I AM A DIGITAL CITIZEN 4.7

Digital Citizen News March 2021

MARCH IS WOMEN'S HISTORY MONTH

Volume 4 : Issue 7 - March 2021

This month we focus on Digital Reputation

This month our main topic is **Digital Reputation.**

This is important for **Good Digital Citizens** to consider and is closely related the the topics of **Digital Privacy** and **Digital Security**.

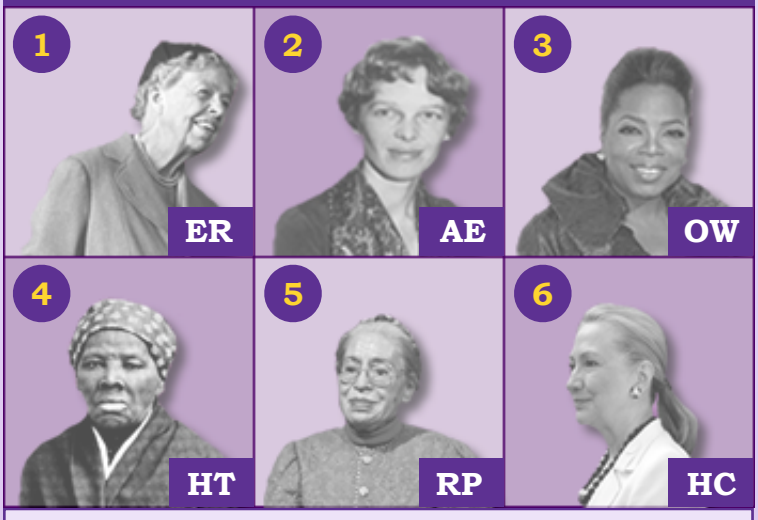
So what is your **Digital Reputation**? It is **all of the information** that someone can find if they were to search for **your name online**.

Is it easy to find **personal information** about you like where you live, what school you go to, or where you work? Can someone find **what you ate last** night? Or **where you are** shopping right now?

Have others posted things about you on **social media**? Are they **positive** messages? Or do they put you in a **bad light**?

(Continue reading about digital reputation on page 3.)

WOMEN IN HISTORY - WHO ARE THEY?



WHO ARE THESE WOMEN? WHAT ARE THEIR ACCOMPLISHMENTS?

Use your Digital Citizenship Detective Skills to identify these women. We've included their initials in the bottom right corner of each image to help you on your way. Let us know what you learn. Visit http://dc.gstboces.org

#ChooseToChallenge

International Women's Day March 8th, 2021

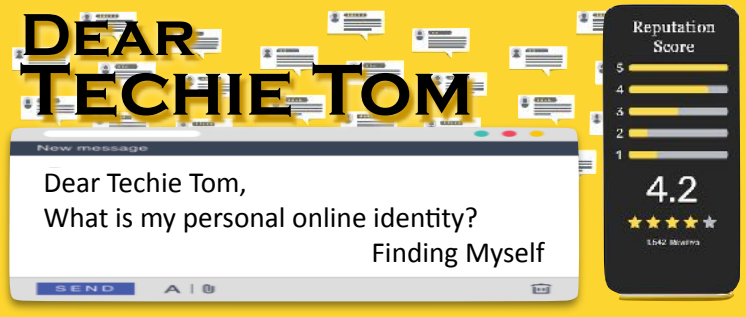
MISSION: To celebrate digital advancement and champion the women forging innovation through technology

"Technology is way too important for women to be excluded from its development and use."

Int'l Women's Day site - http://go.gstric.org/407-IWD

Selfie Card Activity - http://go.gstric.org/407-selfies

DEAR TECHIE TOM



Dear Finding Myself,

Your personal online identity is anything you put online. You need to be careful with this data because it could be stolen or sold to do harm to your digital reputation. Things you can do to keep yourself safe is to never use your home address or phone number when signing up for something, being mindful that anything you put on the internet is always on the internet even after you delete it and check your privacy settings on any accounts you may have. You should also always read the privacy statements for any accounts you may have. Even if they say they are safe and secure often they are using data in some way. Remember free accounts are free for a reason! Stay Safe!

Techie Tom

THIS MONTH'S DISTRICT SPOTLIGHT

"Roomers" and "Zoomers" Learning Together

Elmira City School District

Investing in Relationships and Experiencing How to Interact in an Online Environment

In our current pandemic world, many districts are moving toward a model referred to as concurrent teaching. This method of teaching is bringing our virtual and in-person learners together, allowing them to connect, collaborate and learn together in real time!

For this month's Digital Citizenship Spotlight, we will highlight Shelley MacPherson, a third grade teacher at Hendy Avenue Elementary School in Elmira, NY. Mrs. MacPherson, who describes herself as "the least techie person", considers why she and her students are so successful with this model of Roomers and Zoomers learning together. See four of her insights below.

By having clear expectations on how to interact in a respectful and positive way online, Mrs. MacPherson and many more amazing and hard-working teachers are setting the stage for these students to understand and build a positive Digital Reputation.

