Susmita Roy Chowdhury
Fulbrighter and Global Educator

"PROTECTING YOURSELF and YOUR STUDENTS ONLINE"

The Need for Online Protection

With the rise of technology in the classroom, protecting yourself and your students online has become a crucial aspect of modern education. Schools and educational professionals now rely on digital tools for teaching, communication, and management. However, this digital integration comes with multiple risks of cyberbullying, identity theft, and data privacy issues are just a few of the challenges educators face.

For Educators, creating a safe digital environment is not only about preventing threats but also about fostering a sense of responsibility, awareness, and digital literacy. For teachers, it's about understanding these risks to protect personal information and model safe practices for students. For students, it's about teaching the skills they need to navigate the internet responsibly. Both teachers and students need to understand the risks and learn how to navigate online spaces responsibly. Let's examine these concepts through real-life case studies that highlight the importance of online protection for both educators and students.

Understanding Online Risks

Cyberbullying

Cyberbullying can take various forms, including harassment, impersonation, or spreading false information. Cyberbullying incidents can lead to severe emotional distress and, in extreme cases, legal consequences.

Case Study 1: Cyberbullying in a Middle School Setting

Situation:
At a reputed Private School in Kolkata, West Bengal, an eighth-grade student created a private social media group where classmates posted hurtful comments about each other.

Initially, the students believed it was harmless fun. However, as the comments escalated, one student felt targeted and humiliated, which led her to withdraw from classes and avoid social situations altogether.

Response:

The school addressed the situation by holding sessions on digital citizenship and the consequences of cyberbullying. They introduced guidelines about appropriate online conduct, emphasizing the importance of empathy, respect, and awareness of others' feelings. Students also participated in workshops to learn about safe online practices, setting up privacycontrols, and understanding the legal consequences of cyberbullying.

Outcome:

The case highlighted for students and staff alike how cyberbullying can harm mental health and disrupt the school environment. The students involved in the incident gained a deeper understanding of responsible digital behaviour, and the school subsequently updated its policies on digital conduct and strengthened online monitoring measures.

Takeaway:

This case underscores the need for schools to educate students about the impact of their online actions and to foster a respectful digital environment. Teaching students to recognize cyberbullying and to be mindful of others online can prevent harm and encourage responsible online behaviour.

Link: https://www.unicef.org/end-violence/how-to-stop-cyberbullying

https://www.stopbullying.gov/cyberbullying/prevention

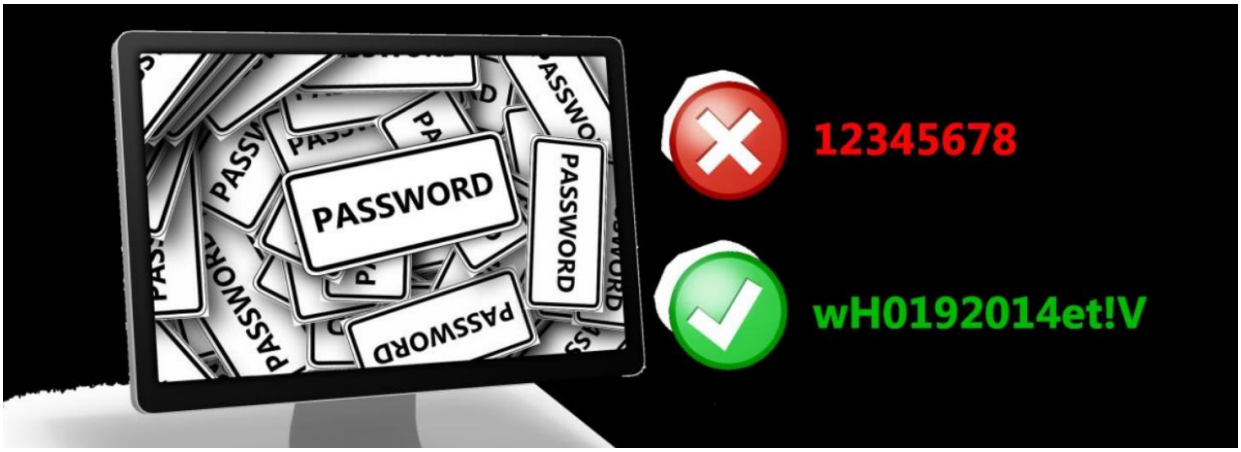
Digital Literacy and Cyber Awareness Programs both for students and teachers:

- **Cybersecurity Training**: Implementing training programs to help students and teachers understand online threats, such as phishing, malware, and social engineering.
- **Privacy Education**: Imparting training to students and staff about protecting personal information and understanding privacy settings on social platforms and learning management systems.
- **Critical Thinking**: Encouraging critical thinking around information sources to help students recognize credible information and avoid misinformation.

