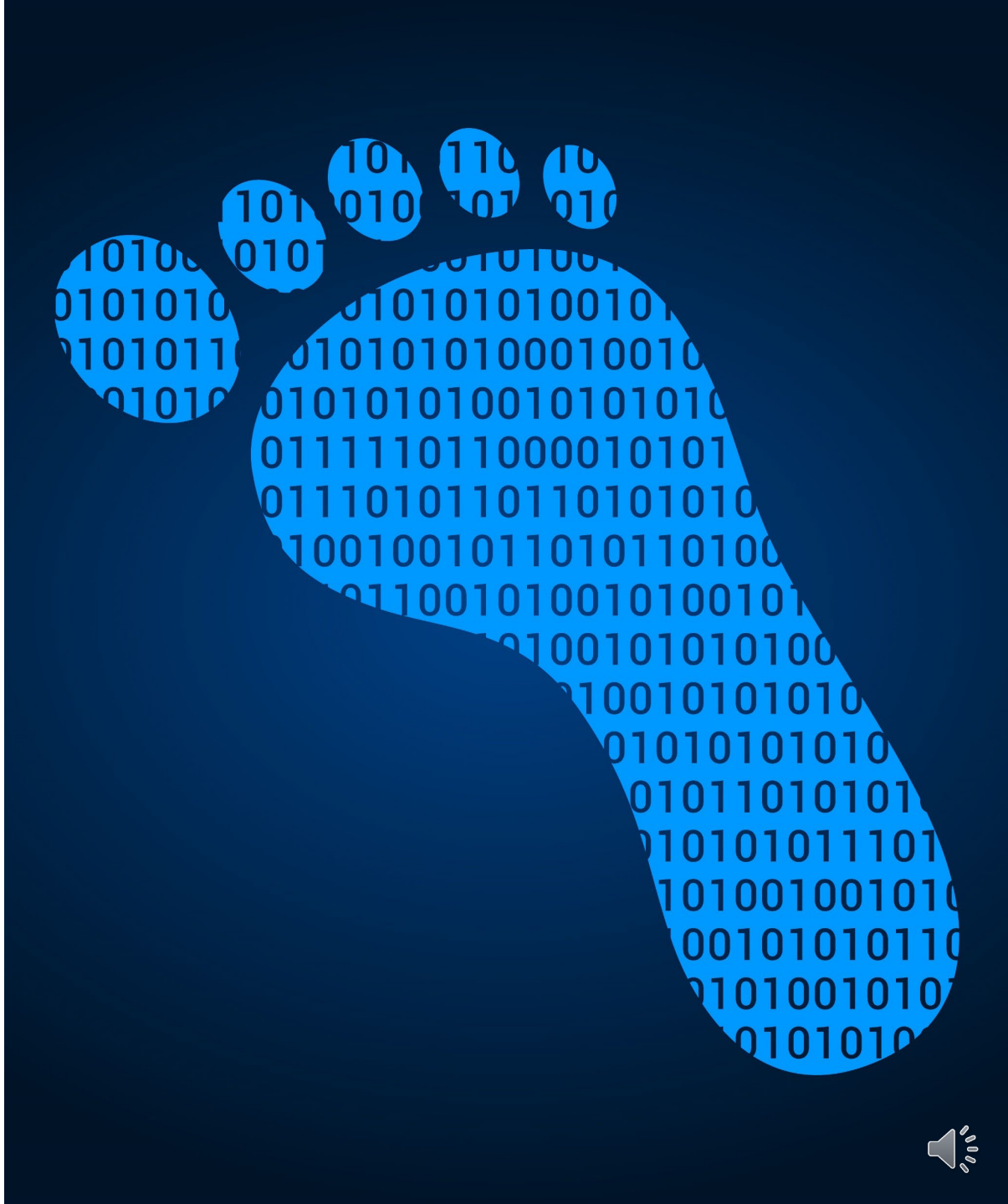
YouTube videos you make and upload

Any information that can be seen by other people (some who you don't know) or tracked in a database.



What is your Digital Footprint?

???



Digital Etiquette or "Netiquette"

Refers to electronic standards of conduct or procedures and has to do with the process of thinking about others when using digital devices. Being aware of others is an important idea whether we are together in person or online.

What Do You Share Online?

- Do they differ from the things you see others share online?
- Are you ever concerned about what you share or about what you see others sharing online?
- Have you ever regretted something you have shared online?

Share with care

It’s important to remember that you lose control once you post something, and it can be on the Internet forever.

Don’t take or share suggestive photos or videos

Did you know that anyone under the age of 18 who has sent a suggestive photo or video of themselves or friends—in a text or Facebook message, (also known as *sexting)*—runs the risk of being charged with breaking laws that prohibit the distribution of child pornography? And that anyone who gets the images may also violate laws which forbid *possessing* child pornography?

