Digital Citizen News - September 2018

Volume 2 : Issue 01 - September 2018

Greater Southern Tier BOCES

We are celebrating the 2nd year of our Digital Citizenship Initiative.

#I_AM_A_DIGITAL_CITIZEN

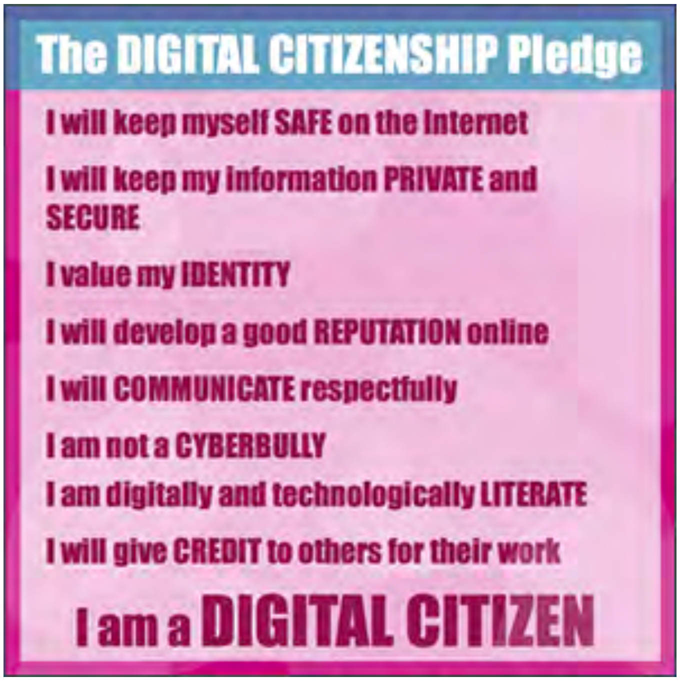
Being a good Digital Citizen requires knowledge of many related topics. Our monthly newsletters will continue to raise awareness of current issues with short articles and links for parents, teachers, and students in the following areas.

- DIGITAL ACCESS
- DIGITAL COMMERCE
- DIGITAL COMMUNICATION
- DIGITAL ETIQUETTE
- DIGITAL LAW
- DIGITAL LITERACY
- DIGITAL SECURITY
- DIGITAL RIGHTS AND RESPONSIBILITIES
- DIGITAL WELLNESS

NEW TO DIGITAL CITIZENSHIP ?

START HERE

A good place to start would be to look at our **DIGITAL CITIZENSHIP** pledge. The pledge is a series of positive statements that touches on several of the nine component areas listed above.



The DIGITAL CITIZENSHIP Pledge

I will keep myself SAFE on the Internet

I will keep my information PRIVATE and SECURE

I value my IDENTITY

I will develop a good REPUTATION online

I will COMMUNICATE respectfully

I am not a CYBERBULLY

I am digitally and technologically LITERATE

I will give CREDIT to others for their work

I am a DIGITAL CITIZEN

You can download a printable PDF of the pledge using this URL **http://go.gstric.org/201-100**

Sign Up to receive this newsletter in your email inbox.

Scan this QR code with your phone, or go to http://go.gstboces.org/dcnews-signup in your browser.

PROTECTING YOUR INFORMATION

One of the most important ways to protect your information and identity online is to learn and practice GOOD PASSWORD HABITS.

Here are some tips for creating passwords:

1. You want to create a password that someone can't guess easily (like a birthdate or pet's name).
2. You want to create a password that you can remember easily.
3. You should change your password regularly. (some systems may actually force you to change it on a certain schedule or interval.)
4. You do not want to use the same password for all of your accounts. (You may need to use a password manager program to keep track of them.)
5. Wherever possible use **Two-Factor Authentication**.

For more password tips, go to **http://go.gstric.org/201-101**

What is Two-Factor Authentication (2FA) ?

Two-factor authentication adds a second level of authentication to an account log-in. It requires the user to have two out of three types of credentials before being able to access an account.

The three types are:
Something you know, such as a PIN, password or a pattern.
Something you have, such as an ID card, phone, or key fob.
Something you are, such as a biometric like a fingerprint or voice print.

Source: **http://go.gstric.org/201-102**

DIGITAL SECURITY and DIGITAL LITERACY

ASK THE IT GUY

Making Yourself AWARE of MALWARE

What is Malware?