Password Management:

A password is typically a secret string of characters, usually used to confirm a user's identity.

By verifying the password, a system can differentiate between authorized and unauthorized user before giving access to a resource. Your password is your first line of defence against hackers and unauthorized access to your accounts. The strength of your passwords directly impacts your online security. The following are the best practices for your password management



Create strong password with a minimum length of 10characters using the combination of letters, numbers and special characters such as! @ #$ % ^ & * . Remember weak passwords are a gift to criminals

- Never use common pattern of alphabets and numbers such as abc123, 12345678, 777, 654321etc.
- Don’t use common easy-to-guess passwords such as nick names of self, friends, family members, pets name, favourite player name, birthday of anyone, birth year, etc.
- Do not use computer names or account names.
- **Do not use dictionary words** like sunshine, monkey, or football or names in any languages. Try combining two or more unrelated words.
- Switching a letter for a symbol such as p@ssword is an obvious trick hackers know well.
- Avoid common or famous statements, for example, lyrics from a popular song.
- Using the same password for all your online accounts is like using the same key for all your locked doors. **Don't use the same password** for multiple accounts, especially for the most sensitive ones, such as bank accounts, credit cards, tax records etc. Even if one password gets hacked, your other accounts will not be compromised.
- Since we all have more than one online account, and each account having a unique password, there will be a lot of passwords to remember. The best solution is to use a **password manager.** A password manager stores and encrypts all of your different

and complex passwords and help you to log into your online accounts automatically. You only need to remember your master password to access the password manager.

- **Don't reuse old passwords**. Re-used passwords are easier to crack through observing key-log patterns or through social engineering.
- Use **Passphrase** Rather Than a Password. Choose a meaningful statement rather than a word. The longer length makes passphrases less vulnerable to brute force attacks.
- Be very careful while entering passwords in front of others. Improve **typing accuracy** so that you can enter password quickly before anybody can follow the keystrokes.
- **Never select the "Save password"** option prompted by your web browser. There are many websites that prompts you to save your login credentials or payment detail for future use. **Decline to them**.
- Don't store the passwords in readable form in computers, notebook, notice board etc.
- Never disclose any password with anyone. Change your password immediately if you suspect that it has been compromised.
- You can check the strength of your password and how long it would take to crack your password at https://howsecureismypassword.net or at other similar sites like https://password.kaspersky.com or https://www.my1login.com/resources/password-strength-test

PASSWORD DO'S AND DON'TS	
DO'S	**DON'TS**
Do combine two or more unrelated words. Change letters to numbers or special characters.	**Don't** use the word "password," or any combination of it. "P@ssword!" is easy for hackers to guess.
Do make your passwords at least 8characters long. Aim for 12-15 characters.	**Don't** use short, one-word passwords, like sunshine, monkey, or football.
Do use a combination of upper- and lower-case letters, numbers, and symbols.	**Don't** place special characters (@, 0, etc.) only at the beginning or at the end.
Do include unusual words only you would know. It should seem nonsensical to other people.	**Don't** include personal information like your birthdate, address, or family members' names.

Case Study 2: Phishing Attack Targeting Teachers

Situation:

In 2021, teachers at a high school in Texas received an email that appeared to be from the school's IT department. The email requested login details for a "mandatory system update" and included a link to a fake login page. Several teachers unknowingly entered their credentials, resulting in compromised accounts. The breach allowed hackers to access confidential information, including grades, student records, and internal communications.

Response:

Upon discovering the phishing attack, the school's IT team reset passwords and conducted a full audit of affected accounts. They also implemented mandatory multi-factor authentication (MFA) for all school accounts, adding an extra layer of security. In response to the incident, the school organized a cybersecurity awareness program, teaching educators and students about phishing, suspicious links, and how to recognize scams.

