

Creative Guide for Teachers & Parents

Introduction

If you have young people in your life – your own children, students, nieces or nephews or team members – then this guide is for you. Because if they aren't online in some capacity already, then chances are they will be soon and will need guidance on how to protect their personal privacy.

Young people are more in need of this information than ever before, as more and more gadgets and toys offer the option of going online – even traditional stuffed animals now come with codes that allow kids to register online and play with other kids! And young people are embracing this technology, going online to connect with friends and make new ones, to buy products, listen to music, watch videos, play games, learn – the list could go on and on.

According to the Media Awareness Network, 37 per cent of young Canadians have their own Internet-connected computer. Twenty per cent of grade four students access the Internet through their own personal computer – that number climbs to 51 per cent by grade 11. Since young people are so enthusiastic about technology, it's only fair that we take the time to teach them about proper "netiquette". The following information is intended as a guide to address important data privacy issues that relate especially to youth. Each section starts with an important privacy issue and then offers ideas for generating discussion about that issue with your young people.

The videos and other resources mentioned in this guide are links so you can connect directly to them whenever you like. They are also listed at the end so you can easily access them if you choose to print the guide out. We also include links to other youth privacy sites that are sprouting up from all over the world, including Norway, Australia and Hong Kong. The Internet makes it easy for people to connect and chat, no matter where they live, and privacy is something that young people all around the world are thinking about.

SUBJECT & DISCUSSION IDEA #1

Think before you click!

Online services and applications can create wonderful opportunities for creativity, networking, social engagement and learning. Online, you can research the most mundane or exotic of topics, connect with friends all around the world, watch videos, play games – the sky is the limit.

If you remember one thing about online activities, remember this: online, everything is public and it's permanent. The web is exactly that – a spider web with connections going off in a million different directions. Once you post a comment or a picture, you have no control over who copies that information or who they send it to. Do you have friends on your social networking sites? Do they have friends and so on and so on? Once something is on the Internet it can go anywhere and be sent to anyone.

Information that you post online is also very difficult, almost impossible, to delete. Once it's there it can be copied, and it also exists in computers' caches and archives. So you need to be careful about what you post – think about what you're putting up there and ask yourself: will I be comfortable in five years, or 10, with that information being online?

The key is: think before you click! Make sure you are comfortable with what you are posting before you post it.

Discussion idea:

Have you posted anything online that you wouldn't want your parents or teachers to see? How about a new crush – would you want that person to see everything you have posted? If you're uncomfortable with anything you've put up there, remove it, and then think before you click in the future.

Think about your friends when you are posting, too. Have you ever posted a photo or other information that one of your friends may not want online for everyone to see? Are you careful to monitor what your friends are posting about you?

SUBJECT & DISCUSSION IDEA #2

Do you pay attention to privacy settings?

Did you know that there are over 350,000,000 active users on Facebook, who check their accounts at least once a week? Did you know that if your Facebook profile is “open” every one of those users can see everything you post on your page?

In 2009, MySpace announced that it had kicked 90,000 registered sex offenders off of their site – registered means they’ve been caught. How many registered sex offenders do you think may be on other social networking sites? Perhaps more importantly, how many creepy people are using these sites who haven’t been caught for their actions?

If you have an open profile on any social networking site, it’s a good idea to go into the privacy settings and mark it “closed” – that way only the friends on your list can see the details of your profile. The privacy settings give you lots of options – you can even limit what different friends see – for example, you can adjust the settings so that only good friends can see everything and you can limit the information that casual acquaintances see. Do you have friends on your list who you don’t know at all? Check out Subject and Discussion Idea #3!

Discussion idea:

John carefully chooses who he allows on his “friends” list on his favourite social networking site, but he’s never looked at the privacy settings. The default is an “open” profile, so his profile is open for everyone who uses that social networking tool. Discuss what this means.

SUBJECT & DISCUSSION IDEA #3

Do you know who your friends are?

It's not unheard of for people to join social networking sites like Facebook and Bebo and create a profile for themselves, only to discover that someone has already created one. It's just one way fraudsters are using the Internet for hurtful purposes.

If a real-life friend asks you to be a friend online, the simplest way to make sure that friend is who they say they are is to ask them in person. The next time you see that person, make a point of mentioning his or her profile. Chances are, your real-life friend is your online friend. But it never hurts to ask – you never know, you could be doing your friend a favour.

Be cautious – online you really can't be 100 per cent sure of who you're talking to. So, if your online friends have little or no connection to you in the real world, always use caution. The more real-world connections you have with an online friend, the more confident you can be in sharing information with that person. So, while you can be confident in sharing your vacation photos online with your real-life best friend, you might want to think twice about sending those photos to the friend you made at tennis camp last summer, or the friend you met through another friend while chatting online.