WikiPedia article on Malware: **http://go.gstric.org/201-103**

The term malware is short for **malicious software**, software that is designed to cause damage to a computer or computer network. The software can take many forms and includes programs also knows as trojan horses, ransomware, spyware, adware among other terms. Sometimes the malware is innocently downloaded by an unsuspecting user who believes it to be it to be legitimate. Malware may also be installed by rogue or infected web sites. Many types of malware are difficult to uninstall and may require special software to help the user remove it from their computers. Fortunately, many of the well-known antivirus software companies provide products that can search for, detect, and remove malware. (see below)

Popular Anti-Malware Software

Spybot Search & Destroy - https://www.safer-networking.org/private/
ComboFix - https://combofix.org/
MalwareBytes - https://www.malwarebytes.com/
HijackThis - https://sourceforge.net/projects/hjt/
SUPERAntiSpyware - https://www.superantispyware.com/

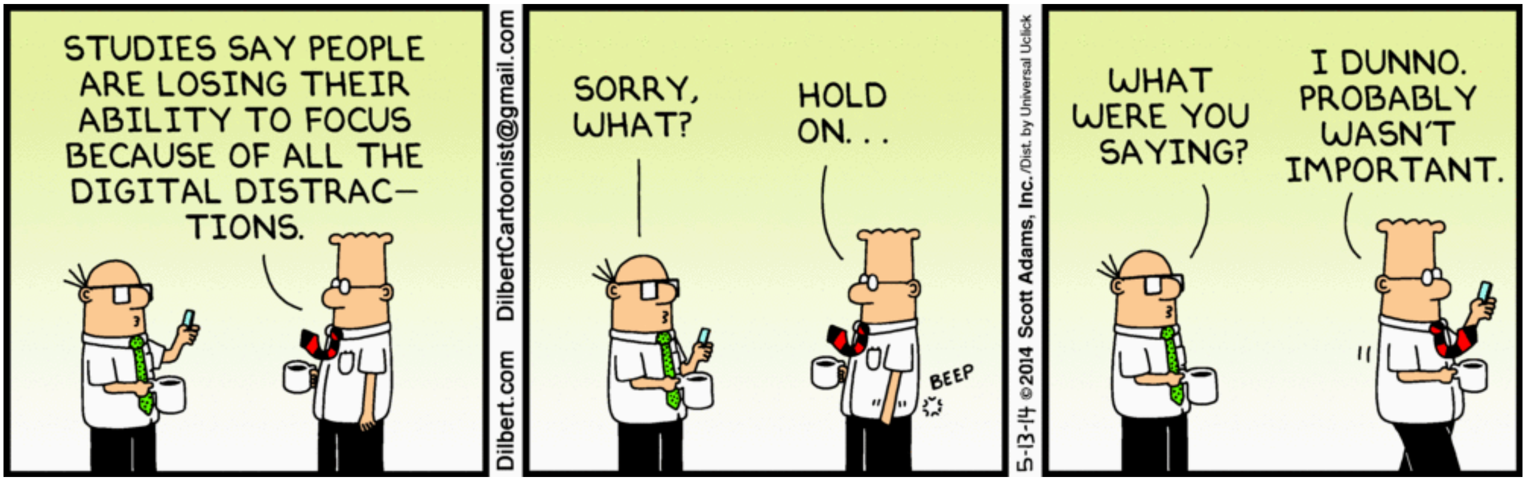
RANSOMWARE IS ON THE RISE AND CAN BE EXPENSIVE

Ransomware is software that locks the computer so that the user cannot access any information or data until a ransom is paid.

Criminals are making lots of money from ransomware. Individuals have paid 100s of dollars to get their data back, companies and school districts have spent thousands of dollars to unlock their systems.

More on ransomware: **http://go.gstric.org/201-104**

The best strategy for dealing with Malware is to keep your computer system and software up to date with security patches. GST BOCES regularly updates computers and devices on its network. Make sure that your home computer has some kind of anti-virus / anti-malware installed and that you update it often.


STUDIES SAY PEOPLE ARE LOSING THEIR ABILITY TO FOCUS BECAUSE OF ALL THE DIGITAL DISTRACTIONS.
DilbertCartoonist@gmail.com
Dilbert.com
SORRY, WHAT?
HOLD ON. . .
BEEP
5-13-14 ©2014 Scott Adams, Inc./Dist. by Universal Uclick
WHAT WERE YOU SAYING?
I DUNNO. PROBABLY WASN'T IMPORTANT.