Outcome:

This case illustrated the importance of cybersecurity training for staff and students. By learning to identify phishing emails and being vigilant about email security, the school community became more informed and better protected against future attacks.

Takeaway:

Phishing attacks can have severe consequences, especially in education settings where confidential information is at stake. This incident emphasizes the importance of continuous cybersecurity education and practical measures, like MFA, to strengthen online security.

Links of resources to know more about the topic:

https://www.cloudflare.com/en-gb/learning/email-security/secure-email-gateway-seg/

https://safebrowsing.google.com/

https://www.dnsfilter.com/

Strong Authentication Protocols:

- **Multi-Factor Authentication (MFA):** Use MFA for logging into school accounts, especially for accessing sensitive data. This adds an extra layer of security.
- **Secure Password Policies**: Encourage the use of unique, strong passwords for school accounts and guide students on using secure password management tools.

Phishing and Online Scams

Phishing attacks is "a technological medium to exploit human weaknesses" and that technology cannot fully compensate for human weaknesses. Every day, millions of emails and messages are sent to communicate with friends and conduct business. Criminals also send fraudulent emails containing malicious links and attachments, pretending to be from a legitimate sender and with a valid important reason. Phishing attacks involve tricking individuals into providing sensitive information like passwords or bank details. These attacks are common and can cause significant damage if students or staff fall for them.

However, there are different techniques to identify phishing attempts and you can follow the best practices to prevent the phishing attacks.

Best Practices for Emails, Messages, Attachments and Links:

Many companies, services, apps, and websites ask for your email. But it’s not always required.

- For example, many online shopping portals allow you to check out as a guest. Don’t create an account if it’s not required.
- If a website requires an email address, use services like 10minutemail or getnada, which allow you to create a temporary one.
- Create a different email to sign up for promotions and newsletters.
- Don’t include personal information that could be used to identify you in that email address, like your name or birthday.
- One of the top techniques used by hackers is to create an email with a familiar name. Check the sender’s name. Are there unusual initials, spaces or misspellings in the person’s name?
- Always double check the e-mail sender's address. Even if you know the name of the person, verify if it is the correct e-mail address.
- Fake or scam emails are always sent from a random private email address which do not belong to the official domain of any reputed organisation, bank or business. Check the domain of the email.
- Look for the manipulated domains. Check for the spelling of the domain, likeemail@domian.com
- Do not open emails from unknown sender which do not seem relevant to any ongoing official communication.

- Doubt all unexpected emails because they want to target a big audience, criminals send phishing emails which are often not personalised to the recipient and rarely use your name. Check the greeting phrase.
- Review email content. While scammers are getting better at making their messages look more professional, but lack of consistency is very common in their emails, like odd spacing, different font styles or sizes, poor spelling and grammar or mismatching logos. Interestingly enough, the poor grammar is used purposefully to filter out the more cautious prey.
- Emails from banks and credit card companies often include partial account numbers (usually last 4 digits). If you are contacted for verification or renew your credentials of your account through email or messages, it is sensible to contact the company directly before giving account detail.
- Criminals often exploit specific festival times of the year or ongoing big events in their scams. Be particularly careful with any emails referencing the corona virus, as these may be phishing attempts or scams.
- If you see an attachment that doesn't make sense, be cautious. Attachments may contain viruses including ransomware.
- Do not click on any attachment if the e-mail sender appears suspicious or un-trustworthy. Never open attachments unless you are absolutely sure they are coming from a validated sender.
- Do not click on any link provided on the emails (or download files) from unknown people.
- Don’t allow your e-mail programs to “auto open” attachments.
- If you have to open pdfs/docs/Excel-sheets from unknown senders, it is much better to upload them to a cloud service like Google Drive, and open via Web tools.
- Scan for and remove suspicious e-mail attachments; ensure the scanned attachment is its "true file type" (i.e. the extension matches the file header). Block the attachments of file types.
- Never click on a URL contained in an unsolicited e-mail, even if the link seems benign. In cases of genuine URLs close out the e-mail and go to the organization's website directly through browser.
- Beware of clicking on phishing URLs providing special offers like big discounts, winning prize, rewards, cash-back offers or ask you to fill up customer review form. Lucrative offers and eye-catching statements are often used to attract people’s focus.
- Avoid phone calls/ emails/ SMS regarding unknown inheritance, foreign lottery, fund

transfer requests from foreign country, etc.