Discussion idea:

How can you make sure your friends are who they say they are? Be a sleuth. Talk about how you can investigate your friends' profiles. Does one of your friends have two brothers – but, online, she only mentions one? Could this be a fake profile? This exercise could help you weed out some fakes – or maybe you'll simply learn a few things you never knew before, like how much one of your friends loves cheese fries and old video games!

SUBJECT & DISCUSSION IDEA #4

Pick and protect the perfect password

Your information is only as safe as your password. Without a strong password your online information is vulnerable to being accessed by others.

The perfect password should:

- Be **strong** (8 characters or more is recommended). The more characters you use, the stronger your password will be.
- Use a **variety** of characters. Using a combination of letters, numbers and symbols makes the password more complex and therefore harder to guess.
- Be **changed** regularly to reduce the likelihood of someone accessing your personal information.

Typical password mistakes include:

- Using **sequences** or repeated characters. This makes it easier for others to guess the password.
- Using **personal information**, such as any part of your name, birthday, social security number, or similar information about your loved ones.
- Using the **same** password for many different systems.
- **Revealing** your password to others, for any reason.
- Typing passwords on computers that you do not control or own because others may be able to extract your password from that computer after you use them.

Discussion idea:

Katie is really excited when she receives a mobile phone for her 14th birthday. She is required to choose a password and chooses 141414. She gives all her friends the password so they can use the phone too. When she gets home she changes her computer password to 141414 as well, so she won't confuse the two passwords in the future. Discuss Katie's choice of a password, her decision to give the password to her friends and her decision to make her computer and phone password the same.

SUBJECT & DISCUSSION IDEA #5

Keep your personal information private – and protect your identity

Are you at risk for identity theft? Here are some important questions to ask yourself:

- 1) Do you carry your Social Insurance Number in your wallet?
- 2) Do you throw your balance statements and receipts in the garbage?
- 3) Have you revealed your PIN to your friends?
- 4) Do you choose passwords that are common and easy to guess?

If you responded “yes” to any of these questions you are in danger of being the victim of identity theft!

Some statistics involving identity theft from a recent survey:¹

- 1.7 million Canadians were affected by identity theft in 2008
- While more than 45% of cases of identity theft involve Internet use, most identity thieves don’t use cyberspace to acquire information.
- 40% of offenders are women – this may be attributed to the absence of violence and the possibility of committing the crime without help from an accomplice.
- The average age of an identity thief is 33 years.
- 64.6% of the offenders acted alone in the majority of cases.
- 53.4% of incidents involve the theft of wallets and purses, and fraud.

It turns out that many people choose to steal identities simply because it’s easy. Identity theft has one of the fastest growing crime rates seen in recent years.

Discussion idea:

Students from John F. Ross CVI in Guelph sent in a video for our 2008 video contest entitled “ It’s Your Life...And Your Privacy” which takes the viewer through the mindset of an Identity thief and how easy it is to be tricked into giving out information over the Internet. See the video, which won third-place in the 2008 contest [here](#). Discuss the video and the facts about identity theft with your young people.

¹ Statistics from Benoît Dupont and Guillaume Louis’s second report (“Identity thieves: a common delinquency profile”) from the Université de Montréal’s Canada Research Chair in Security, Identity and Technology.

SUBJECT & DISCUSSION IDEA #6

Be careful on online gaming sites

What kind of online gaming sites are you aware of?

Although online games can be fun and entertaining, your identity and personal information can be compromised if you don't exercise caution.

Online game sites have become a growing area for people to access personal information. If the wrong person obtains information about you from the profiles you create in games, they could use it to establish accounts in your name, resell it, or use it to access your existing financial accounts.

When on gaming sites:

- Be aware of having your computer in "administrator" mode. With some games, your computer will be switched to that setting automatically. This is a problem because a hacker can gain full control of your computer at the administrator level.

One way to avoid this problem is by web browsing from a "user" account – while this won't completely safeguard your computer it is safer than using administrator mode.

When gaming, it's also important to remember that **firewalls** are in place to help protect your computer. Playing a multiplayer game sometimes requires an exception in the rule set for the firewall. A firewall is there to protect your computer from viruses. By removing it you are making you and your information extremely vulnerable.

Discussion idea:

Think about the profiles you have created for yourself in some of the online games that you play. Have you used your full name? Your date of birth? Your address or any other personal information that might be valuable to the wrong people? Think about the people you play games with – are some of them people you don't know in real life? If one of those people was a hacker would you want them to have access to all the information you've included in your profile?