Time has been invested in checking in on student social and emotional health.

Mrs. MacPherson and her student teacher, Mrs. Romeo, who is a Zoomer spend their Morning Meeting time having ALL students share how they are feeling based on the emoji icons shared on the teacher's screen.

Clear protocols are in place and time has been invested in classroom management!

A "Roomer" was rewarded immediately with a silent cheer from Zoomers when she shared her happy feeling about the act of kindness she did that morning (which was giving everyone in-person a picture to color). The zoomers reaction was part of the regular classroom protocol.

An amazing team of teachers working together with no fear of asking questions!

Mrs. MacPherson is not afraid to ask technical questions to build on her understanding of technology, and credits her amazing team of teachers with helping to build her confidence with technology.

Nurturing Positive Relationships are

HUGE!

Mrs. MacPherson has had the benefit of these students looping with her for multiple years. "No matter what is thrown our way, including COVID and quarantining, you have to have positive relationships for student success and growth."

A FEW MORE THOUGHTS ABOUT PROTECTING YOUR REPUTATION ONLINE

CONTINUED FROM PAGE ONE

Your Digital Footprint, which we have written about many times, is all of the little bits of information that you leave behind as you use browsers, apps, and digital devices.

What does your Digital Footprint or Digital Reputation say about you?

Does it represent you in a fair way? Is it something that you would be proud of? Would you be embarrassed by anything that you have posted? Are there any images that don't reflect your current intellectual, or maturity level?

Has anyone deliberately posted something to try to make you look bad? If a future employer did research on you, what would they find? Would they hire you?

Do you judge other people by the information that you see posted about them online? Or do you keep an open mind about people until you have gotten to know them?
Finally, would someone be able to track you by following all of the little pieces of information that you give freely online?

Try to manage what is available in your digital footprint. Use privacy settings, delete items and close old social media accounts if they don't show you in a positive light.

Tips for protecting your digital footprint http://go.gstric.org/407-footprint

New York State Education Law Section 2-d & What it Means for You

Last month's issue had a short article introducing NYS Ed Law 2-d. We follow up this month by providing a few more details about this important addition to education law in New York State.

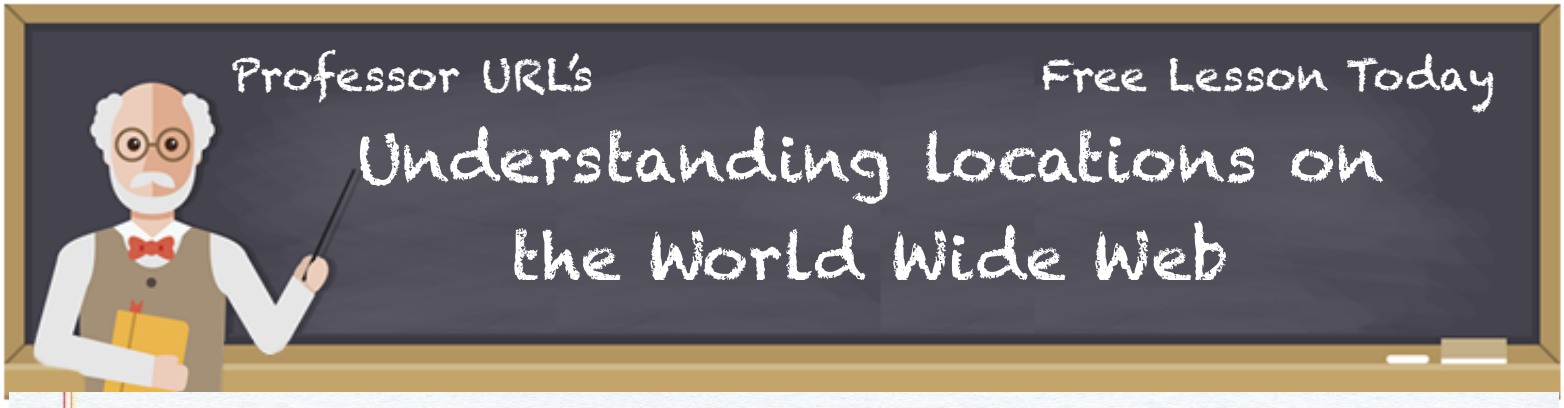
Digital data is everywhere and is being created at a dizzying pace. It is important as an employee of an Educational Institution **that you know and understand your responsibility for protecting data** and adhering to State and Federal laws.

In 2014 New York State implemented Education Law Section 2-D which addresses the **unauthorized release of personally identifiable information**. In January 2020 section §121.7, Training for Educational Agency Employees, was approved as part of the NYS Education Law Section 2-D law. It states that **"All staff must receive annual training on Data Privacy and Security Awareness."**

GST BOCES provides a self-paced online interactive training, including audio narration, to meet this new requirement. This training offers an opportunity to learn about State and Federal **laws protecting personally identifiable information**, and **what districts and employees must do to comply with such laws**. Part 2 introduces the **concepts of Phishing, Business Email Compromise and other malicious attempts** to gain your network credentials. Part 3 **outlines Best Practices and offers privacy and data security tips** for use not only at school but home as well. Your district decides which of the three parts are required and the training will track your progress.