- A popular tactic amongst cyber-criminals is to urge you to act quickly by using various pretexts like super deals that shall last only for a short period of time.

  Instilling this sense of urgency is meant to make you take a decision in haste, rather than after weighing its pros and cons. Avoid.
- Be sceptical, if you receive a mail or SMS from a delivery company claiming that you have missed a courier delivery and ask you to reschedule the delivery by clicking on a link and paying a little delivery charge. All online shopping / delivery service providers post the delivery information on their websites. Go to the shipper's actual website to see if the tracking number is real.
- A phishing email is not like a standard email. The cybercriminal simply wants your click, and nothing else. The Unsubscribe button won't stop the email. So don't click on the Unsubscribe button. The best solution in these cases is for you to simply mark the email as spam, this will remove the mail from your inbox and block the sender from sending more spam.
- Update spam filters with latest spam mail contents. Use specialized spam filters to reduce the number of phishing emails that reach their addressees' inboxes. These filters use a number of techniques to classify phishing emails, and reject email with forged addresses.
- While using public/ multi-user systems, make sure that you always log out before leaving the system.

Module 9: Safety Tips for Safe Browsing

- Always use pre-installed, trusted and updated web browsers like Google Chrome, Mozilla Firefox, Microsoft Edge, etc. for web-browsing.
- Consider using Safe Browsing tools, filtering tools (antivirus and content-based filtering) in your antivirus, firewall, and filtering services.
- Anyone with physical access to your computer, or your router, can view which websites you have visited using web browser history, cache, and possibly log files. This problem can be minimized by enabling the in-private browsing mode on the web browser. With private mode enabled, cookies are disabled, and temporary Internet files and browsing history are removed after closing the window or program. Most of the popular web browsers have their own name for private browser mode:
- Microsoft Internet Explorer: InPrivate
- Google Chrome: Incognito
- Mozilla Firefox: Private tab / private window

- Safari: Private: Private browsing
- Always check for genuine https and green/grey padlock symbol to ensure that you are not being re-directed toa fake website. Yellow or red https means the website is insecure.
- You may see the yellow warning triangle and the lock icon in the address bar while visiting a webpage that's secured with SSL. This means that the website uses non-secured third-party resources, like scripts or images.
- For Google Chrome, it is an indication that the browser had found insecure content on that page, either because the page contains both HTTPS and HTTP content, or because the browser detected that the website is using an obsolete encryption mechanism, such as SHA-1.
- For Firefox, a grey padlock with a yellow warning triangle indicates that the connection between Firefox and the website is only partially encrypted and doesn't prevent eavesdropping. By default, Firefox does not block insecure passive content such as images; you will simply see a warning that the page isn't fully secure.
- Sometimes Firefox shows a grey padlock with a red strike-through line over it, when the user reaches an HTTP page that contains a username+password log-on combination. A padlock with a red strikeover it indicates that the connection between Firefox and the website is either delivered using an insecure protocol (HTTP or FTP) or that it is only partially encrypted because you've manually deactivated mixed content blocking.
- Do not send any sensitive information to sites where the Site Identity button is a grey padlock with a red strike over it
- . Check the integrity of URLs before providing login credentials or clicking a link.
- Do not submit personal information to unknown and unfamiliar websites.
- If there is any known Web address in any e-mail, instead of clicking them, type them in the browser and open the site. Remember, criminals can easily fool you by faking URLs.
- Verify shortened URL. Never click on a link without knowing where the link will finally redirect you. Rather use shortened URL expander websites www.expandurl.net. The website helps users intaking an informed decision by providing the title, description and key-words of the destination webpage.
- Check for errors. Phishing websites for malicious purposes are often made hastily, therefore likely to have grammatical, punctuation, spelling or other errors.
- While browsing, always turn ON the popup blocker in the browsers.

