Institute for Responsible Online and Cell-Phone Communication

Introducing Digital Responsibility to a Digital Generation

www.IROC2.org

DEVELOPING DIGITAL CONSCIOUSNESS™

Tips & Tools to Prevent Digital Issues & Promote Responsible Use

PUBLIC & PERMANENT™

THE 21ST CENTURY GOLDEN RULE

For More Information about

THE COURSE TO DIGITAL CONSCIOUSNESS™

Please visit www.IROC2.org

TOP 50 CHAT ACRONYMS PARENTS NEED TO KNOW

8 - it means ate, it also refers to oral sex
1337 - Elite -or- leet -or- L337
143 - I love you
182 - I hate you
1174 - Nude club
420 - Marijuana
459 - I love you
ADR - Address
AEAP - As Early As Possible
ALAP - As Late As Possible
ASL - Age/Sex/Location
CD9 - Code 9 - it means parents are around
C-P - Sleepy
F2F - Face-to-Face, a.k.a. face time
GNOC - Get Naked On Cam
GYPO - Get Your Pants Off
HAK - Hugs And Kisses
ILU - I Love You
IWSN - I Want Sex Now
J/O - Jerking Off
KOTL - Kiss On The Lips
KFY -or- K4Y - Kiss For You
KPC - Keeping Parents Clueless
LMIRL - Let's Meet In Real Life
MOOS - Member Of The Opposite Sex
MOSS - Member(s) Of The Same Sex
MorF - Male or Female
MOS - Mom Over Shoulder
MPFB - My Personal F*** Buddy
NALOPKT - Not A Lot Of People Know That

NIFOC - Nude In Front Of The Computer
NMU - Not Much, You?
P911 - Parent Alert
PAL - Parents Are Listening -or- Peace And Love
PAW - Parents Are Watching
PIR - Parent In Room
POS - Parent Over Shoulder -or- Piece Of Sh**
pron - porn
Q2C - Quick To Cum
RU/18 - Are You Over 18?
RUMORF - Are You Male OR Female?
RUH - Are You Horny?
S2R - Send To Receive
SorG - Straight or Gay
TDTM - Talk Dirty To Me
WTF - What The F***
WUF - Where You From
WYCM - Will You Call Me?
WYRN - What's Your Real Name?
zerg - To gang up on someone

Parents & Educators

Now is not the time to be coy, shy, timid, or indirect with your kids and students. Every time they use Digital Technology, they open themselves up to the world, and the risks that we all inherit once we power up!

Here are a few tips that we strongly recommend:

1: Talk candidly and openly with your kids and students about what they are doing online or with their mobile device before it's too late!

2: Try your best to know who your kids and students are communicating with and what apps and tools your kids are using.

3: Maintain constant communication about expectations of responsible use, and offer constant reinforcement about the importance of maintaining a mindset of Public and Permanent™ while they are operating powerful tools that connect them to the world.

4: Try to be aware of what your kids or students are posting online. Do they have a My Space or Facebook account? If so, ask them to see their page. If they say no, ask them why. Explain to them that anything they are posting online should be something that they should be ok with you seeing as well as the rest of the world because nothing is truly private online.

The preceding is a message from the Institute for Responsible Online and Cell-Phone Communication's Safety Lab.
To Schedule a Program for Your Community, Contact the Speakers Bureau at helpdesk@iroc2.org

5: If you have not already, we also strongly suggest contacting our Speakers Bureau about putting together a seminar for your school or community. You can reach them via email at helpdesk@iroc2.org.

- Teachers: Prohibit [unauthorized] personal mobile device use in the classroom, and talk to your IT administrator about filtering websites reachable through school computers and your online service.

- Parents: If you are trying to limit or block unauthorized web browsing, turn your internet access off from the router, or clearly set rules about time limits the time in which your child is allowed to spend on the internet per day.

- Parents: Based on your preferences, set a time for your kids to "turn in" their mobile devices for the day. You are the parent and you can set limits on the time of day the devices may be used.

Did You Know?

There has been a lot of talk about "Sexting", but you don't have to send or "Sext" somebody a picture, video or text message for it to become public to the world online, and you don't have to be a teen to "Sext".

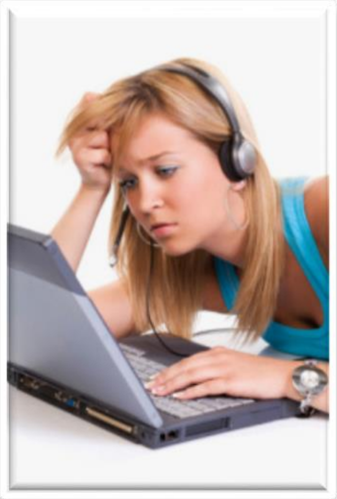
Myth: Deleting a picture or video from your web page deletes it forever.
Myth: Deleting a picture or video from your digital camera or phone deletes it forever.
Myth: Simply deleting a picture or video from your computer deletes it forever.
Myth: Nobody else can ever gain access to your private webpage.
Myth: Broadcasting from your webcam is always private and never being recorded.
Myth: Your actions while using the internet, cell phones and other digital technologies has no effect on anyone else including your friends and family.

TRUE: If you apply a Digital Consciousness™ – a mindset of Public and Permanent™ - when using the internet, cell phones, apps, social media, interactive gaming, and any other digital tools & technologies, you eliminate any potential for self-inflicted challenges and reduce your risk of facing devastating and sometimes life altering consequences that often accompany the abuse of powerful digital tools.

