Embrace Civility in the Digital Age, a program of the Center for Safe and Responsible Internet Use, a non-profit corporation, is launching an innovative new approach to address youth risk when using digital technologies. This approach focuses on reinforcing positive norms, strengthening effective skills, and encouraging young people to be helpful allies if they see that a peer is at risk or being hurt. This approach is more fully described Cyber Savvy: Embracing Digital Safety and Civility, written by Nancy Willard, M.S., J.D., Director of Embrace Civility in the Digital Age, and is briefly described later in this document.

An important component of this approach is the use of a school-based survey to assess student norms and practices. A positive peer norms approach has been found very effective in reducing binge drinking among college students, bullying among middle school students, and other youth risk behavior. The Cyber Savvy approach encourages the use of survey insight to identify the positive norms and effective strategies used by the majority of young people when using digital technologies. This insight, especially locally derived, can be "transformative" -- the description of Gary McDaniel, a West Virginia school social worker who has been working with Willard in the implementation and assessment of this new approach.

At this time, Embrace Civility in the Digital Age seeks to obtain national data from high school students on the survey that will be made available for schools to use to support their own instructional program. The objective is to obtain the participation of a minimum of 18 high schools from throughout the United States. These schools will be asked to deliver the survey to 50 - 100 students. The survey takes approximately 30 minutes to complete. The survey is anonymous and provides students with information indicating that their participation is voluntary. An opt-out informed consent letter is provided in this packet.

It is our objective to complete the survey by October 5, 2012. The survey will be administered through Survey Monkey. The questions from the survey are provided in this document. Note, however, that the survey is in final stages of pretesting and may change slightly based on insight through this process.

The data will be collected at a national level. However, schools that participate in this national study will be offered free use of the survey and related instructional materials, including infographics and a slides presentation. Embrace Civility in the Digital Age is also providing a series of instructional videos that will provide the professional development necessary to support instruction. These will be available through SchoolTube.

Please contact us at nwillard@embracecivility.org if you are willing to participate.
Parent's Informed Consent

(Name of School) is participating in a national survey that seeks to assess students' norms and practices when using digital technologies. The insight from this survey will be used to guide instruction to make sure that young people make safe and responsible choices when using digital technologies.

This survey is being conducted by Embrace Civility in the Digital Age, a program of the Center for Safe and Responsible Internet Use. You can find more information about Embrace Civility on their web site at http://embracecivility.org. Director of Embrace Civility, Nancy Willard, M.S., J.D. is also author of a book for teachers on teaching digital safety entitled Cyber Savvy: Embracing Digital Safety and Civility.

Your son or daughter will be asked to complete a survey that assesses his or her norms and practices when using digital technologies. The survey takes about 30 minutes to complete. Participation in the survey will increase your son or daughter’s attention to how he or she is making choices when using digital technologies. The survey is anonymous, so no one will know how your son or daughter responded. Participation is voluntary.

If you do not want to have your son or daughter participate in this study, please sign this document and send it to school with your son or daughter or simply email * at * indicating you desire to have your son or daughter opt-out of this study.
Cyber Savvy Survey

This survey asks questions about how students make decisions when using digital technologies, including the Internet, cell phones, and other personal digital devices.

This survey is anonymous, so no one will know how you responded. Your participation in completing this survey is voluntary. You may also skip any questions you want.

Please answer honestly with what you think and are doing. Please do not try to figure out what the “right answer” is based on what you have been told you are supposed to do. We want to know what you really think and how you are making decisions.

As you are going through this survey, some of you might think to yourselves, “I know this stuff, so why are they asking?” One of the reasons for conducting the survey is to get insight into the good decisions that most older teens are making. This insight will be helpful in making younger teens aware of some of the things you have already learned.

The survey will require you to think about what you are doing when using digital technologies. It will take you about 30 minutes to complete. So do not start unless you have this much time.

Thank you for your participation.

Q1
What grade in school are you?
7th grade.
8th grade.
9th grade.
10th grade.
11th grade.
12th grade.

Q2
Are you male or female?
Male.
Female.

Q3
How do you make decisions when you post, send, or text?
I am always very careful about what I post, send, or text.
I am careful about what I post publicly, but am less careful about what I send privately or text.
I do not think about it much.
I should be able to post, send, or text whatever I want to.