- Avoid downloading unnecessary programs from anywhere, even from legitimate trusted sources.
- Do not use torrents or download illegal content – it is a criminal offence.
- Do not visit any illegal web-sites.
- Always avoid Public Wi-Fi for web-browsing.
- Don't do office works on Public Computers or Cyber Cafes'.
- Don't conduct financial transactions by using public computers or public Wi-Fi connections.
- Beware of Shoulder-surfing. Don't let others watch over your shoulder while logging in or doing online transactions.
- In Cyber Cafe, always use virtual keyboard while typing password or anything important.
- All documents downloaded on public computers for any reason should be permanently deleted with [**Shift + Delete**].
- Always ensure that you close and delete your browsing content when using public computers.
- While working in public computers, never forget to close all browsers and logging out from all sessions before leaving.
- For video chatting, it is always better to use Web clients inside of your browser. If you have to download and install any software, make sure that you are downloading from a legitimate website. Criminals often spoof websites and stack them with malware, which may spy into your work.
- Note that many of the well-known video-chatting services are not end-to-end encrypted. Do not share any password or authentication details over it. There is a chance that attackers can access that information.
- Remember to close all software that are not required during the web-meeting.
- Connect to the internet via secure networks. Avoid open/free networks. Most Wi-Fi systems at home these days are correctly secured, but some older installations might not be.

Case Study 3: Identity Theft Impacting a Teacher's Professional and Personal Life

Situation:

A high school teacher in Hyderabad, noticed that her personal social media profile was duplicated by an unknown person. The impersonator used her profile picture and name to

create fake accounts that reached out to students and parents, requesting personal information under the guise of "school updates." The impersonator even attempted to solicit money, claiming it was for school fundraising.

Response:

The teacher immediately reported the fake profile to the platform, which removed it after verifying her identity. However, the damage had already begun, with parents and students expressing concerns. To address the incident, the school issued a formal notice explaining the situation and advising everyone to verify all communications. The teacher also took additional steps to secure her personal information online, including enhancing privacy settings on social media accounts and using only secure school-authorized channels for all communications.

Outcome:

This incident reinforced the importance of identity protection for educators, who are particularly vulnerable to impersonation given their trusted positions. The school initiated new guidelines encouraging teachers to keep personal and professional profiles separate and to use official channels for all student and parent communications.

Takeaway:

Identity theft can have serious repercussions on an educator's reputation and relationships with students and parents. By establishing strict guidelines and keeping communications secure, educators can protect themselves and maintain trust within their school community.

Links to stop identity theft:

https://www.identitytheft.gov/

https://www.security.org/

https://lifelock.norton.com/

How To Use Social Media Safely

Social media plays a crucial role in connecting people, developing relationships, sharing ideas, thoughts and information through virtual networks and communities. Regardless of age and gender, people are making their online presence for connecting with each other in the virtual world. Some have thousands of friends and followers spread across multiple profiles.

At the same time, cyber criminals are also active in the social media platforms creating fake profiles, posting inappropriate or illegal contents, spreading fake news, and causing

harassment to legitimate users. Various un-desirable incidents of “public outrage” and “mob lynching” have happened due to the viral propagation of fake news through WhatsApp and Facebook.

But ultimately, it is the user’s responsibility to safeguard his data, identity, and his reputation. A few simple precautions may save these big problems later.

- ✓ Always use only one social media account for each platform i.e. WhatsApp, Facebook, X(Twitter), Instagram, Google Plus, etc.
- ✓ Your username or alias is your online identity and how you present yourself to others in the virtual world. The username should not include any personal information. It should be something appropriate and respectful. This username should not lead strangers to think you are an easy target for cybercrimes or unwanted attention.
- ✓ Share as little information as possible. You should not share information like your birth date, email address, or your phone number on your profile. The more personal information you share online, the easier it is for someone to create a fake profile in your name and take advantage of your identity.
- ✓ Do not fill out your social media profile completely, only provide the minimum required information.
- ✓ Do not share your login credentials with anyone.
- ✓ Set your social media privacy settings to allow only your friends to see your activities or engage in your conversations.
- ✓ Sometimes security questions like “What is your mother’s maiden name?” or “In which city were you born?” are set, which help you to retrieve your account in case you have forgotten the user name or password of an online account. Better to answer these questions with false information, as long as you can remember the false answers. If you have a problem remembering them, you can use password manager to manage them for you.
- ✓ Be cautious that social media profiles can actually be fake or honey-traps created to extract information through social engineering. Attackers often pose as genuine person and make a data theft attempt like a fair communication.
- ✓ Attractive profiles of the opposite sex may be created specifically to lure you into divulging personal information. Do not add and communicate with such profiles without verification.