YOU!

Hey You......Yeah You!

Whether you are 10 years old, 100 years old, or somewhere in between, here are a few things to think about before using the internet, cell phone or other digital technology:



1: Don't assume anything that you send or post or even save on your phone or computer is going to remain private!

2: Do NOT ever give into pressure to do something that makes you uncomfortable, especially if it involves the internet or digital technologies.

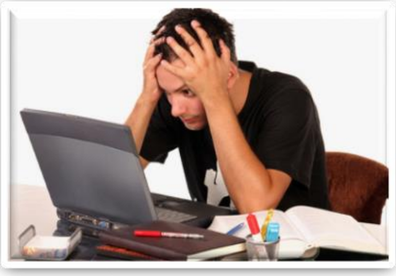
3: Consider the reaction of the person you are sending a "private" (or any) message to. Are they expecting it? How will they receive it? Are they going to share it with someone else?

4: Nothing online is truly anonymous, private or secret. **NOTHING!**

5: There is no going back, changing your mind, cleaning the slate in a digital world. In other words, anything that you send or post today will never truly go away or be deleted.

AND FINALLY...REMEMBER

YOU CANNOT UNPLUG THE INTERNET!!!



.

The preceding is a message from the Institute for Responsible Online and Cell-Phone Communication’s Safety Lab.
To Schedule a Program for Your Community, Contact the Speakers Bureau at helpdesk@iroc2.org

OBTAINING SECURITY ASSISTANCE

Step 1: Visit Google Play the App Store and search for "security", or visit a trusted software review site. We like www.cnet.com which is used for the following process description.

Step 2: Once at Cnet.com, select the "Downloads" tab under the Search Bar.

Step 3: Select Your Preferred Operating System or Device (Windows, Mac, Mobile, etc).

Step 4: Search for the keyword, anti spyware in the search box.

Step 5: Prior to reviewing the list of search results, utilize the drop down menu titled, "Sort By", and select "Editors Rating".

Step 6: Scroll down until you see search results with red star ratings. The red stars indicate an Editor's rating. It is these

Step 7: Select a variety of free programs you wish to try on your machine.

Step 8: Repeat the aforementioned steps using the search term, security, and any others you find relevant to your antivirus & anti spyware requirements.

Note: *Please proceed at your own risk. The aforementioned information is provided to offer assistance; however, IROC2 shall be in no way liable to you for any usage or damages caused by the 3rd party websites and / or programs downloaded by you, or anyone else to your digital device(s).*

Institute for Responsible Online and Cell-Phone Communication

Introducing Digital Responsibility to a Digital Generation

Guidance for Preventing Cyber Cruelty

Note: While victims need support, it is important to focus on the bully!
Preventing an incident = less victims

7 Things to Consider Before Bullying

1) There is no winner in a “Bully” or “Cruelty” Situation, but at the end of the day, it is the Bully, NOT the victim, that harms their reputation and future.

2) You never know what the person you are being cruel to. Or their friends and family members are capable of. *(Reference Link 1)*

3) The hate you share on a global public platform today could become part of your legacy for future generations to see and know about you! *(Reference Link 2)*

4) To friends and family, you may be terrific, but to a billion other people, you just look like a jerk -

5) Employers, educational facilities, awards panels, relatives, etc. may not like what they see during a background check or research

6) You are about to hand your victim information that can destroy your reputation and future

7) You are NOT anonymous! *(Reference Link 3)*

Link 1 - **MAN GETS KILLED OVER A TWITTER BEEF GONE WRONG!**

Link 2 - **2 Florida teens charged with felony over cyberbullying incident**

Link 3 - **The case that could end cyberbullying**

Are You A Victim of Bullying?

1) Print, copy and save everything being said or created

2) Do NOT respond or provoke the bully

3) Report the incident accordingly whether it be to a parent, teacher, law enforcement or school / community threat assessment program (e.g. http://www.tipsprevent.com/IROC2).

The following information has been extrapolated with permission from the book,
"Creating a Mindset That Our Digital Actions Are Public and Permanent."

Thoughts to Review and Discuss About Cyber Bullies

A Digital Consciousness for Cyber Bullies: If you or anyone you know is about to use digital technology to spew hatred across the World Wide Web, please consider and communicate these thoughts:

- Think about this for a moment: The individual or group being harassed will have digital proof that you are not exactly a "stand up" individual. Quite frankly, the instant your victim (and the world) receive your harassing note, is the instant you give everyone power over you! Your victim may now take it upon themselves to save and send the email, picture, video or file to just about anyone they want, including an employer, a principal, a parent, to anyone who will cause you grief.

- The message (ammunition) you provide your victim is not going to go away, so anything your victim has in their possession from you, they will be able to hold over your head as leverage. They could potentially affect your reputation, scholastic career or employment as all they have to do is "show off" what you did to them. What's more, so too can a C.E.L disrupt your future through blackmail should they obtain your digital blunder and threaten to use it against you.

- Before you draft and send anything malicious using a digital tool, stop and think about what your family, friends, employers or future relatives might think when they are presented with the "cowardly hate" you are about to communicate over a digital platform because you did not have the backbone to approach your adversary offline and peacefully.

- What you write today will be [digitally] available forever. Do you want your kids and grandkids to know what you are about to write? Do you want your "hate" to be part of your digital legacy? Do you want your hate to be what shows up on a page about you that your kids or grand kids search for on sites like Spokeo.com or Ancestry.com in years to come?