If convicted, they could face the same fate as adult pornographers—jail time as felons (with potentially long sentences), registration as a sexual offender, and so on.

Share with care

Make social network pages private

- Look in **Settings**, **Options**, or **Preferences** for ways to manage your privacy: who can see your profile or photos tagged with your name, how people can search for you, who can make comments, and how to block people.
- Some sites let you create separate friend lists—for family, your sports team or school club, your closest friends, and so on—so you can manage what you share with each group.
- From time to time, review your settings because these sites change what you can control (particularly in response to public pressure—Facebook is a perfect example)

Share with care

Keep personal info to yourself

No matter how private you make your pages, remember that whoever has access (your friends) can still forward what you post. You still need to use good judgment.

- Keep to yourself sensitive details that could be used to impersonate you, defraud you, or find you in person—your home address, phone and account numbers, age or birth date, even photos, especially suggestive ones. This also means creating profile pages on socials sites or in games that don't show such details.
- Don't post anything you'd ordinarily say only to a close friend, including feelings. Whether you're happy, sad, angry, or have money worries, confiding broadly could increase your risk of being bullied or targeted for scams.
- If you use a check-in service, pay attention to where and when you check in. Think about who will know where you are—a teacher, your parents? Will it harm your reputation?

Share with care

Be choosy about adding friends

- Consider friending only those you or your close friends have met in person, or with whom you have friends in common.
- Look at your friends list from time to time and make sure everyone who's there still belongs. Friends change over time.
- Review what others write about you.
- Make sure they don't post anything you don't want to share, like private photos, or tell where you are (like you're out of town on vacation with your family).
- It's okay to ask someone to remove information that you don't want to tell.

Share with care

- DO share your accomplishments

Post what you're proud of and want others to see—a recital video, academic successes, pictures from a school play, a persuasive essay, art you made, or music you performed.

Adding good material about yourself is also a way to push the negative stuff lower on your pages, like pictures you wish you hadn't posted or mean comments by others.

Share with care

- DO share your accomplishments

???

Why protect your online reputation?

- **40%** of college admissions officers visit applicants' social media pages
- **52%** of employers view a future employee's social media presence
- With so many eyes potentially judging you, do you think you need to clean up your digital footprint?

Why protect your online reputation?

???

Take charge of your online reputation

Take charge of your online reputation

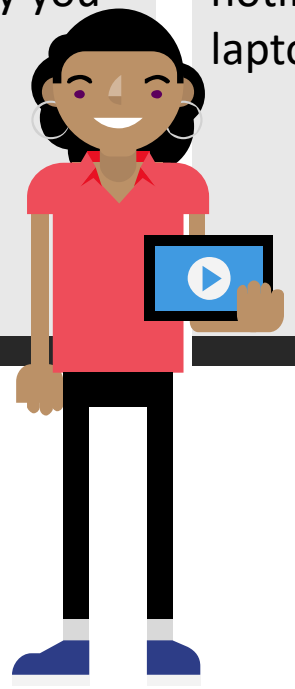
Discover	Evaluate	Protect	Cultivate	Restore
Discover what is on the Internet about you.	Evaluate the story that information tells.	Take steps to protect your reputation.	Cultivate your reputation.	Restore your online reputation.
Use multiple search engines and all variations of your name. Search for images as well as text. Review what others have posted about you in comments, pictures, or videos. Explore blogs, personal pages on social networks, and photosharing sites	Does it reflect the reputation you want to have? Is it accurate? If not, what should be deleted or corrected? Do you want your profiles to be public or more private?	Talk with friends about what you do and do not want shared. Ask them to remove anything you don't want disclosed. Periodically reassess who has access to your pages. It's okay to remove those who no longer belong in your circle.	Be proactive about sharing online the positive things you do. For example, link anything you publish to your name.	In a respectful way, ask the person who posted it to remove it or correct an error. If the person doesn't respond or refuses to help, ask the site administrator to remove the digital damage.

Take charge of your online reputation

Discover	Evaluate	Protect	Cultivate	Restore
		???		

Stay in control of your time and attention

Making smart choices regarding what you post on social media isn't the only smart choice you need to make when it comes to your digital footprint. You also need to think about how frequently you are connected.
It feels good when someone likes or comments on a post, and it is fun to keep up with your friends' activities.



Because of the positive feelings we experience when we see another like or get a message from a friend, it is tempting to turn on social media notifications for your phone or the apps on your laptop. No one wants to miss out, right?