Do You Experience Digital Distraction in your daily life?

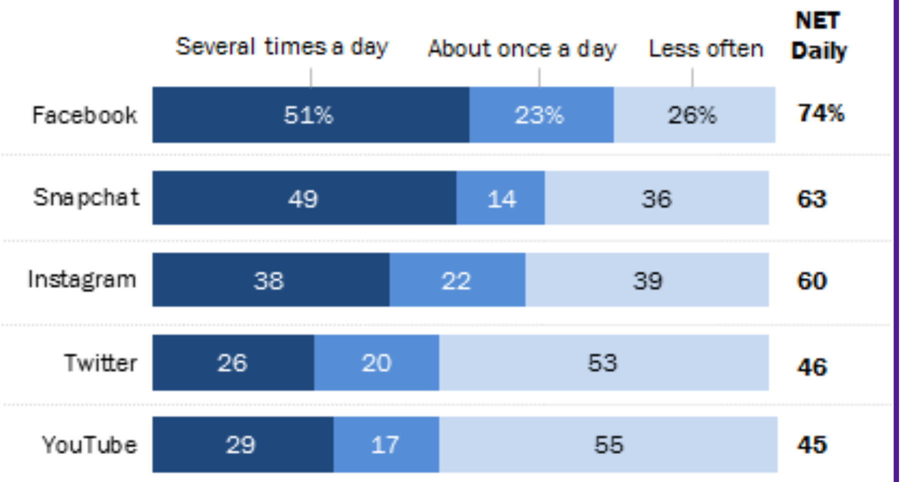
Source: **http://go.gstric.org/201-105**

What can you do to strike a balance between staying connected and letting technology take over your life? Here are some simple ideas of how to cope.

1. Create a “tech blackout” day once a week.
2. Set boundaries for text-free spaces and times.
3. If you can’t disconnect, relocate. Bring your gadgets into a shared space.
4. Turn off notifications and set times to answer email just a few times a day.

DIGITAL ACCESS STATISTICS
PEW RESEARCH CENTER

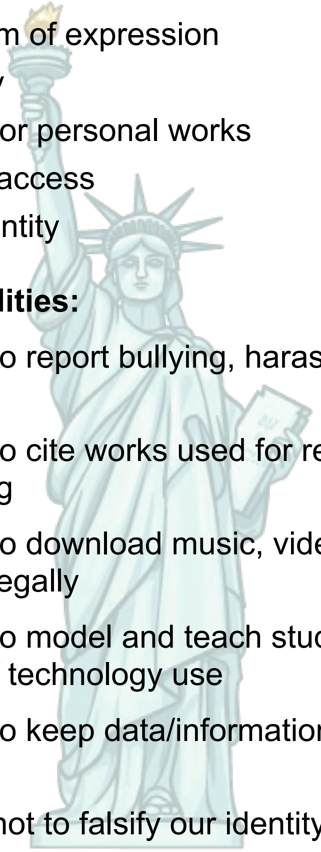
A social media use report compiled by the Pew Research Center in 2018 finds that Youtube and Facebook are the most used social media sites with 73% and 68% of users. They were followed by Instagram, Pinterest and SnapChat at 35%, 29%, and 27% respectively.



This graph shows the percentages of users that use each site daily or multiple times a day.

Source: **http://go.gstric.org/201-106**

MORE RIGHTS and RESPONSIBILITIES



Digital Rights:

- Right to freedom of expression
- Right to privacy
- Right to credit for personal works
- Right to digital access
- Right to our identity

Digital Responsibilities:

- Responsibility to report bullying, harassing, sexting, or identity theft
- Responsibility to cite works used for resources and researching
- Responsibility to download music, videos, and other material legally
- Responsibility to model and teach student expectations of technology use
- Responsibility to keep data/information safe from hackers
- Responsibility not to falsify our identity in any way

Source: **http://go.gstric.org/201-107**

THE BEST OF DIGITAL PARENTING

Do you know what your children are doing online? Who are they talking to? What apps are they using? What social media sites do they frequent?

If you are very lucky you have a great relationship with your kids and you can talk openly about these questions. However, most young people don't like to feel that their parents are monitoring their activity on their computers and devices. Some kids see it as an invasion of privacy and they resist talking about their activities. Even the most honest children may not tell you absolutely everything they are doing.