- Do not assume any sort of privacy when harassing someone via digital technology. A "bully" does not warrant any privacy or protection based on the malicious actions they are employing and if a "bully" is investigated (proxy or not) they will be found, just as we would all want a terrorist to be found should they be plotting against our country.

- To your family and friends, you may be the greatest thing since sliced bread, but to a billion other people, you are going to look like a jerk. When you harass someone over a global public platform known as the World Wide Web, you do not just "bully" the victim, you bully the world, and you never know who will take exception to your remarks. You never know when your victim’s friend or relative could turn out to be the next Eric Harris and Dylan Klebold (the shooters behind Columbine) or the next Charles Manson or Ted Bundy (serial killers). Hurtful remarks may just move bullies to the head of a “kill list” – and it is not that hard to find anyone through the Internet.

Discussion Questions:

1) Do you know anyone who has been bullied through digital technology?

2) Think about a time when you have been really frustrated at someone. Maybe it was a boss, or a friend, or someone that just cut you off on the road:

- If you had no digital technology and no Internet, how would you handle it?

- Would you ever take time out of your day to call everyone in your town or the world to vent about what just happened?

3) What are some of the things that bullying others can stop us from obtaining / achieving (i.e. a job)? List some examples.

4) How can we most effectively communicate to potential bullies, why it is a bad idea to “bully?”

Find more information for Bullies and Victims of Bullying in the book, “Creating a Mindset That Our Digital Actions Are Public and Permanent.”

Institute for Responsible Online and Cell-Phone Communication

Introducing Digital Responsibility to a Digital Generation

Phone: (877) 295-2005 **Fax:** (240) 363-0070 **Address:** P.O. Box 1131 200 Walt Whitman Ave. Mount Laurel, NJ 08054-9998 **Website:** www.iroc2.org

DECLARATION OF DIGITAL CITIZENSHIP

Becoming an informed and responsible citizen in our global village is a vital developmental task necessary for anyone utilizing and relying on evolving digital tools and technologies. Obtaining a uniform social guideline based on accurate knowledge, and then knowing how to apply it appropriately – achieving a digital consciousness™ – requires the integration of psychological, societal, cultural, educational, economic and spiritual elements.

Digital consciousness encompasses accurate education about the power of digital technologies and positive judgment while utilizing these technologies, as well as the ability to develop and maintain meaningful relationships; appreciate one's own self worth; interact with individuals of any age, culture and sex in respectful and appropriate ways; and express emotions in ways consistent with one's own values.

We can encourage digital consciousness in ourselves and others by:

- Obtaining and communicating *accurate* information and education about the responsible use of digital technologies;
- clearly outlining the consequences that stem from the abuse of digital technology;
- clearly illustrating that we are all now digital citizens existing in one global community or "global village;"
- offering digital citizens support and guidance to explore and affirm their own values;
- modeling healthy emotions, attitudes and behaviors when digitally interacting with others; and
- fostering and applying informed, responsible and preventative decision-making skills to all digital decision making

Society can enhance the communication and practice of 21st century digital safety, responsibility and awareness (2.1C) by providing access to comprehensive and *accurate* education and giving anyone of any demographic opportunities to receive that information.

Families, media, schools and universities, youth groups, community agencies, religious institutions, digital technology manufacturers and other businesses, and government at all levels have important roles to play to ensure all citizens in the global neighborhood have knowledge to understand and apply a uniform and necessary guideline to promote good digital citizenship and prevent social issues stemming from the abuse of digital tools (digital disease).

Society should encourage the guided and supervised use of digital technology until the end user has exhibited that they are cognitively and emotionally mature enough to be held economically, morally and legally accountable for their actions and the consequences inherited through the use of digital tools and technologies. This support should include education about:

- the public nature of digital actions;
- the permanence of actions in a digital society ;
- resisting social, media, peer and partner pressure;
- all members of society must be considered a [digital] neighbor;
- benefits of abstaining from sexual behavior through digital tools and technologies; and
- the potential economical, moral and legal liabilities of digital abuse.

Society must also recognize that many digital citizens will utilize digital tools and technologies irresponsibly for instant gratification. Therefore, all citizens should receive education and support materials to help them clearly understand and evaluate their own preparedness and digital consciousness before operating digital tools and technologies. Responsible use of digital tools and technologies should be based on a universal and preventative mindset that digital activity is public and permanent, and interaction with other digital citizens through digital means should be:

- consensual
- non-exploitative
- honest, and
- legal.

MY COMMITMENT TO DIGITAL CITIZENSHIP

Train yourself to maintain this thought system as you use and rely on your rapidly evolving digital tools and technologies:

- I am aware of the personal and global issues caused by digital ignorance and irresponsibility, and I am committed to cultivating good citizenship for myself, my family and my global community by using my digital tools with a Digital Consciousness.

- I am aware that poor digital judgment betrays my ancestors, my parents, my community and my future generations, and I will strive to eliminate the violence, fear, anger, ignorance and confusion stemming from digital abuse by understanding, practicing and communicating the mindset that my digital activity is public and permanent.