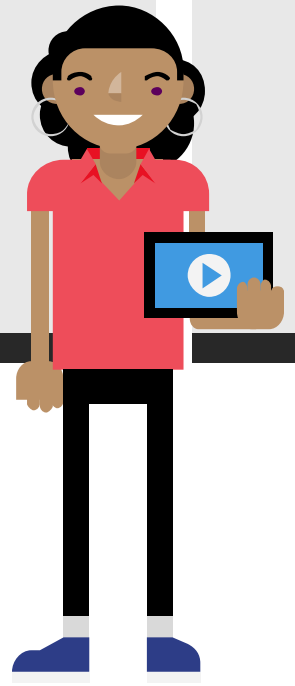
Stay in control of your time and attention

What's the concern?

Studies, however, indicate that the frequent notifications that come with email and social media apps can negatively impact your concentration and make you less efficient.

According to a poll by CivicScience, 43% of US Tech users NEVER unplug. Which means their phone is always on and always alerting them to the next like, comment, or post.

Such connection is too much, and over time will make you feel overwhelmed and exhausted. Additionally, these notifications impact your productivity by up to 40%!



Stay in control of your time and attention

???

From the Bear Creek Family Handbook

8.2.11 Internet Access and Computer Use Policy

Students are expected to use digital devices for educational purposes that serve the mission of The Bear Creek school, using good judgment when working in areas not covered explicitly in the Family Handbook. All members of the Bear Creek community are expected to contribute positively to our digital environment and to uphold the mission and values of The Bear Creek School.

- Users may use the Internet to visit educationally relevant material
- All users are expected to uphold our Core Values through all forms of communication, networking sites, discussion boards, texting, email communications, and Internet searching activities. Users may not visit, or attempt to visit, any site associated with pornographic materials.
- Students may only connect to the TBCS Guest Wireless Network.

This policy is included with Back-to-School Registration.

From the Bear Creek Family Handbook

8.2.12 Digital Citizenship and Care for School-Issued Devices

Upper School students will be issued Office 365 accounts and laptop devices. These accounts are used for educational purposes that serve the mission of The Bear Creek School, using good judgement when working in areas not covered explicitly in this Family Handbook. All members of the Bear Creek community are expected to contribute positively to our digital environment and to uphold the mission and values of The Bear Creek School.

Student safety is a primary concern for all of us.

From the Bear Creek Family Handbook

8.2.12 Digital Citizenship and Care for School-Issued Devices

The following behaviors apply to our codes of conduct articulated in this handbook whether students are working at home or school:

- Students agree to use these accounts only for school-related purposes.
- Students agree not to record images or video of Bear Creek teachers or class materials or share such items with those outside our school community.
- Using any accounts or digital device to engage in harassment, bullying, stealing intellectual work, storing inappropriate materials, distracting yourself or others in class, or breaking any other such rule will result in disciplinary action. This includes recording and/or taking screenshots of teachers or other students without their consent.
- Using these accounts or any digital device for non-academic purposes during class is not permitted unless your current instructor specifically permits it for a class-related activity.

From the Bear Creek Family Handbook

8.2.12 Digital Citizenship and Care for School-Issued Devices

Students should pay careful attention to the following:

- Keep your passwords secure.
- Do not use your device to access other people's accounts, computers, or folders, nor borrow computers or computer accessories without the express permission from the owner.
- Bring your fully charged device and pen to school daily
- Protect your device with an attached protective cover.
- Label your charger and your pen so you can identify it as your own.
- Respect copyright law by only using licensed software, audio, and visual materials.
- Check your Bear Creek student email account daily.
- Respect the power of distraction that your digital devices hold and make a conscious effort to limit distractions.
- Respect the installed technology in each classroom, only mirroring your device to a screen when permitted and displaying the appropriate content for the activity at hand.
- Lock up your device when it is not in your possession.
- Keep track of your pen and other accessories.

From the Bear Creek Family Handbook

???

Communicating with Teachers

You are likely to communicate regularly with your teachers either via email or perhaps in a Teams Chat. You may need to notify a teacher of a class you'll miss due to athletics or illness. Your teachers may have different ways they want you to communicate with them about missing class or missing assignments in their class. Remember this:

- Give your teachers as much advanced notice as possible for a planned absence.
- Be respectful in your tone as you communicate via Teams Chat. A Teams Chat with your teacher shouldn't look like a text to a good friend full of abbreviations and casual tone. It should be brief and professional.
- Be respectful of the time of day when you communicate. Your teacher may be teaching class and will get back to you when she can. You may have a question at 9 PM that you wish your teacher would answer—but he may already be sleeping and won't see your message until the next morning.

Congratulations!

You've completed the training. You're ready to take good care of your new school issued device…and be a good digital citizen!