Parents may be uncomfortable talking to their children about technology use because they feel that they don't understand the technology, or they don't want to start a confrontation with the kids.

It is important to know that kids need to have their parents checking up on them because they may not yet have the judgement or skills to keep themselves out of dangerous situations.

There are many software programs and apps that can help parents keep track of what their children are doing. Some of these apps can filter or block access to web sites with inappropriate content. Others can be set to restrict the times that they can use certain apps, or can give them a time limit for game playing or social media. Often parents can create reports or receive notifications from these apps.

The apps range in cost from free to inexpensive one-time fees to monthly or yearly subscription costs per device. As with the purchase of any app or software program, make sure to do your homework. Check the features and online documentation. Look for reviews from users who have actually used the program. Ask if they have a free trial period.

DIGITAL ETIQUETTE

Build a mini-lesson plan for Middle School or High School students

Use the GST BOCES online resource **Technology Use Scenarios** to lead a discussion with your students.

1. Go to **http://www.gstric.org/digital-citizenship/scenarios/story_html5.cfm**
2. Click through the list of scenarios and choose 1 or 2 that are appropriate for the level of your students. You may modify the scenarios to make them more realistic for your students.
3. Read the scenario to the students and ask them to consider several questions while they are listening to it.
4. Lead the class through a discussion, or split them into smaller discussion groups and then have them report out to the whole group.

Some questions you can have them discuss are:

Could this scenario happen in our school or school district?
Does our school have a policy addressing this issue?
What issues/consequences might this cause?
How could this scenario have been avoided?

More sample questions are available in the scenario resource.

BLUE LIGHT SPECIAL?

I DON'T THINK SO - MORE STUDIES SHOW HARMFUL EFFECTS FROM BLUE LIGHT GIVEN OFF BY DEVICES.

This article from the FAST COMPANY online magazine looks at a new study published by Scientific Reports that shows our blue-tinted display screens are slowing blinding us. **http://go.gstric.org/201-108**

ISTE U

INTERNATIONAL SOCIETY FOR TECHNOLOGY IN EDUCATION (ISTE)

TEACHERS! ISTE has developed a 15-hour instructor-led course to make you comfortable creating and teaching digital citizenship lessons.

view the syllabus at http://go.gstric.org/201-109

DIGITAL PRIVACY vs. DIGITAL SECURITY

Facial Recognition Technology: Innovation or Invasion?

A New York State school district is planning to install a new security system that uses facial recognition technology to identify expelled students, sex offenders, and other known troublemakers entering their school buildings.

The system compares the faces of entering students against a database of known local individuals who should not be allowed in the schools. The district says that the system does not store images of other students or district employees and doesn't infringe on student privacy.

The New York Civil Liberties Union has sent a letter to the New York State Education Department asking them to bar school districts from implementing this kind of technology because it is invasive to student privacy and is prone to false-positive errors.

Parents and Teachers how do you feel about this new technology? Would you like your school district to implement this in your schools? What do you feel are the pros and cons for your school?

We would like to know what you think - send us an email at dc@gstboces.org. Put "Facial recognition" in the subject line.