Creating a Mindset That Our Digital Actions Are
Public and Permanent
A Golden Rule for the 21st Century

The following information has been extrapolated with permission from the book,
"Creating a Mindset That Our Digital Actions Are Public and Permanent"

A GUIDE TO DECISION MAKING – SELF ASSESSMENTS

As you walk through each self-assessment exercise, remember that the steps and criteria for you to practice are not meant to communicate that you have no privacy in the world, only in the digital world. You must understand that if you "do it" with a digital tool, you have to have the mindset that what you are about to "do" is going to be public and permanent.

Self-Assessment Exercise 1

Each time you power up any digital tool (camera, computer, Internet, cell phone) picture a family member(s), friend, child, enemy, criminal, a deceased loved one, whomever means (or meant) the most to you in this world standing right over your shoulder.

- If you are truly OK with the person who means the most to you in this world seeing and knowing what you are about to do, and you are OK with what you are about to do becoming a part of your digital legacy – then go for it.

- If you are NOT OK with the person that means the most to you in this world seeing and knowing what you are about to do, and you are NOT OK with what you are about to do becoming a part of your digital legacy – then DO NOT DO IT!

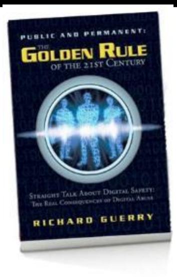
- If you are NOT OK with the person that means the most to you in this world seeing and knowing what you are about to do, and you are NOT OK with what you are about to do becoming a part of your digital legacy –BUT – you do it anyway; then you are abusing your digital tools and technologies!

Self-Assessment Exercise 2

When you leave your home with any digital tool whether it be a digital camera, cell phone, MP3 player, anything with "memory" (I will stress cell phones and digital cameras here, even MP3 players that shoot video and take pictures based on their, usually smaller size), be willing to hand that digital device to anybody, at any time and let them look at the memory card, let them "recover" or "un-delete" the memory card right in front of you.

If you are willing to walk out of your home with ANY digital tool, and you would not mind anyone seeing anything on that device, you are using your technology responsibly. If you are NOT willing to let anybody, at any time inspect and recover your device's memory card, then you are abusing digital technology **because you do not understand that you are just one second from losing it.**

DIGITAL RISK ASSESSMENT


PUBLIC AND PERMANENT:
THE GOLDEN RULE OF THE 21ST CENTURY
STRAIGHT TALK ABOUT DIGITAL SAFETY: THE REAL CONSEQUENCES OF DIGITAL ABUSE
RICHARD GUERRY

The following information has been extrapolated with permission from the book,
"Public and Permanent: The Golden Rule of the 21st Century

The History and Rationale of the Digital Risk Assessment

A popular tool created to help make the line between responsible use and abuse clear is the Cumulative Digital Risk Assessment created by the Institute for Responsible Online and Cell-Phone Communication. The assessment was conceptualized based on the increased momentum of society's narcissism and voyeurism as if they were two speeding locomotives headed towards each other until they collide creating , well, what looks like this – Λ – a spike. The Assessment helps to illustrate how much negative attention you are calling to yourself based on your digital behaviors. It consists of a series of questions that helps to cast a light on the poor judgment you may be (blindly) employing with digital tools and technologies so you can stop immediately.

The questions are very simple, and all you have to answer are a series of "yes or no" questions. If you answer incorrectly, you get a point value, and your "risk spike" goes up, and if you answer appropriately, you stay at zero. The higher your risk spike, the more negative attention you are calling to yourself and your actions – the further you are from the line of consciousness. The more negative attention you call, the more temptation there is for "someone" to look in on you through your digital device, your "window to the world." Remember, your "window" works two ways, and all you have to do is give someone a reason to look in, and they will. However, if you stay close to the line of consciousness through responsible use, your odds of becoming a victim of a C.E.L are very low as you are one in a billion digital users.

While the Risk Assessment was conceptualized from society's increase in narcissism and voyeurism, its actual creation and execution stems from an idea far more simple. Imagine you and I are standing outside of a stadium after a sporting event, just minding our own business. There are 50,000 people standing around us, and one of them is a thief. If nobody is doing anything to call attention to themselves, then it is likely that somebody who gets pick pocketed would have been selected at random by the criminal. Now imagine the same situation, however, just prior to the thief pick pocketing somebody, I stand up on a table in that sea of 50,000 people and I hold up a sign with my full name, social security number, address, credit card number, bank card and pin and a sexy picture.

Whereas before I was just one person in a sea of 50,000 people who *might* get robbed, I have just increased my chances of facing an issue (it is not guaranteed) because like an idiot I stood up and shared all kinds of personal information with complete strangers. In fact, with that kind of information, perhaps some people in the crowd who were not thieves before will be tempted to become one considering the info I just handed to them. By standing up and sharing certain information with 50,000 people, I increased my risk of exploitation.

The Risk Assessment applies the same theory. The more you answer yes, the more information you are sharing with the global [digital] village and everyone that lives in it. The more you answer yes, the higher you are holding a bull's-eye up over your head, and the larger the bulls-eye gets (like me standing on that table in front of 50,000 people holding up information for criminals to take advantage of). However, if your answers are consistently "no" then your spike is low, thus you remain close to the line of consciousness. The lower your risk spike, the less negative attention you call to yourself, the less you stand out to everyone in the digital world, and the less liability you incur.