Q4
What do you think are the most common reasons why people sometimes make mistakes or bad choices when they post, send, or text? (Click all the reasons you think are most common.)
They thought they were invisible so no one would know they did this.
They did not think about the fact that their digital actions could harm someone else.
They did not think about the fact that their digital actions could harm their own reputation.
They did not recognize they were being deceived by another person.
They posted digital material without thinking things through, forgetting that it could be seen by lots of people.
They sent or texted a digital message privately to someone, forgetting that it was possible for 
this person to forward the message to others. 
They acted in anger when they posted, sent, or texted something. 
They following what someone else was doing. 
They thought that because they could easily do something using technologies, it was okay to 
do so. 
They were trying to get attention and forgot to think about the kind of attention they were 
going to get. 
They were pressured or manipulated by someone else.

Q5
If you were thinking about doing something hurtful or inappropriate online, what are the three 
most important reasons why you might change your mind? 
How I would feel about myself after I did this. 
How I would feel if someone did this to me. 
What my friends would think about me. 
What my parents, guardian, or other important adults would think about me. 
What my teachers or other school staff would think about me. 
What people I don't know would think about me. 
Whether someone might file an Abuse Report. 
Whether my Internet access would be restricted or my cell phone taken away. 
Whether I could get into trouble at home. 
Whether I could get into trouble at school. 
Whether I could be arrested.

Q6
How should teens handle the privacy settings on their social networking profile? 
Use the initial settings that the company provides. 
Use settings that only allow the people they have specifically friended see what they post. 
Use settings that allow people who their friends have friended see what they post. 
Use settings that allow their personal information and posts to be public.

Q7
Who should you share the following kinds of personal information with by posting, sending, or 
texting? 

Never post or send 
Very trusted friend 
Friends 
People I have friended on my profile 
People my friends have friended on their profiles 
Someone met online 
Public 
Professional support site 
Company web site

Material about my interests and activities. 
My full name. 
The city I live in. 
The school I attend. 
My password. 
Personal contact information (my home address and phone numbers).
Digital contact information (my profile name, e-mail address, IM address, and/or Twitter address).
Financial account information (debit card, credit card, or bank account information).
Material that discloses personal difficulties I am having.
Material that could make people think I make bad choices.
Material I want to be kept secret.
Material that could make someone reading it think that I intended to harm someone.
Material about someone else that discloses the personal difficulties he or she is having.
Material about someone else that could make people think that he or she makes bad choices.
Material about someone else that he or she would want to be kept secret.

Q8
How likely are you to friend the following types of people on your social networking profile?

Very likely to friend
Likely to friend
Not likely to friend
Will not friend

Know face-to-face and like
Know face-to-face, but not very well
Know face-to-face, but are not really friends
A trusted friend of mine knows face-to-face
Met online doing activities we both enjoy
Sent me a friend request, but we have no other connection

Q9
If you have temporarily friended someone who you do not know very well, how important to your decision about whether to continue this friendship connection are the following things?

Very Important
Important
Not that important
Not at all important

What I think about what this person has posted about him or herself.
What I think about the other people who this person is friends with.
Why this person appears to be interested in having a friendship with me.
Whether what this person says to me fits in with what else I know about this person
Whether this person appears to be trying to manipulate me.
My “gut” reaction to this person.
What my friends think about this person.
What my parent or guardian thinks about this person.

Q10
How likely would you continue friending someone on your personal profile who does the following?

Very likely to continue to friend
Likely to continue to friend
Likely to unfriend
Very likely to unfriend

- Posts comments about others that are hurtful.
- Posts nice comments online about other people.
- Always seems to be doing things that create a lot of "drama."
- Posts inaccurate information about him or herself.
- Posts funny information and sayings.
- Posts material that makes me question whether he or she makes good choices.
- Uses digital postings to make sure that people know about important or fun activities.
- Is being overly friendly, always posting comments on my posts and images, although we do not really know each other.
- Has taken the time to communicate with me so we can learn more about each other.
- Posts nice, friendly comments about other people.
- Is constantly messaging me about things that are not important.
- Encourages people to do things that could be risky.
- Privately makes suggestions to me if he or she has concerns about something I have done online.
- Has lots of friends on his or her profile, who this person obviously does not know face-to-face.
- Has other friends on his or her profile who appear to make good choices and have lots of fun.
- Does not appear to have anyone on his or her profile who he or she knows face-to-face.
- Has friends on his or her profile who do not appear to make good choices.
- Posts comments on my images that are sexually suggestive.
- Posts images or comments on his or her profile that are sexually suggestive.
- Constantly posts status updates describing what he or she is doing.

Q11
Sometimes teens want to meet face-to-face with someone they have gotten to know online. How safe is this?
- Totally safe.
- Only safe if you take steps to be careful.
- Never safe.

Q12
If you were thinking about meeting face-to-face with someone you had gotten to know online, how important do you think the following actions would be?