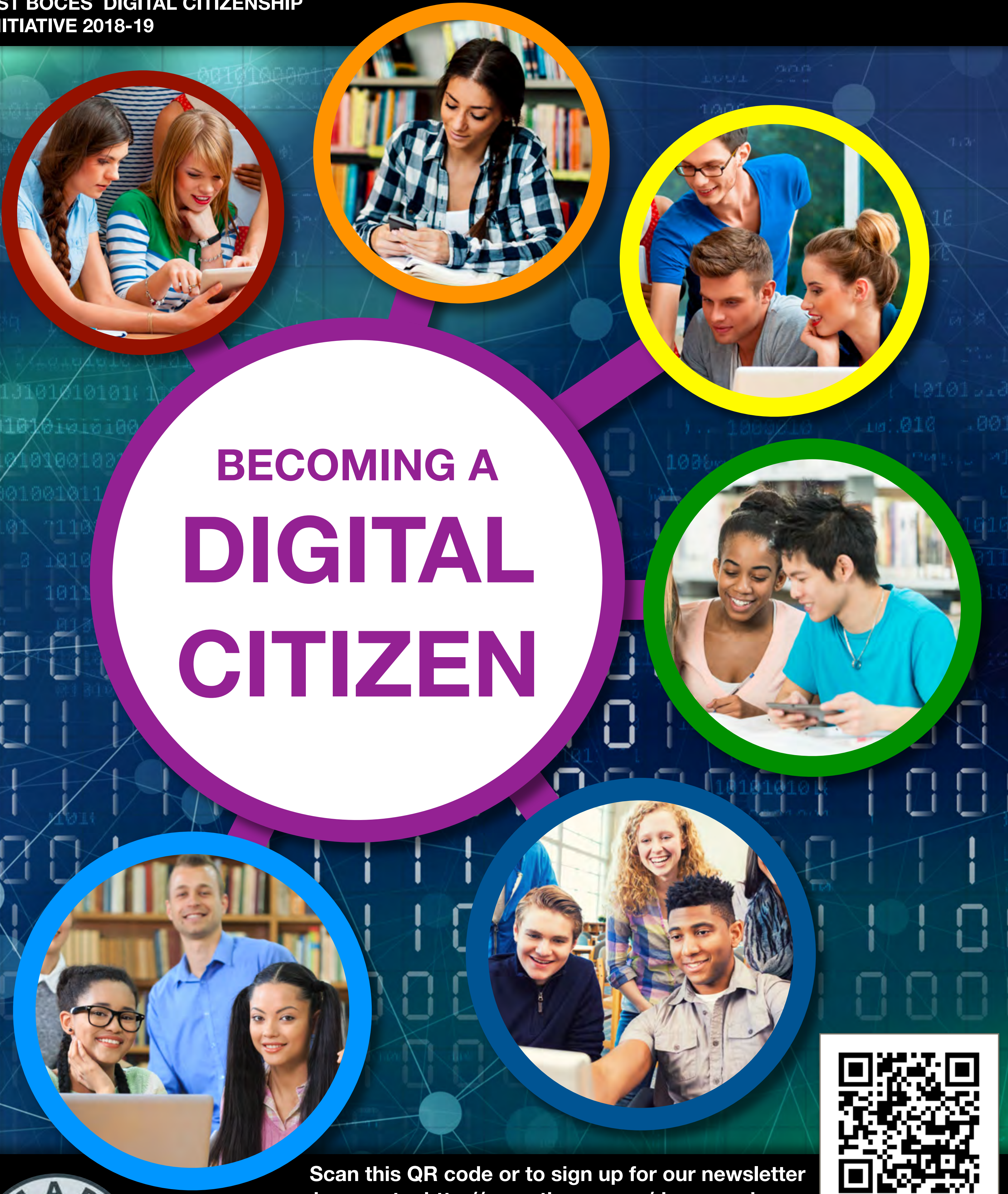
About the GST BOCES Digital Citizenship Initiative

This initiative began during the 2016-17 school year after technology survey results showed that very few students and staff were knowledgeable about Digital Citizenship topics and practices. Students also indicated that they had not received any direct instruction about Digital Citizenship. GST BOCES Computer Services and Instructional Support staff met and agreed to create this initiative to help raise awareness of Digital Citizenship in all of our component districts and to provide resources for students, parents, teachers, and other district staff to learn knowledge and best practices.

The initiative has a website at **http://www.gstric.org/digital-citizenship** (the shortcut **http://dc.gstboces.org** also works.) From the website you access downloadable resources and a blog with news and reviews of Digital Citizen topics.

I AM A DIGITAL CITIZEN

GST BOCES DIGITAL CITIZENSHIP INITIATIVE 2018-19



BECOMING A DIGITAL CITIZEN

Scan this QR code or to sign up for our newsletter
or browse to http://go.gstboces.org/dcnews-signup

LEARN HOW TO BE A GOOD DIGITAL CITIZEN AND SHARE YOUR KNOWLEDGE WITH OTHERS AT YOUR SCHOOL

For more information visit our website at **http://dc.gstboces.org**

DC Bear says, "Being safe online is as easy as ..."

A. Asking a Parent or Teacher before going online.

B. Being polite to others you meet online.

C. Courtesy is always cool.

YOU'RE NEVER TOO YOUNG TO BE A GOOD DIGITAL CITIZEN

GST BOCES Digital Citizenship Initiative 2018-19

Sign up for our monthly newsletter at **http://go.gstboces.org/dcnews-signup**

For more information visit our website at **http://dc.gstboces.org**

I AM A DIGITAL CITIZEN