THE DIGITAL RISK ASSESSMENT

1. You have a PERSONAL social web page (e.g. Facebook, My Space, Linked In, Blogger, etc). **If Answer is Yes: 10 Points**
2. I have posted my PERSONAL phone / cell number on a social website, chat room, board, etc. **If Answer is Yes: 10 Points**
3. I have posted my HOME address on a social website, chat room, public board, etc. **If Answer is Yes: 10 Points**
4. I have posted my SCHOOL / WORK address on a social website, chat room, public board, etc. **If Answer is Yes: 10 Points**
5. I post current / future status updates - Example: Going on vacation tomorrow. **If Answer is Yes: 10 Points**
6. I think deleting a file (pic, vid, text, etc) from Digital Tools removes it permanently. **If Answer is Yes: 10 Points**
7. I have anti-virus AND anti-spyware programs installed on my computer. **If Answer is No: 10 Points**
8. I run my anti-virus AND anti-spyware programs daily. **If Answer is No: 10 Points**
9. I believe that I am truly anonymous in a digital world. **If Answer is Yes: 20 Points**
10. I believe my social site (i.e. Facebook) password truly keeps my content private. **If Answer is Yes: 20 Points**
11. I have taken digital pics / vids of myself that I wouldn't show my family or enemy. **If Answer is Yes: 50 Points**
12. I shared pics, vids or text about myself I wouldn't show my family or enemy. **If Answer is Yes: 100 Points**
13. I do and say things in front of my webcam that I wouldn't show my family. **If Answer is Yes: 50 Points**
14. I have harassed or bullied others through digital technology. **If Answer is Yes: 100 Points**

Additional Resources:

- The Answer Key for correct and incorrect answers can be found by taking the digital quiz online at www.iroc2.org/Digital_Risk_Assessment. The answer key includes hyperlinked articles, video examples and more.

- Resources for Teaching and Practicing Good Digital Citizenship including **The Declaration of Digital Citizenship** - www.iroc2.org/101.html

Notes:

Institute for Responsible Online and Cell-Phone Communication

Introducing Digital Responsibility to a Digital Generation

www.IROC2.org

DIGITAL CONSCIOUSNESS CONTRACT

Talking to your child about the dangers of digital abuse isn't always easy, but it is important. Now is not the time to be coy, shy, timid, or indirect with your kids. Every time they use digital technology, they open themselves up to the world, and to the benefits and risks that we all inherit once we power up! To help you talk with your child, and to establish fair and informed usage guidelines IROC2 has created the **Digital Consciousness Contract** to assist you with;

- Defining your child's approved digital devices
- Clearly outlining prohibited behaviors
- Setting up scheduled Check-Ups to monitor activity for irresponsibility or abuse
- Clearly communicating the consequences associated with your child's abuse of technology

Once you discuss and come to an agreement for each section below, sign and date this contract, and keep it in a prominent place, like the computer table or on the refrigerator as a constant reminder for everyone.

1) Authorized Digital Tools & Technologies

The following Digital Tools & Technologies are authorized to be used.

______________________________ ______________________________

______________________________ ______________________________

2) Digital Tools & Technologies Check-Ups

All authorized digital tools & technologies will be inspected by a Parent/Guardian according to the schedule below.

Every ______ □ Days □ Weeks □ Months – the agreed upon digital tools will be handed in for inspection.
[Insert #]

3) Issues Leading to Consequences: Prohibited Behaviors Should Be Listed.

Review the Issues on Page 2. Customize this list by adding your own. If necessary, use another sheet of paper to complete this section. Everyone initial & date the page(s) and staple it to this document.

4) Consequences and Rewards

Review the Consequences and Rewards on Page 2. Customize these lists by circling our suggestions or adding your own. If necessary, use another sheet of paper to complete this section. Everyone initial & date the page(s) and staple it to this document.

Son/Daughter:

I promise to abide by the contract outlined above. If I break any part of this contract, I will accept the consequences and will not utilize any unauthorized digital tools & technologies while the aforementioned consequences are in effect.

____

Son/Daughter Signature

Date: ______________________

Parent/Guardian:

I promise to do what I can to help my child succeed in following this contract. I understand this will be an evolving contract and promise to make myself available to discuss these rules and their consequences when necessary.

____

Parent/Guardian Signature

Date: ______________________

PUBLIC & PERMANENT
THE 21ST CENTURY GOLDEN RULE

Institute for Responsible Online
and Cell-Phone Communication

Introducing Digital Responsibility to a Digital Generation

www.IROC2.org

DIGITAL CONSCIOUSNESS CONTRACT

Issues Being Looked For:

- Posting, sharing or viewing sexually explicit, vulgar or illegal webcam sessions, images & videos (content)
- Posting, sharing or viewing sexually explicit texts, emails, or communication
- Posting, sharing or viewing any harassing or malicious internet posts or texts
- Posting or sharing any inappropriate personal information online
    - Home or Cell Phone Numbers
    - Home or School Name / Address
    - Inappropriate language or content
- Not updating and running antivirus and anti-spyware programs (at least weekly)
- Missing a scheduled Check-Up date
- Not adhering to established consequences if an Issue is discovered
- Using any 3rd party digital tools & technologies if any of the established consequences are in effect.
- Add Your Own

_______________________________________ _______________________________________

_______________________________________ _______________________________________

_______________________________________ _______________________________________

Consequence Options:

(circle those that apply)

In the event that any of the "Issues" stated herein are discovered during a Check-Up, the Consequences circled below shall be in effect for a period of

______ □ **Days** □ **Weeks** □ **Months** □ **Other**

- Digital Device Usage Suspension / Removal
- Digital Device Service Suspension / Removal
- Limited Internet Hours
- Relocation of Computer / Digital Device to "Common Area"
- Create Your Own

____

____

____

____

____

Potential Rewards to Earn:

(circle those that apply)

In the event that none of the "Issues" stated herein are discovered during a Check-Up, a Reward will be offered.

