Instructor and Parents

Effective C3 Tech Tips

INSIDE THIS ISSUE:

C3 Framework

- Cyberethics
- Cybersafety
- Cybersecurity

- Taught as a whole, yet each having a unique focus
- Spotlights the importance of each component
- Provides the opportunity for more complete coverage
- Accounts for intervention differences

Words to Remember

Parents and teachers want to know what messages to send to kids regarding the C3 issues that pop up every day. Decades of research on effective communication with children tell us that the messages need to be **positive**, **short**, and **repeated often**. This means that in addition to positive, succinct lessons, kids also need to hear about good C3 practice from parents and instructors frequently. High-quality messages repeated often will help turn C3 content into good C3 habits.

Parents and teachers should set the expectation that kids should develop the following four habits.

I am responsible

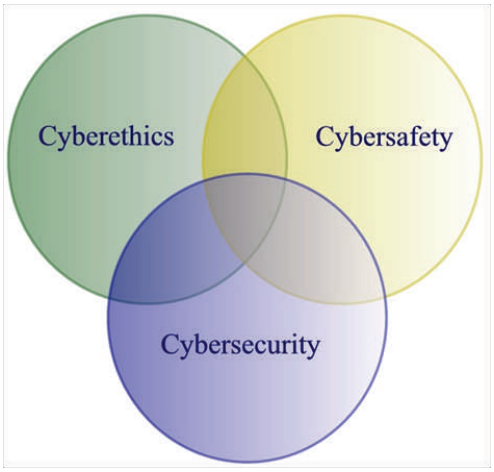
I am respectful

I am prepared

I am safe

These life lessons augment the C3 framework by defining the behaviors that are expected of every person using technology. It is only when these C3 habits are practiced by every individual who uses information and communication technology (ICT) that our data, personal information, and the places where we work, learn and play will be safe. Read on to see what specific C3 tips kids need to hear early and often.

In this newsletter you will learn what content to cover for each of the C3 topics as well as good habits to help your kids be responsible, respectful, prepared and safe when using ICT. Associated with each good habit is a quote in blue which is a positive, short message you can tell your kids to reinforce good C3 practice.



The C3 Framework: Assuring Complete Content Coverage

In research conducted by Educational Technology Policy, Research and Outreach (ETPRO), it was learned that the label "Internet safety" is over-used to describe selected content that is taught in schools. While plagiarism and cyberbullying are important topics, cybersafety and cybersecurity encompass a much broader scope of topics. Only recently have cybersecurity topics been discussed in the public arena, yet they are virtually ignored in the educational setting. Teaching all C3 topics as one, through branding such as *digital citizenship* or *Internet safety* curriculum, makes it far too easy to check off the topic as "covered," while only scratching the surface of individual domains.

ETPRO developed the C3 Framework in 2000 to assure that all important content is included in curriculum, policy, and most importantly in conversations with children. By detailing particular elements under each domain, organizations can better design and address critical content.

Cyberethics

Cyberethics is the discipline dealing with what is good and bad, and with moral duty and obligation as they pertain to online environments and digital media. Topics include:

- Plagiarism
- Copyright
- Hacking
- Fair use
- File sharing

File sharing is not only illegal it leaves computers susceptible to malware.

- Online etiquette protocols
- Posting incorrect/ inaccurate information
- Cyberbullying
- Stealing software, music, and videos
- Online gambling
- Gaming/ Internet addiction
- Reputation management

Cybersafety

Cybersafety addresses the ability to act in a safe and responsible manner on the Internet and online environments. These behaviors can protect personal information and one's reputation, and include safe practices to minimize danger — from behavioral-based rather than hardware/software-based problems. most of the issues covered in Cybersafety are steps that one can take to avoid revealing information by "social" means. Topics include:

- Online predators
- Objectionable content
- Cyberstalking
- Harassment
- Pedophiles
- Hate groups
- Pornography
- Unwanted communications
- Online threats

More dangerous than any technical threat to your computer is a lack of awareness of the dangers and what to do if they occur.

Cybersecurity

Cybersecurity is defined by the HR 4246, Cyber Security Information Act (2000) as "the vulnerability of any computing system, software program, or critical infrastructure to, or their ability to resist, intentional interference, compromise, or incapacitation through the misuse of, or by unauthorized means of, the Internet, public or private telecommunications systems, or other similar conduct that violates Federal, State, or international law, that harms interstate commerce of the US, or that threatens public health or safety." Cybersecurity covers physical protection (both hardware and software) of personal information and technology resources from unauthorized access gained via *technological* means. Topics include:

- Hoaxes
- Viruses and other malicious self-replicating code
- Junk email with links to malicious sites
- Chain letters
- Ponzi schemes
- Get-rich-quick schemes
- Scams
- Criminal hackers
- Hacktivists
- Spyware
- Adware
- Malware
- Trojans
- Phishing
- Pharming scams
- Theft of identity
- Spoofing
- Privacy