- Very important
- Important
- Not necessary
- Should not do this

Have my parent or guardian look over this person’s profile.
Have my friends look over this person’s profile.
Talk on the telephone before getting together in person.
Meet in a public place.
Bring along at least one trusted friend to a meeting in a public place.
Have my parent or guardian nearby.
Have both of our parents or guardians come to this meeting.
Have my cell phone so I can call or text for help if I need to.
Have this person come to my school to pick me up.
Go to this person’s school to pick him or her up.
Post a status update that we are meeting.
Give this person my home address.
Make sure to have an “escape” plan.
Have my parent or guardian’s approval.
Never leave the public place with this person.

Q13
What do you think if you see or find out that someone is cyberbullying another person?

"Cyberbullying" means intentionally posting statements, rumors, or pictures to hurt another person or damage his or her reputation or sending hurtful messages or texts.
I really do not like to see this.
The person doing this is just joking around.
The target probably deserves it.
It's none of my business.
It's no big deal.

Q14
How helpful do you think the following responses are if someone is being cyberbullied?

Very helpful
Helpful
Not that helpful
Not at all helpful

Take time to calm down before you do anything.
Talk with someone you trust before you do anything.
Immediately send a message telling this person what you think.
Ignore hurtful messages or texts.
Ignore the fact that something hurtful about you has been posted online.
Block the person from sending any more messages.
Calmly talk with the person face-to-face.
Calmly communicate with the person by text.
Calmly call the person.
Confront the person face-to-face demanding the person stop.
Send a message to the person demanding he or she stop.
Call and demand the person stop.
Apologize to this person if you have also done something hurtful.
Send hurtful messages back to this person.
Post hurtful information about this person online.
Get into a public argument with this person online.
Get into a public argument with this person face-to-face.
Talk with a friend to help figure out how to respond.
Ask a mutual friend to communicate with the person being hurtful.
Talk with your parent, guardian, or other trusted adult.
Report this to someone at school.
Report this to a police officer.
File an Abuse Report on the site.

Q15
Think about what other students might do when they see someone being cyberbullied. How likely would you want to be friends with someone who responded in this way?
Very likely
Likely
Not that likely
Not at all likely

Joined in and posted hurtful material.
"Liked" the hurtful material.
Told others what was happening, but nothing more.
Read the material, but did nothing more.
Just ignored the situation.
Reached out to be kind to the person being cyberbullied.
Helped the person being cyberbullied figure out what to do.
Privately told the person being hurtful to stop.
Publicly posted "stop."
Told an adult who could help.
Filed an abuse report.

Q16
Sometimes older teens may meet someone online and form a close personal relationship.
Which statement best describes your thoughts on this?
This is a great way to form a close personal relationship.
There are generally no problems forming a close personal relationship in this way.
It may be possible to form a close personal relationship in this way, but only if you are really careful.
It is very dangerous to form a close personal relationship in this way.

Q17
Older teens might get to know someone through digital communications, without face-to-face contact.
We would like to find out what you think about forming a personal relationship in this way.

Strongly agree
Agree
Sort of agree/sort of disagree
Disagree
Strongly disagree

When you communicate with someone using digital technologies it is possible to get to know them in an effective way.
If you are currently having difficulties with your friends at school, finding someone online is a good thing to try.
It is very important to look closely at what he or she has posted online and who his or her other friends are.
What this person tells you is most likely true.
What you think is a real relationship could just be a fantasy.
Teens can get lured into unsafe relationships because they really want someone to pay attention to them.
It is okay to form a close relationship online with someone who is significantly older than you.
If the person offers you a chance for a modeling job, this is a sign the person can really help you.
If the person asks for a sexy nude image, sends you a nude sexy image, or wants to talk about sex, these are signs of danger.
If this person sends you lots of messages or texts, this is a sign this person really likes you. If this person constantly sends you messages/texts asking where you are, what you are doing, and who you are with, this is a sign this person is trying to control you.

Q18
If you detect any signs of concern, what should you do? (Click all that apply.)
Continue the relationship.
Discuss your concerns with this person.
Ask your friend for his or her opinion.
End the relationship.
Block the person from communicating with you.
Tell an adult who can help you.
Tell an adult who can help you, only if you have difficulties ending the relationship.
Tell an adult even if you have ended the relationship, because this person could be dangerous to another teen.
Cyber Savvy Students

The majority of young people make positive choices online, effectively respond to the negative situations that do occur, and are not overly distressed by these situations. They may make mistakes that could be prevented through better education. A minority of young people face greater risks that must be addressed through effective prevention and intervention.