- Modification of Check-Ups Schedule
- Elimination of Check-Ups
- Allowance (Financial or Gift)
- Mutually Approved Software
- Mutually Approved Hardware or Digital Device
- Mutually Approved Games
- Continued Use of Approved Digital Device(s)
- Create Your Own

____

____

____

____

PUBLIC & PERMANENT

THE 21ST CENTURY GOLDEN RULE

NEWS & RESOURCES

The following lists include some excellent websites, news items and safety resources for you and your peers to review, share and discuss. Just copy and paste the URL into your browser.

News Items of Reference:

FACEBOOK COSTS JOB: Conn. superintendent loses job because of comments:
http://www.middletownpress.com/articles/2010/09/16/news/doc4c919100dd427985201086.txt

Report: Teen gets 15 years for Facebook blackmail:
http://news.cnet.com/8301-1023_3-10459536-93.html

Nude Pics In Phone Lost At McDonald's End Up Online:
http://www.huffingtonpost.com/2008/11/23/nude-pics-in-phone-lost-a_n_145872.html

2 Florida Teens Charged with Felony Over Cyberbullying Incident:
http://facecrooks.com/Blog/Creeps-of-the-Week/2-Florida-teens-charged-with-felony-over-cyberbullying-incident.html

The Case That Could End Cyberbullying:
http://www.salon.com/life/feature/2010/10/18/carla_franklin_google_lawsuit

2 N.J. teens labeled sex offenders for life after 'horseplay' incident:
http://www.nj.com/news/index.ssf/2011/07/teens_sex_offenders_horseplay.html

Social Media History Becomes a New Job Hurdle:
http://www.nytimes.com/2011/07/21/technology/social-media-history-becomes-a-new-job-hurdle.html?_r=1&pagewanted=all

Resources:

Digital Risk Assessment – Measure your Digital Consciousness™:
http://www.iroc2.org/Digital_Risk_Assessment

Institute for Responsible Online and Cell-Phone Communication – Award Winning Nonprofit:
http://www.iroc2.org

Public and Permanent – Learn more about the 21st Century Golden Rule:
http://www.publicandpermanent.com/index.html

Tips Prevent – Threat Assessment and Resolution Systems:
http://www.tipsprevent.com/IROC2

YouthLight, Inc – Educational Books and Materials:
http://youthlight.com

YourSphere for Parents - Great Informational Blog for Teachers & Parents:
http://internet-safety.yoursphere.com/

Family Watchdog - Find a Sex Offender (US):
http://www.familywatchdog.us/

National Center for Missing & Exploited Children - Report an Incident:
http://www.missingkids.com/missingkids/servlet/PublicHomeServlet?LanguageCountry=en_US

EveryClickMatters - Computer Security Information:
http://everyclickmatters.com/dangers/hoff.html

Spokeo.com - Personal Information Site Pipl - Personal Information Site:
http://www.spokeo.com/

Institute for Responsible Online and Cell-Phone Communication

Introducing Digital Responsibility to a Digital Generation

Phone: (877) 295-2005 **Fax:** (240) 363-0070 **Address:** P.O. Box 1131 200 Walt Whitman Ave. Mount Laurel, NJ 08054-9998 **Website:** www.iroc2.org

21st CENTURY GLOSSARY

2.1C: The Institute for Responsible Online and Cell-Phone Communication's precept of 21st century digital safety, responsibility and awareness ("2.1C") practiced through the mindset that use and actions taken with any form of current or future digital technology should be considered [globally] public & permanent.

Adware: A form of malicious code that displays unsolicited advertising on your computer.

Anti-virus / Anti-Spyware Software: Software that attempts to block malicious programs/code/software (called viruses or spyware) from harming your computer.

Blog (a.k.a weblog): A diary or personal journal kept on a website. Blogs are usually updated frequently and sometimes entries are grouped by specific subjects, such as politics, news, pop culture, or computers. Readers often post comments in response to blog entries.

Bookmark: A saved link to a website that has been added to a list of saved links or favorite sites (i.e., "Favorites") that you can click on directly, rather than having to retype the address when revisiting the site.

Browser: A program that lets you find, see, and hear material on web pages. Popular browsers include Netscape navigator, safari, Microsoft internet Explorer, Firefox, and chrome.

Buddies: A list of friends a user interacts with online through various media such as instant messaging (IM) and chat.

CDA: The Communications Decency Act of 1996, a part of the Telecommunications Act of 1996, was the first attempt by the U.S. Congress to protect children on the Internet from pornography. CDA prohibited knowingly sending or displaying "indecent" material to minors through the computer, defined as: "any comment, request, suggestion, proposal, image, or other communication that, in context, depicts or describes, in terms of patently offensive as measured by contemporary community standards, sexual or excretory activities or organs." The Act was immediately challenged by a law suit by the ACLU and blocked by a lower court. A year later the U.S. Supreme Court struck down the indecency provisions of the CDA in the historical cyberlaw case of Reno v. ACLU (1997). The Supreme Court held that a law that places a "burden on adult speech is unacceptable if less restrictive alternatives would be at least as effective in achieving" the same goal. However, the court reaffirmed the application of obscenity and child pornography laws in cyberspace.