- ✓ Avoid making friends with someone whom you do not know from other sources. In social media platforms only add and communicate with real persons whom you know outside of social media.
- ✓ Do not share or post any sensitive personal private information, photo or video of yourself and others in social media or through their messenger services. Once they are published on the internet they can be downloaded and used for malicious purposes by other people without your knowledge.
- ✓ Never disclose your travel plan, itinerary in social media. Criminal can stalk you and follow you with malicious intentions.
- ✓ If your vacation status updates are publicly viewable, the potential burglars can also discover how long you are going to be away and get the opportunity to rob your empty house.
- ✓ Don't share virtual meeting URLs, or screenshots from your video calls on the social media. You may accidentally be leaking information (meeting ID or other confidential information).
- ✓ All employees, contractual staff and consultants, engaged with Government offices or on Government projects should practice extra caution to maintain confidentiality of official information on social media or at any other place.
- ✓ Do not accept any image/ video or news received from social media to be true unless the genuineness has been verified by other sources.
- ✓ Do not post and forward materials which appear as a statement of some event, incident, news item, statement of fact, etc, unless there has been corroboration from trusted source.
- ✓ Do not forward any controversial communal image/video/news without verifying its genuineness or you may be criminally liable.
- ✓ Erase your digital footprints. Close all sessions and delete all your browsing history before leaving.
- ✓ If it appears that the matter in hand is serious, and may lead to some undesirable event, report to nearest police station.

Safe Online Behaviour Policies:

Acceptable Use Policies (AUPs): Develop and enforce policies outlining safe and responsible online behaviour for students and teachers. These should cover respectful communication, avoiding harmful content, and restrictions on sharing personal data.

Case Study 4: Data Privacy Concerns in a Primary School

Situation:

A primary school in New York was faced with a data breach when an unsecured school laptop was stolen from a teacher's car. The laptop contained sensitive student information, including names, medical records, and emergency contact information. Without encryption or password protection, the information was at high risk of misuse.

Response:

The school took immediate action by notifying affected families and working with law enforcement to try to retrieve the laptop. They also mandated that all staff encrypt their devices, use password protection, and store confidential data only on school-managed, secure cloud platforms. In addition, they provided teachers with training on proper data handling and security protocols.

Outcome:

The breach brought attention to data privacy and the need for strict security measures, especially when dealing with sensitive student information. Following this incident, the school implemented stronger cybersecurity policies, including guidelines for securely transporting and storing data outside of school.

Takeaway:

Data privacy breaches can cause serious concerns and disrupt the trust between families and schools. This case emphasizes the importance of secure data handling practices and training teachers to be vigilant about protecting student information

Links for keeping Data safe:

https://onerep.com/

https://www.torproject.org/

https://1password.com/

Protecting Your Data and Device Safe:

Always use genuine software and operating system. Do not download and install pirated software or anything else from random sites off the Internet. Many of them are malware ridden.

- **Firewalls and Filtering:** Use firewalls, VPNs, and web filtering tools to block harmful websites, restrict access to potentially dangerous content, and prevent unauthorized access.
- **Device Security:** Ensure that devices used in the classroom are updated with the latest security patches and antivirus software. Discourage the use of personal devices for accessing school networks unless they're also protected.
- **Controlled Access**: Limit access to sensitive data (grades, health information, etc.) based on roles, ensuring only authorized personnel can view or modify this information.

✓ **Vetted Educational Tools:** Use trusted and secure educational platforms that prioritize student data privacy. Avoid apps and websites that collect unnecessary information.

✓ Do not keep any applications or software which you do not require regularly.

✓ Always use device specific licensed Anti-virus and run virus scan on regular basis. Never go for installing free Anti-virus software available in the internet.

✓ Keep the Firewall On. All operating systems come with default firewalls and you should not disable them. They are essential to defend against many known attacks. Whether it is a software firewall or a hardware firewall on a router, the firewall should be turned on and updated to prevent hackers from accessing your data.

✓ As and when companies find bugs in their software and OS, they also fix them by releasing regular updates. Run software and app updates as soon as they're available. These updates fix software vulnerabilities, and security problems. Turn on automatic updates.