Links about NYS Education Law Section 2-d

GST BOCES Data Privacy and Security Training site - http://go.gstric.org/407-gst-dps
NYS State Education Law site on NY Senate website - http://go.gstric.org/407-edlaw2d
NYSED site with details of Part 121 of the Education Law - http://go.gstric.org/407-part121
NYSED site with details of Parent's Bill of Rights regarding Data Privacy - http://go.gstric.org/407-billofrights



Most of us use an internet browser program to navigate the World Wide Web every day. Near the top of the browser is the location box, or as some call it, the address bar. Often we see a location that looks something like this one: (This just happens to be the address of the training for the article above.)

https://www.gstric.org/training/dps/index.cfm

protocol | host and domain name | the path to the | page content

The first part of the URL (Uniform Resource Locator - because it is uniform it can be used to address any piece of content on the web; a page, an image, a video, etc.) is the **protocol**. In this case it is **http://** (the hypertext) protocol, but you might see other protocols like **ftp://** (file transfer), or **rtsp://** (for streaming media). The next part of the URL is the **host name** and **domain name** of the server that you will be connecting to. The part up to the first dot, **www**, is a host server in our domain **gstric.org**. (We also have another domain name that we use **gstboces.org**).

The next part of the URL is the path to where the content is located on the host server. Usually it is a **list of words separated by /** ("forward" slashes - note: all of the slashes in a URL are forward slashes). These words represent directories on the server. You could think of the directories like folders on your computer. This piece of content is in a directory called **"dps"**, which is inside a directory called **"training"**, which is at the top level of that server. The path tells the where to find the content that you want. The final part of the URL is the content itself. Usually it is a filename followed by a dot and a file extension like **index.htm**. Files ending in **.htm**, **.cfm**, **.aspx** are types of **web pages**, **.gif** and **.jpg** are **image files**, **.mp4** or **.mov** are **video files**. Sometimes a URL may end with a forward slash (/). In this case the web server will look for an "index" file like **index.htm**, **index.cfm**, or **index.aspx**.

Sites can include more than just the address in the URL.

https://www.google.com/search?ei=tYIqYOq&q=url+location&gs_lcp=Cgdnd3Mtd . . .

the query string

You may see a ? (question mark) in a URL. Everything after the question mark is called "the query string". Each piece of information in the query is separated by an ampersand (&). The &q= shows the string searched for at Google ("url location").

The TLD (Top-Level Domain) or "End Domain" - in the lesson above we learned about the domain name of a web site but we didn't mention the top-level domain. Common TLDs are .com (commercial), .edu (higher education), .gov (government), .org (non-profit organizations), etc. Google has their own TLD .google. Try these domain names below.

about.google design.google safety.google teachfromanywhere.google and wellbeing.google

STAYING SAFE IN A DIGITAL WORLD

MARCH 2021 POSTER

• Keep personal information secret – your phone number, your email address, your home or school address, or the name of your school. • • Avoid using flirty or suggestive usernames. • • Use privacy settings to limit viewing of your information and enhance your cybersafety. • • Ensure all online communication is respectful. • • Only post comments you would be happy to receive yourself. • • Make sure emotions are expressed appropriately. • • Avoid posting photos which may identify any personal information like schools, or sporting teams. • • Be very aware of the risks involved of sexting. • • Understand the concept of digital archives – once an image or information is in a digital format and is live through technology, it is there for a long time. • • It's public! It is possible that many other people across the world could be watching. • • Think twice before you post – your parents, future employers (and perhaps your children) may end up seeing what you have posted. • • If you wouldn't say it face to face, then you shouldn't write it in a digital environment. • • Think before posting photos of others without their permission – you never know if it will hurt, humiliate or offend them. • • Free offers are usually too good to be true – just say no. • • Delete junk mails immediately and forget about them. • • Use strong passwords for all your accounts. • • Before you believe everything you read – make sure it comes from a reliable source. • • Do not allow anyone else to access your mobile phone. What they do might be attributed to you. • • If someone sends you a nasty, bullying message that makes you feel uncomfortable tell an adult (parents or someone you trust). • • Only Accept friend requests from people you know. • • Do not access sites that contain personal or sensitive information from public computers. •

Research tells us that cyberbullying stops within 10 seconds of peer intervention. Students who are defended online by a peer recover far more quickly from the actions of the bully. If students are aware of cyberbullying they must have the courage to take the appropriate action to ensure the safety and welfare of others.

RIC one DPS

GST BOCES Digital Citizenship Initiative
Staying Safe in a Digital World - March 2021

From a page at BEACONHILLS COLLEGE, MELBOURNE, AUSTRALIA • http://go.gstric.org/407-staying-safe