Chatroom: A location online that allows multiple users to communicate electronically with each other in real time, as opposed to delayed time as with e-mail.

Circumventor Sites: Parallel websites that allow users (e.g. children) to get around filtering software and access sites that have been blocked.

Closed Systems: A limited network of sites that are rated and categorized by maturity level and quality. Within a closed system, users cannot go beyond
the network white list of approved websites.

Cookie: A piece of information about your visit to a website that some websites record automatically on your computer. By using a cookie, a website operator can determine a lot of information about you and your computer.

COPA: The Child Online Protection Act (COPA) of 1998 was an effort by the U.S. Congress to modify the CDA in response to the Supreme Court's decision in Reno v. ACLU. The law sought to make it a crime for commercial websites to make pornographic material that is "harmful to minors" available to juveniles. The purpose of COPA was to protect children from instant access to pornographic "teaser images" on porn syndicate web pages, by requiring pornographers to take credit card numbers, adult verification numbers, or access codes to restrict children's access to pornographic material and to allow access to this material for consenting adults only. Despite the critical need for measures to protect children from accessing harmful materials, the law was immediately challenged and blocked by lower courts, and has become the subject of an epic legal battle.

COPPA: The Children's Online Privacy Protection Act of 1998, which went into effect in April 2000, requires websites that market to children under the age of 13 to get "verifiable parental consent" before allowing children access to their sites. The Federal Trade commission (FTC), which is responsible for enforcing COPPA, adopted a sliding scale approach to obtaining parental consent.xviii The sliding scale approach allows website operators to use a mix of methods to comply with the law, including print-and-fax forms, follow-up phone calls and e-mails, and credit card authorizations.

CIPA: The Children's Internet Protection Act (CIPA) of 2000 requires public schools and libraries receiving federal e-rate funds to use a portion of those funds to filter their internet access. They must filter out obscenity on library computer terminals used by adults and both obscenity and harmful-to-minors materials on terminals used by minor children. CIPA was upheld by the u.s. supreme court as constitutional in June 2003.

Cyber Bullying: Cyber bullying is the use of e-mail, instant messaging, chat rooms, pagers, cell phones, or other forms of digital technology to deliberately harass, threaten, or intimidate someone. The problem is compounded by the fact that a bully can hide behind an electronic veil, disguising his or her true identity. This makes it difficult to trace the source, and encourages bullies to behave more aggressively than they might face-to-face. Cyber bullying can include such acts as making threats, sending provocative insults or racial or ethnic slurs, gay bashing, attempting to infect the victim's computer with a virus, and flooding an e-mail inbox with nonsense messages.

Cyber Exploiter of Life (C.E.L): A C.E.L is any individual(s) or organization(s) that "gains", "profits" or "benefits" personally or professionally from the exploitation of (digital) citizens through digital tools and technologies or cyber space.

Cybercrime: Any cyber-related illegal activity.

Cybersecurity: Any technique, software, etc., used to protect digital devices like smart phones and computers and prevent online crime.

Cybersex (a.k.a "cybering"): Refers to virtual sexual encounters between two or more persons.

Cyberstalking: Methods individuals use to track, lure, or harass another person through digital technologies.

Denigration: A form of bullying or cruelty - to attack the character or reputation of another.

Digital Details: The information discovered during an investigation into a crime or "occurrence" whereby the victim's digital information and behavior(s) offers insight into the motive for the attack or incident to occur.

Digital Disease™: Digital Disease™ is a term trademarked by The Institute for Responsible Online and Cell-Phone Communication for any current or future malicious, harmful, or socially negative action or trend utilizing digital technologies. Examples of Digital Disease™ include, but are not limited to viruses, spyware, SPAM, cyber bullying, sexting and sextcasting.

Digital Risk Spike: An assessment tool to both; (i) illustrate your level of digital risk based on your digital behavior, as well as (ii) illustrate what behaviors you need to modify to minimize your digital risk.

Discussion Boards: Also called internet forums, message boards, and bulletin boards. These are online sites that allow users to post comments on a particular issue.

Domain name: The part of an internet address to the right of the final dot used to identify the type of organization using the server, such as .gov or .com.

Download: To copy a file from one computer system to another via the internet (usually your computer or mobile device).

Electronic Footprint: Digital tools accessing the internet maintain a record of all website visits and e-mail messages, leaving a trail of the user's activity in cyberspace. These data can still exist even after the browser history has been cleared and e-mail messages have been deleted.

Electronic mail (email): An electronic mail message sent from one computer or mobile device to another computer or mobile device.

Favorites: The name for bookmarks used by Microsoft's internet Explorer browser.

File Sharing: This software enables multiple users to access the same computer file simultaneously. File sharing sometimes is used illegally to download music or software.

Filter/Filtering: Allows you to block certain types of content from being displayed. some of the things you can screen for include course language, nudity, sexual content, and violence. Different methods to screen unwanted Internet content include whitelisting, blacklisting, monitoring activity, keyword recognition, or blocking-specific functions such as e-mail or instant messages. Filtering options are available through parental control software.

Firewall: A security system usually made up of hardware and software used to block hackers, viruses, and other malicious threats to your computer.

Flame: A hostile, strongly worded message that may contain obscene language.

Gamer Tag: The nickname a user has chosen to be identified by when playing Internet games.

Gaming: Internet games, which can be played either individually or by multiple online users at the same time.

Griefers: Internet gamers who intentionally cause problems and/or cyberbully other gamers (i.e., individuals who play online games).