SUBJECT & DISCUSSION IDEA #7

Be wary of e-mail or instant messages from unknown people

Are you familiar with the term “phishing”? It is the criminal attempt to gain access to private or sensitive data, like Internet passwords and credit card numbers, by someone posing to be a trustworthy and legitimate organization online. These attempts are frequently made through e-mails or instant messaging.

Social networking sites have become a target for phishing. Many criminals will:

- create a website that looks identical to the homepage of a social networking site to get you to enter your username and password.
- use the information they receive to hack your account and gain access to all of your information.
- set up a link in a message within the internal messaging system of the social networking site itself.

What you can do:

- **Don't respond** to an e-mail asking for personal banking information. Authentic companies will not ask their clients for usernames or passwords via e-mail.
- Exercise **caution** with e-mails and personal messages. If you don't know the sender, try to find out if they are legitimate before you respond.
- **Protect** your computer with spam-filters and anti-virus software, and make sure your firewalls are turned on.
- Be **cautious** and critical of messages from people you don't know and trust. Never enter personal information online unless you are 100% sure that the website is legitimate and authentic. If you are not sure, it's a good idea to ask an adult for help.

Discussion idea:

Amy recently opened a bank account at her local mall. One day, she receives an e-mail from that institution – they want her to verify her passwords, online. Would a bank ask a customer to verify passwords this way? If the e-mail looks like it comes from the bank (it's got all the right logos and colours, etc., and is signed by the bank president) what should Amy do? What might happen if she responds and verifies her passwords online?

SUBJECT & DISCUSSION IDEA #8

Parents on Facebook

Are **YOUR** parents on Facebook?

It doesn't matter who it is – your parents, colleagues, employer or coach. If you're putting information online it is public and permanent and there is a real possibility that almost anyone can see it. If you aren't comfortable with certain photos or information being seen by everyone then you should probably not post them online. Screen what you upload. Think before you click and avoid any uneasiness!

But what if you are careful about what you post and you're still uncomfortable with having your parents as friends on Facebook? Maybe they constantly write messages on your wall and comment on everything you do. This could be more incentive for you to get more comfortable with the privacy settings. Is it possible to give them limited access? If you want to commiserate with other teens who are in the same boat, check out [Oh Crap. My Parents Joined Facebook](#). The site was created by two twenty-something girls who discuss and give examples of the parent-child relationship on Facebook.

Discussion idea:

A Norwegian [website](#) dealing with youth privacy has videos which show kids how easy it is for others to find out what they have been doing on the Internet. This scenario takes place at a student- teacher conference where the teacher is discussing what she discovered after simply googling the students work.

SUBJECT & DISCUSSION IDEA #9

iPhone and other Applications

How many of you have a cellphone? And how many of those cell phones have Internet capabilities? With phones like the iPhone and Blackberry, you can even download applications that do really cool stuff such as recommend restaurants, provide movie show times, and much more.

What you may not know about these “apps” is that with some of them, your location data is being broadcast across your cellular data network. While it is believed these servers are secure, there is really no way of knowing who has access to your location information.

It’s important to play it safe with these applications, and to make sure you know what you’re getting into. If you don’t know if your information is being broadcast through an app or not, find out!

Discussion idea:

Have you or any of your friends used a GPS-enabled cell phone to track someone’s whereabouts or to broadcast your own location? Location information is very sensitive and if you allow a dangerous adult to have access to your location, you could be at risk.

SUBJECT & DISCUSSION IDEA #10

Online Dating sites

Dating is tricky no matter HOW old you are, and it can be very difficult. That's why some people decide to engage in online dating. If you choose to do this, you've got to keep in mind that the Internet is:

- completely anonymous, and there is no way of really knowing who you are speaking to when you are online.

Here are some important tips that you should always keep in mind when engaging in online dating:

- **Listen** to your instincts. If something doesn't feel right about a person, or you get a "creepy" vibe, just stop contact.
- **Be careful** when giving out your personal information.
- It is a good idea to set up an **anonymous** email account if you wish to extend contact beyond the online dating community. This way, your personal and identifying information is kept anonymous and you'll have a much easier time stopping contact if you need to.
- If you choose to take the online into the real world, **NEVER** meet the person alone. If you are under 18 years of age, ask your parents before meeting with anybody you met online. Always remember: the person may not be who s/he says s/he is.

Discussion idea:

The youth privacy website from [Norway](#) illustrates how a young person could be having online dating conversations with someone who is not who they think they are. The scenario poses the question "Did you fall in love with your little brother?"

SUBJECT & DISCUSSION IDEA #11

Sexting

The Pew Research Center has published a [research paper](#) surrounding this topic which has shown that 4% of youths aged 12-17 have sent a sext message, and 15% have received a sext.

