Fulton County Schools
Where Students Come First

WORKING FROM HOME Privacy and Security Tips

REMOTE LEARNING 2020 » ONWARDS

DEVICE PRIVACY

Tips to Help Keep Your Personal Information Private When Using Technology

SECURE your devices

Use strong passphrases and passcodes and/or touch ID features with screen timeouts to lock your devices. These security measures can help protect your information if your devices are lost or stolen.

THINK before you install free apps

"Free" apps make money by selling your personal and private data. Before installing, take time to read the app's permissions list and Terms and Conditions as well as users' reviews. Be thoughtful and mindful about how your data is being collected and shared.

DELETE when done

Not only does it free up more space on your devices, but it is also a good security practice to delete apps you no longer use. Unused apps make your devices more vulnerable to being attacked since they are not getting critical updates and patches that can improve the device's security and stability.

KEEP your mobile phones and apps up to date

Your mobile devices are just as vulnerable as your PC or laptop is to security breaches. Having the most up-to-date apps and operating system on your devices is your best defense against hacks, viruses, malware, and other online threats.

LIMIT what you do on public Wi-Fi

...and avoid logging in to sensitive accounts, like financial services, using these networks.

THINK before you click or tap

Cybercriminals often use current news, interesting topics, and false promises to lure you into clicking on malicious links or sharing your personal information with them. Don't fall for it! Stop and think before you click or tap.

HOME DEFENSE

Tips to Help Keep Your Information Private When Using Technology

PROTECT your home technology and Internet of Things (IoT)

...by ensuring the password on all Internet-enabled devices, such as your home Wi-Fi modem/router, Alexa/Echo, cameras and smart devices, is changed from the default manufacture setting to something not easily guessed.

LIMIT the amount of personal data you share with others

Avoid oversharing, especially on social media platforms, to reduce your cyber threat landscape.

USE online collaboration tools

...such as Microsoft's Office 365, to securely share data.

WATCH OUT for ransomware, phishing, and scam emails

Use your mouse to hover (not click) over the sender's name to validate the sender's email and over any hyperlinks to show its true URL destination. If the email sounds too good to be true, it may very well be a scam. Trust your instincts. When in doubt, it is best to delete and *not* click on any links in the email.

RECOGNIZE that all emails originating outside of the Fulton County Schools' domain...

...will include this warning message at the top of the email:

WARNING - this email originated outside of Fulton County Schools. Use extreme caution even if you recognize the sender's name. Contact ITServiceDesk@fultonschools.org with any concerns.

If you come across a suspicious email, please report it to our IT Service Desk team at:
ITServiceDesk@fultonschools.org

ONLINE LEARNING

Tips and Resources for Parents and Students

DIGITAL CITIZENSHIP is a community effort

Schools can go only so far with teaching students how to be good digital citizens, but we cannot do it alone. We need and want parents to be actively involved in their child's digital exploration while using their personal device and/or FCS-supplied device.

KEEP AN EYE ON your child...

GlobalProtect VPN is installed on student devices to filter inappropriate Internet content. Parents can verify if GlobalProtect is working on their child's FCS-issued device by opening a browser and attempting to access any unapproved FCS websites, such as www.netflix.com or www.galottery.com. If you are successful, suspect that GlobalProtect is not working and notify the IT Service Desk at TechnologyHelpDesk@fultonschools.org.

KNOW the rules

All staff, parents, and students are expected to be familiar with and adhere to the FCS policies as it relates to "**Responsible Use of Enterprise Network**" and **Digital Citizenship**. These policies and guidelines are in place to promote a safe and secure digital environment for everyone and are applicable to all FCS technology and cloud-resource offerings.

Responsible Use of Enterprise Network
https://go.boarddocs.com/ga/fcss/Board.nsf/goto?open&id=B3QJVD4E41C7

FCS Digital Citizenship Program/Resources/Guidelines
https://www.fultonschools.org/Page/1925

For Parents – Digital Citizenship/Internet Safety Tips
http://www.kathleenamorris.com/2019/05/16/internet-safety-parents/

VTC TECHNOLOGY

Video Teleconferencing, Device, and Online Usage Safety Tips

Many of us have become increasingly dependent on video teleconferencing (VTC) platforms, such as Microsoft Teams, Zoom, Skype, GoTo Meetings, Cisco WebEx, etc., to stay connected during the COVID-19 pandemic. Lately, much of the buzz has been about Zoom with multiple FBI reporting of hijacked conferences being disrupted by pornographic and/or hate images and threatening language.

Not using proper security precautions or enabling the security features when using these collaboration platforms could cause unwanted guests to gain access to your conference with grave consequences. Here are tips to help mitigate VTC hijacking threats, so incidents – like what Zoom's users experienced – can be prevented:

DO NOT make meetings or classrooms public

Require a meeting password or use the waiting room feature and control the admittance of guests.

DO NOT post or share the link to a teleconference or classroom

Only invite the intended guest(s) and include a message to *not* share the invite.

MANAGE screensharing options

Setting the screen sharing to "Host Only" gives you sole control of what is seen on the screen and prevents others from sharing random content.

ENSURE you are using the most updated VTC or web portal

You cannot be protected if recently released updates to patch security flaws are not installed on your devices.

Share your Remote Learning stories with us: **#FCSRising**