Grooming: Refers to the techniques sexual predators use to get to know and seduce their victims in preparation for sexual abuse.

Hardware: A term for the actual computer equipment and related machines or computer parts.

History: A tracking feature of Internet browsers that shows all the recent websites visited.

Homepage: The site that is the starting point on the web for a particular group or organization.

Identity Theft: Illegally obtain the vital information (e.g., credit card, social security number, bank account numbers) of another person, usually to steal money. E-mail scams, spyware, and viruses are among the most typical methods for stealing someone's identity.

Instant message (IM): Real-time text conversation between two users.

Internet: A giant collection of computer networks that connects people and information all over the world.

Internet Relay Chat (IRC): A multi-use live chat facility. IRC is an area of the Internet comprising thousands of chat rooms. IRC is run by IRC servers and requires client software to use.

Internet Service Provider (ISP): A generic term for any company that can connect you directly to the Internet.

JPEG: A popular file format for images.

Malware: Stands for malicious software or code, which includes any harmful code—trojans, worms, spyware, adware, etc.—that is designed to damage the computer or collect information.

Mobile Web: The World Wide Web as accessed from mobile devices such as cell phones, PDAs, and other portable gadgets connected to a public network. Access does not require a desktop computer.

Modem: A device installed in your computer or an external piece of hardware that connects your computer to the Internet through a phone or cable line and allows communication between computers.

Monitoring Software: Software that allows you to monitor or track web activity (e.g. websites or e-mail messages) that a digital user visits or reads.

Mouse: A small hand-controlled device for pointing and clicking to make selections on the screen.

Netiquette: Rules or manners for interacting courteously with others online.

Outing: The practice of publicly revealing that a person is not straight without that person's consent.

Password: A secret word or number that must be used to gain access to an online service or to modify software, such as a parental control.

Parental controls: Specific features or software that allow parents to manage the online activities of children.

Peer-to-Peer (P2P): A method of sharing files directly over the internet from one Internet-enabled device to another (computer, mobile phone, etc.), without being routed through a server.

Phishing: In the field of computer security, phishing is the criminally fraudulent process of attempting to acquire sensitive information such as usernames, passwords and credit card details by masquerading as a trustworthy entity in an electronic communication. Communications purporting to be from popular social web sites, auction sites, online payment processors or IT administrators are commonly used to lure the unsuspecting public. Phishing is typically carried out by e-mail or instant messaging, and it often directs users to enter details at a fake website whose look and feel are almost identical to the legitimate one. Even when using server authentication, it may require tremendous skill to detect that the website is fake.

Post: To upload information to the Web.

Real Time: "Live" time; the actual time during which something takes place.

Search engine: An Internet service that helps you search for information on the web.

SextCasting: The process by which an individual(s) performs actions of a risqué or sexually explicit nature via a (live) webcam (or webcast), digital (image or video) camera, or other form of digital technology and sends and/or saves the content of their actions using digital technologies (i.e. a computer, camera card, email, social website, message board, etc).

Sextortion: A form of sexual exploitation where people are extorted with a sexually explicit image or video of themselves typically acquired by a criminal through digital technology.

Sexting: The act of poor judgment when using a cell-phone, smart phone, or PDA (digital technology) by sending an image, video or text message of an explicit (adult) or risqué nature to another individual.

Skype™: A popular computer program that enables users to set up profiles, make free phone calls, chat, and video chat through their computer or mobile device from any point around the world. This free service functions through a “peer-to-peer” network, which allows individuals to communicate directly with each other rather than through a central server.

SMS: Stands for “Short Message Service,” a form of text messaging on cell phones, sometimes used between computers and cell phones.

Social Networks: Online communities where people share information about themselves, music files, photos, etc. There are many social networking websites (e.g., Myspace, Facebook, or Friendster).

Software: A program, or set of instructions, that runs on a computer.

Spam: Any unsolicited e-mail, or junk mail. Most spam is either a money scam or sexual in nature. Internet service Providers, e-mail software, and other software can help block some, but not all, spam.

Spyware: Spyware is a type of malware that is installed on computers and to collect information about users without their knowledge. The presence of spyware is typically hidden from the user as it is secretly installed on the user's computer. Sometimes, however, spywares such as keyloggers are installed by the owner of a shared, corporate, or public computer on purpose in order to secretly monitor other users.

Surfing: Users browsing around various websites.

Texting: A method of sending short messages between mobile phones and other computer-enabled devices.

Uniform Resource Locator (a.k.a URL): The address of a web site on the World Wide Web.

Upload: To send information from your computer to another computer.

Username: The name a user selects to be identified on through the internet, computer, network, online gaming and other interactive technologies.

Virus: A digital or computer virus is a program that can copy itself and infect a digital device. A true virus can only spread from one computer to another (in some form of executable code) when its host is taken to the target computer; for instance because a user sent it over a network or the Internet, or carried it on a removable medium such as a floppy disk, CD, DVD, or USB drive. Viruses can increase their chances of spreading to other computers by infecting files on a network file system or a file system that is accessed by another computer.

Webcam: Internal or external [video] cameras often attached to a digital device so that a (often live) video image can be sent to another while communicating online.

Wireless computers: Enable computers to access the Internet without being connected with wires.

World Wide Web (a.k.a www or web): A hypertext-based navigation system on the internet that lets you browse through a variety of linked resources, using typed commands or clicking on hot links.