It is important to keep in mind that:

- Everything you put on the Internet is **public** and **permanent**. Once a picture is sent there is the risk that it can be made **public**.
- Once something is posted on the Internet it can leave a mark on your **record** which can be seen by peers, family and future employers.
- Nude pictures of anyone under the age of 18 are considered to be **child pornography**. Those who take these pictures, even if you took them of yourself, are subject to the law. Also, the people who receive the pictures can be charged with possession of child pornography.

It is also important to think about the **consequences** that your actions will have. A private photograph sent via cell phones can so easily cause terrible humiliation.

Questions to ask yourself before posting photos on the Internet:

- Who could find your online pictures/video of you? Your parents? Friends? Family? Teachers?
- If they found these pictures/videos, would you be embarrassed?
- If you're not embarrassed now do you think you might be 5 or 10 years from now?
- What could someone do with your pictures, video, or personal information?
- What would you do if people at school got a hold of the pictures/video?
- How much do you want people to know about you?

Discussion idea:

The Norwegian [web site](#) for youth privacy produced a video on sexting. It involves two teenagers discussing a picture's ability to humiliate an individual on the Internet. It then shows a revealing picture being uploaded for all to see online.

SUBJECT & DISCUSSION IDEA #12

Cyberbullying

What is cyberbullying?

Cyber bullying is very different from other forms of bullying, which involve face-to-face contact. With cyberbullying, the bully employs the use of technology (such as cell phones or the Internet) to intentionally hurt or harass another person. A 2008 survey indicates that nearly one in five students have been bullied online.

This type of bullying can lead to:

- Depression
- Isolation
- Eating disorders
- Suicide

The bully can be severely punished with the police becoming involved. If you or one of your friends is a victim of cyber bullying, the [Media Awareness Network](#) recommends following these four steps:

- STOP- immediately leave the online environment or activity where bullying is going on.
- BLOCK e-mails or instant messages received from bullies. NEVER RESPOND.
- RECORD all harassing messages and send them to your Internet provider (Yahoo, Hotmail, etc.). Most providers have policies about users harassing people on their server.
- TALK to a trusted adult about the cyber bullying; alert the police when bullying involves physical threats.

It is important to come forward with instances of cyber bullying so that the bully does not continue to harass the victim.

Discussion idea:

Cyberbullying has happened to many people all over the world. There have been incidents involving MySpace and Facebook where users created fake profiles to harass other users. Fake websites have also been created with hurtful and demeaning content. Discuss the differences between traditional bullying and cyberbullying and how online tools can make the whole issue so much worse.

Resources mentioned in the text (in order of mention):

Video: “It’s Your Life... And Your Privacy” (students from John F. Ross CVI in Guelph, third-place winner in youthprivacy.ca 2008 video contest). Link: <http://www.youthprivacy.ca/en/contest.html>

Web site: Oh Crap. My Parents Joined Facebook. Link: <http://myparentsjoinedfacebook.com/>

Video: “The parent-teacher-student conference went OK... but all hell broke loose when the teacher googled my work!” (From Norway youth privacy site). Link: <http://www.dubestemmer.no/The+parent-teacher-student+conference+went+ok...9UFRnU4L.ips>

Video: “Did you fall in love with your LITTLE BROTHER?” (From Norway youth privacy site). Link: <http://www.dubestemmer.no/Did+you+fall+in+love+with+your+LITTLE+BROTHER%3F.9UFRzSWw.ips>

Research paper: “Teens and Sexting” (Pew Research Center). Link: <http://pewresearch.org/assets/pdf/teens-and-sexting.pdf>

Video: “It was just a joke... but suddenly I had pressed “Enter”!” (From Norway youth privacy site). Link: <http://www.dubestemmer.no/It+was+just+a+joke...9UFRnWWg.ips>

Cyberbullying resources: Media Awareness Network. Link: http://www.media-awareness.ca/english/tools/main_search/search_results.cfm

Other useful links:

Australia’s youth privacy web site. Link: <http://www.privacy.gov.au/topics/youth>

Hong Kong’s youth privacy web site. Link: http://www.youth.gov.hk/en/info_centre/civic/600E.htm

Norway’s youth privacy web site. Cool ways for students (and teachers) to learn how to “think more deeply about the relationship between privacy, anonymity and identity in a networked world”. Link: <http://www.dubestemmer.no/en/>

The Media Awareness Network. Cool stuff about media and information literacy. Link: <http://www.media-awareness.ca/english/index.cfm>

In Your I. Link: <http://www.idtrail.org/InYourI/>

Office of the Privacy Commissioner of Canada. Geared for adults, with tonnes of information about privacy and your rights. Link: <http://www.priv.gc.ca/>