Top 10 C3 Concepts

1. If you don't know them in real life –use common sense
2. Project a positive image through your posts
3. Limit the information you share about yourself
4. Be thoughtful about what you click on
5. Cite work that is not your own
6. Scan and update your computer
7. Use a firewall
8. Disable or block web cameras when not in use
9. Identify a trusted adult in case of trouble
10. Spend time off-line too

Cyberethics Good Habits

Responsible
For creating their own work and protecting the copyrights of others
"Cite it if you did not create it yourself"

Respectful
Of the feelings of others and use caution in what they post.
"Posting is permanent and can be traced back to the author"

Prepared
To help others who are not behaving ethically or are victims of cyberbullying or harassment.
"Identify a trusted adult you can talk to"

Safe
By setting time limits for using ICT and expanding real life activities.
"Seek a balance between virtual and real life fun."

Cybersafety Good Habits

Responsible
With my personal and other's personal information. Revealing too much information about themselves and others facilitates identity theft and cyberstalking.
"Limit the information you share about yourself and your friends"

Respectful
Of their own reputation and the reputation of others. Objectionable content can be read by parents, grandparents, recruiters, schools and employers.
"Respect yourself by only posting content that projects a positive image about yourself"

Prepared
To help others who are being threatened, stalked, or have too much information revealed about them.
"Print the screen, and save messages to show the police or a trusted adult."

Safe
Responding to unwanted communications is the greatest predictor of physical danger.
"Use common sense communicating with unknown sources"

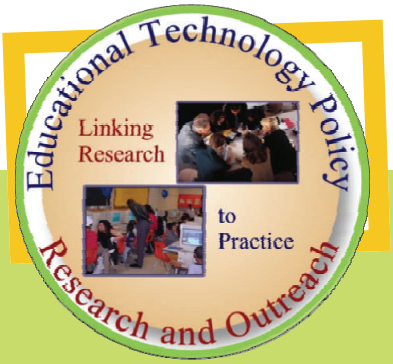
Cybersecurity Good Habits

Responsible
Technical protections include virus and malware software which should be run daily. A hardware or software firewall is also necessary to protect hardware and software.
"Run your malware detection software daily"

Respectful
Links and attachments in emails can cause unwanted software to damage your computer. Respect others who use a computer by avoiding things that can cause viruses and malware infections.
"Protect everyone who shares your computer by thinking before clicking"

Prepared
Updating and patching computer software is an important part of responsible computer ownership. — this includes scanning software as well as operating systems and internet browsers.
"Set the update option on your virus and malware scanning software to automatic .

Safe
Unprotected web cameras can be accessed by anyone.
"Put a Post-it Note over your web camera when not in use"



Phone: 410-531-3910
E-mail: info@edtechpolicy.org

INSTRUCTOR AND PARENTS

www.edtechpolicy.org

Attend the C3 Conference in October!

Educational Technology Policy, Research and Outreach provides expertise for program and grant initiatives that advance effective learning and teaching through technology integration, and research, program evaluation, policy analysis and teacher professional development through workshops, conferences and seminars. ETPRO research and development interests are focused on cyberethics, cybersafety, and cybersecurity (C3) awareness for students, educators and parents and developing programs to help increase the STEM workforce pipeline. ETPRO is responsible for conducting the groundbreaking 2008 National Cyberethics, Cybersafety, Cybersecurity Baseline and creating the C3 framework.

Now that I know, who can do something about it?

The most important role an adult can fulfill for children is be calm and non-judgmental when they come to you for help. Now that you have some tips to offer, there is one more piece of information you need to have. Many organizations provide valuable help when you or your children are exposed to illegal or inappropriate content or contact. The following links can help.

The National Center for Missing and Exploited Children provides a tip line for reporting information about online child pornography and inappropriate solicitation of children. http://www.cybertipline.com or call 1-800-843-5678

The **Federal Trade Commission** has a page of resources for victims of Identity Theft at http://www.ftc.gov/bcp/edu/microcsites/idtheft/tools.html

Prevent Cyberbullying and Internet Harassment provides resources for kids to help them learn more about how to talk to their parents and each other about the effects of cyberbullying and harassment. http://www.cyberbully411.org

Connect to someone who can help or provide more information.

The **Department of Justice** maintains a list of cybercrimes and links to the responding agency — for example, the FBI, U.S. Secret Service and the Internet Crime Complaint Center are responsible for computer intrusion and hacking crimes. http://www.justice.gov/crimal/cybercrime/reporting.htm

If you have purchased something online that is a fake of a genuine item, the government has the STOP Initiative. https://www.stopfakes.gov

If you are not sure who to report the crime to, try the **Internet Crime Complaint Center (IC3)**. This organization is a partner with the FBI, the National White Collar Crime Center and the Bureau of Justice Assistance. To support victims and law enforcement to easily report suspected cybercrimes. http://www.ic3.gov

Spam or "phishing" emails can be forwarded to the **Federal Trade Commission** which maintains a database to support and pursue law enforcement. spam@uce.gov

Also, don't forget to file a complaint with the ISP of the sender and your local law enforcement agency.