✓ Don't leave computer unattended with sensitive information on screen. Make sure to always lock your computer screen when leaving it unattended with "windows + L" or "Ctrl+Alt+Del"

✓ Your computing devices, whether they are PCs, laptops, tablets, or smartphones, should be password protected to prevent unauthorized access.

✓ A very good idea to use Screensavers with timeout period of maximum 2 minutes.

✓ Erase/remove the contents of removable storage media after use.

✓ Protect your sensitive documents by enabling password protection on them.

✓ Do not give your phone/ laptop for use to anyone, especially untrusted people.

- ✓ The stored information should be encrypted, especially for sensitive or confidential data. Encryption is the process of converting the information into a form where an unauthorized party cannot read it. Only a trusted, authorized person with the secret key or password can decrypt the data and access it in its original form.
- ✓ If you are not in a meeting, make sure that your webcam is either taped or blocked. The microphone should always be mute. In times when private topics may be discussed, having the microphone on mute will help prevent any leaks or unnecessary sharing of embarrassing information.
- ✓ Always scan all removable media with antivirus
- ✓ Delete your data permanently. When you move a file to the recycle bin or delete it permanently, the file is only inaccessible from the operating system. Anyone with the right forensic tools can still recover the file.
- ✓ In order to erase data so that it is no longer recoverable, the data must be overwritten with ones and zeroes multiple times. To prevent the recovery of deleted files, you may need to use tools specifically designed to do just that.
- ✓ If you decide to sell your computer or mobile, reset it to Factory Setting and format repeatedly to ensure that all data have been erased permanently.
- ✓ To prevent intruders from entering your wireless network, the pre-set SSID (Service Set Identifier) and default password for the browser-based administrative interface should be changed.
- ✓ Configure the wireless router to not broadcast the SSID, which adds an additional barrier to discovering the network.
- ✓ You should encrypt wireless communication by enabling wireless security and the WPA2 or higher encryption feature on the wireless router.
- ✓ Activate MAC id filter in your wireless router to avoid unauthorized access. Every device that can connect to a Wi-Fi network has a unique ID called the "physical address" or "MAC" address. Set your wireless network to accept connections only from devices with MAC addresses that the router will recognize.
- ✓ Use a Virtual Private Network (VPN), which lets you use public Wi-Fi securely and keeps your online behaviour private. A VPN routes your connection through a secure server that encrypts your data before you land on a web page.
- ✓ Update all wireless routers and wireless capable devices, such as laptops and mobile devices, as soon as security patches become available.
- ✓ Use anti-virus and anti-spyware software on your computer, and use similar apps on your devices that access your wireless network.

- ✓ When transmitting sensitive information, use your cell phone data plan instead of Wi-Fi.
- ✓ Turn off your wireless router when it will not be in use for any extended period of time.
- ✓ Disable remote management feature in routers to protect against unauthorized access.
- ✓ IoT devices pose an even greater risk than your other computing devices. While desktop, laptop and mobile platforms receive frequent software updates, most of the IoT devices still have their original firmware. IoT devices are often designed to access to the customer's local network and data. The best way is to have IoT devices using an isolated network, sharing it only with other IoT devices.

Incident Response Plan:

- **Clear Reporting Channels:** Establish a straightforward process for reporting security incidents, suspicious activity, or privacy concerns.
- **Regular Drills and Simulations:** Conduct cybersecurity drills for students and staff to help them respond effectively in case of a data breach or online threat.
- **Cyber Safety Workshops:** Conduct workshops to educate parents about online safety and their role in helping children practice secure behaviours at home.
- **Transparent Communication:** Keep parents informed about the digital tools being used, data policies, and any security incidents that might affect their children.

Citation:

Cyberbullying and Digital Citizenship in Schools- cyberbullying.org

***Cybersecurity in Education: A Guide for Schools*-ncsc.gov.uk**

ISTE Standards for Students: Digital Citizenship-iste.org

Digital Citizenship Curriculum and Resources-commonsense.org

***CIS Controls for Educational Institutions*- cisecurity.org**

Protecting Student Privacy: A Guide for Schools and Educators- ftc.gov

Student Data Privacy and Security Toolkit- dataqualitycampaign.org
https://www.techopedia.com/

Tackling Cyberbullying in Schools: A Guide for Teachers. - edtechmagazine.com

How Schools Can Improve Cybersecurity Incident Response--unesco.org