**Cyber Savvy Strategy**

Nancy Willard’s new book, Cyber Savvy: Embracing Digital Safety and Civility, provides comprehensive insight for educators to provide instruction. Her focus is on ensuring young people become Cyber Savvy. Cyber Savvy youth:

- **Keep Themselves Safe.** They understand the risks and know how to avoid getting into risky situations, to detect whether they are at risk, and to effectively respond.
- **Present a Positive Image.** They present themselves online as someone who makes positive choices.
- **Respect Others.** They respect the rights, privacy, and property of others and treat others with civility.
- **Take Responsibility for the Well-being of Others.** They help others and report serious concerns to a responsible adult.

**Instructional Components**

Incorporate these three key components into instruction:

- **Reinforce Positive Norms.** Universal education must promote the positive norms and effective practices held by the majority of the students. This can be accomplished through student-led constructive instruction, use of older students to teach younger students, and messaging ground in the insight into positive norms and practices derived through local surveys.
- **Strengthen Effective Skills.** Constructive instruction can also help students gain skills through sharing of effective practices and strategies. Effective skills include problem-solving and decision-making. Students must also recognize possible negative influences related to the use of technologies, as well as the influences for making positive choices.
- **Encourage Helpful Allies.** As helpful allies, young people can provide support to a peer who is at risk or being harmed, challenge irresponsible or hurtful behavior, and report unresolved or serious concerns. Increase skills in responding and emphasize the positive perspective of helpful allies.

**Key School Action Steps**

Implement these key actions steps:

- **Establish a Multidisciplinary Coordinating Committee.** Include educational technology specialists, school librarians, and health teachers—and the school resource officer if this person will be providing instruction. Collaborative involvement of these professionals is essential.
- **Ensure Professional Development.** All members of this team require an understanding of the issues and effective instructional approaches that is ground in research insight. A significant amount of disinformation has been disseminated over the last decade about Internet risk. Fear-based messaging and simplistic rules against normative online behavior will not be effective in preventing risk behavior.

**Instructional Don’t’s & Do’s**

The following are approaches to avoid and alternatives to look for when evaluating curriculum or presenters:

- **Avoid** approaches that communicate the misperception that many young people are at risk online or are engaging in unsafe or irresponsible actions. **Choose** approaches that communicate positive messages that the majority of young people make safe and responsible decisions and effectively respond to negative situations.
Avoid approaches that impart inaccurate, fear-based information and messaging. **Choose** approaches that provide insight grounded in research on actual risks and degree of harm associated with those risks.

Avoid approaches that impart simplistic rules against normative online behavior like rules against communicating with any online strangers or posting photos of oneself or of friends online. **Choose** approaches that focus on problem solving and skill building.

Avoid approaches that impart "stranger danger" warnings and try to make it appear that anyone they meet online is highly likely to want to harm them. **Choose** approaches that focus on strategies young people can use to safely interact online with people who are known in person or not.

Avoid approaches that rely primarily on adults directly instructing secondary students. However, sometimes this approach can be useful, for example, having a law enforcement official make a special presentation. **Create** situations where the majority of the instruction engages students in talking with their peers.

Avoid having students sign "Internet safety pledges." **Encourage** students to develop their own statements of personal standards.

Avoid recommending that parents of teens strongly rely on filtering or monitoring technologies. **Recommend** that parents engage in active and positive interactions, use protective technologies for children, and constructively use monitoring technologies for tweens and at-risk teens.

**Being Cyber Savvy**

Cyber Savvy: Embracing Digital Safety and Civility present the following key areas of necessary insight and steps to being Cyber Savvy:

**Avoid the Impulse. Remember, what you do reflects on you.**

- If you engage in an impulsive negative act that results in posting or sending material in digital format, this material can become widely disseminated and possibly permanently available. This could harm your reputation, friendships, and opportunities; place you at risk; or cause harm to others.

- Engage in effective problem solving and positive decision making before posting or sending anything. Be a helpful ally if you see someone is at risk or is being harmed.

**Read With Your Eyes Open. Assess the credibility of information.**

- Anyone can post or send anything online, and there is no guarantee that what has been posted or sent is accurate. Individuals, organizations, and companies may use sophisticated techniques to seek to influence your attitudes and behavior.

- Carefully assess the credibility of all information accessed on websites or received in messages and the trustworthiness of people you interact with.

**Keep Your Life in Balance. Avoid addictive use of digital technologies.**

- While use of digital technologies can be fun and allow you to connect with your friends, excessive use of digital technologies can be unhealthy.

- Ensure your use of digital technologies does not interfere with other activities that will make your life happy and successful.

**Think Before You Post. Protect your reputation and respect others.**

- Other people will judge your character and decision making based on the material you post and send. This can effect your reputation, friendships, and opportunities positively or negatively. You can hurt others if you post or send material that reveals their personal information.

- Be careful whenever posting or sending material in digital format. Respect the rights and privacy of others.

**Connect Safely. Interact safely with others online.**

- You will interact with many different people online. Most are safe and trustworthy, but some may not be. It is easier for people to be deceitful and manipulative online.
• Be careful when you interact with people online. Only let people you know, or those whom your good friends know, have access to your personal profile. If you want to meet in person with someone you have gotten to know online, make a safe meeting plan and bring along friends.

**Keep Yourself Secure. Implement security and avoid scams.**

• Digital technologies can be corrupted with malware, which often is used to commit identity theft. Criminals use the Internet to commit a variety of scams.

• Ensure your computer security is maintained and your activities do not increase your risk. Watch out for scams—offers that are too good to be true or threaten loss if you do not share personal information.

**Abide by the Terms. Act in accord with policies, terms, and laws.**

• Your online activities are governed by laws, use policies of the organization that provides your access, and the terms of use of the websites or services. These laws, policies, and terms ensure that user’s activities do not cause harm to others or to the technical system.

• Follow the common standards to protect the rights of everyone.

**Stay Out of the Garbage. Avoid objectionable and illegal material.**

• People distribute materials online that are harmful to others, including pornographic material. You could accidentally access this material. Accessing or distributing child pornography is a serious crime.

• Use safe surfing techniques to avoid accidentally accessing this material. Know how to effectively respond if such material is accidentally accessed. Don’t access or distribute child pornography.

**Don’t Sell Yourself. Disclose and consume wisely.**

• The financial model of the Internet involves providing access to free content and services in exchange for market profiling and advertising. Sites and apps track your postings and activities to create a market profile that guides the advertisements you will see. Social networking sites encourage friends to send advertisements to their friends. You can find helpful information about companies and their produces or services online.

• Make a personal decision about how much personal information you want to share with sites and apps. Use the Internet to research companies, products, and services prior to making purchases.

**Protect Your Face and Friends. Be savvy and civil when networking.**

• Social networking sites are fun places to post information and connect with friends but present risks that involve posting inappropriate material or engaging in unsafe interactions with others. These sites encourage users to share personal information and have many friends so they and their advertisers can obtain market profile information and use friendship connections to encourage purchasing. The terms of use prohibit hurtful actions.

• Protect your privacy by limiting access to your profile to those you have friended. Protect your reputation and respect others when you post. Friend only people whom you or a trusted friend know in person. Report abuse.

**Embrace Civility. Prevent hurtful digital communications.**

• The vast majority of people do not like to see others post hurtful material, send hurtful messages, disclose private material, or cause other harm through digital communications.

• Exercise care when posting or sending material so you do not place yourself at risk of attack. If someone is hurting you, wait until you have calmed down to respond. Save the evidence. Then calmly tell the person to stop, ignore or block the communications, or file an abuse report—or all three. If the person does not stop, ask for help. Recognize that no one deserves to be attacked online. If you hurt others, this will damage your reputation and friendships. If you see someone being harmed, provide support to that person and speak up against the harm. If the
situation is serious or continues, report to a responsible adult.

**Cyberdate Safely. Avoid exploitation and abusive relationships.**

- **Watch out for fantasy relationships.**
  - Recognize that forming close personal relationships primarily through digital technologies can lead to unrealistic understandings and expectations.
  - Proceed with caution when forming a relationship digitally.

- **Avoid exploitation.**
  - People you communicate with online may try to exploit you sexually by asking for nude photos or seeking sexual encounters. They may be online strangers or people you know—adults or other teens. Sexual relations between adults and teens are illegal. Common grooming techniques involve sending overly friendly messages and being overly eager to establish a close relationship. If you send a nude photo to anyone, that person could, at any time, distribute the photo to everyone, and your reputation will be trashed or the person could use that photo to blackmail you.
  - If someone appears to be trying to manipulate you to engage in sexual activities or requests a nude photo, discontinue contact and report this to an adult.

- **Do not allow a partner to abuse you.**
  - An abusive partner may try to use digital technologies to control you by constantly texting and controlling your digital communications with others.
  - Do not allow a partner to seek to control you in this manner.

**Embrace Civility in the Digital Age**

Embrace Civility in the Digital Age (a program of Center for Safe and Responsible Internet Use) promotes approaches that will best ensure all young people become cyber savvy and that seek to address youth risk in the digital age in a positive and restorative manner. Web site: http://embracecivility.org 
E-mail: info@embracecivility.org