Good Will Children Private School

Online Safety Guidelines – Parents

We encourage all our parents to read and understand the online safety guidelines and carry out healthy discussion on safe internet usage with their children.

1. Cyber Safety Guidelines

The Internet is an incredible platform for children to learn, express themselves and have fun, but it also has its dark side. Not everything on the Internet is safe and can be trusted. Even though the benefits outweigh the potential dangers, parents and guardians must be aware of the real risks that children may be exposed to online.

Top tips for Parents to keep children safe online

- **Educate**

It is important that you are aware of your child's Internet activities including the social media channels they utilize, games or other online activities they are involved in. Being aware of your child's online activities will help you identify possible threats to educate and advise your child accordingly. It is important that children understand the impact that their online activities can have on themselves and others, today and in the future.

- **Protect**

There are parental control tools available to help protect your children from harmful and inappropriate online content. Phones, tablets, game consoles and other devices that connect to the Internet have parental control settings. Technology can be effective, but no system is 100% fool proof, so education remains key.

- **Monitor**

Keep an open dialogue with your children about their use of Internet. Younger children should only use the Internet when they are in a family area so you can monitor what they are doing and how they are using it. As they grow up they will demand more privacy, but it's important to stay interested and engaged.

- **Support**

Make sure your children know they can talk to you if something goes wrong online. You also need to know how to respond to these situations. Most websites now have "report abuse" buttons where you can report inappropriate behaviour.

Good Will Children Private School

Parent Note

Please teach your children the safeguards for the above scenarios and ensure they follow the below guidelines in cases where bullying might be happening:

- Notify a parent or guardian (someone whom you trust) about the incident immediately
- Don't respond, forward or delete any of the offensive messages
- Obtain screenshots and gather as many details as possible about the profile that has been sending offensive messages
- Tell your teacher / Social worker or other trusted adult as soon as possible.

2. Guidelines on Audio/Video Conferencing

DO's

1. **Safeguard your personal information**: Your surroundings (items in the background which are in focus within the screen) could reveal a lot about you. e.g. school uniform, identity cards, neighborhood that you are in etc.
2. **Adjust security settings**: Review the security settings of the tool you are using and disable features that may be harmful or are not in use.
3. **Keep your password in secret:** Avoid sharing your passwords with other people as they can use them to act on your behalf.

DON'TS

1. **DO NOT Record/livestream people without their consent:** Recording the lectures on live sessions (Microsoft TEAMS and ZOOM) is strictly NOT allowed.
2. **DO NOT Share inappropriate content or use inappropriate language**: Some of your messages could be offensive for other people in the conference. Think twice before you send anything to group or personal chat.
3. **DO NOT invite external participants:** Do NOT invite any other student and share personal chats on Microsoft TEAMS and Zoom.

3. Guidelines on Internet Browsing

DO's

1. **Beware of pop-up scams:** Most pop-up advertisement campaigns that appear when you browse are scams. Some may also trick you into installing malware (damaging software) on your

computers.

2. **Be careful of sharing your details:** Some online services may collect and sell your personal information (including credit card details) to third parties. Refrain from sharing your personal details unless you are confident of the web platform being used.

DON'Ts

1. **DO NOT access illegal sites:** Accessing such sites or using file-sharing programs that offer free downloads of movies, music or software can expose your system to malware, violent or inappropriate images. You could also be breaking the law or committing copyright violations.
2. **DO NOT Save your passwords in the browser:** Doing this could leave you more vulnerable to being hacked.
3. **DO NOT use VPN (Virtual Private Network)**

Parent Note

Make sure your child consults with you before signing up to a new online forum, social media platform or any other service over the Internet.

4. Guidelines on Device & Online Services Security

DO's

1. **Ensure you install a trusted Anti-Malware:** This software will protect your system from majority of common computer threats. Don't forget to keep it up-to-date with product updates.
2. **Make use of parental controls:** Parental control settings are available in most of the modern smartphones and tablets. There are many parental control available in the market to access.
3. **Secure your wireless network:** Reset the router password so it follows good password rules and isn't easy to guess and enable wireless encryption to prevent a stranger from spotting your network from the Internet.

DON'TS

1. **DO NOT turn off security software:** Software such as anti-virus scanner or firewall should never be turned off.
2. **DO NOT install pirated or illegal software**: Pirated software may come cheap but you will have a hidden cost on your privacy and computer security. Always use genuine software.
3. **DO NOT use unknown Wi-Fi networks**: Data exchange between your computer and Internet can be intercepted and monitored by a cyber-criminal. Never use public Wi-Fi to access your financial

data.

Parent Note

Tell your children not to turn off the virus scanner or firewall, even if they think it might speed up a game. It's just not safe to take this risk.

5. Guidelines on Social Media & Online Communication

It is easy for cyber-criminals to create fake accounts and use them for illegal purposes. Remember, all people that you meet online are strangers, no matter how long you may have known them or how friendly they appear to be.

DO's

1. **Review your privacy settings:** Ensure your social media accounts and privacy settings are configured to be restrictive, so that your posts and personal details are only revealed to your friends and not strangers. Review your privacy settings periodically.
2. **Think before you post:** Whether on social media website, mobile apps or any other online platforms. Always take a minute to think before hitting the "Send" button.
3. **Report immediately**: If someone is making you or your child feel uncomfortable by being abusive or inappropriate, or pressurizing you or them to do uncomfortable things, block and report the user on the platform. Social networking sites provide a reporting option which you should familiarize yourself with.
4. **Use your account only**: Use your own account for Microsoft TEAMS and Zoom online sessions and on Classe365 LMS.
5. **Share your concerns with the school**: The students are requested to contact the school social worker directly in case of any online concerns and queries.

DON'TS

1. **DO NOT share your school information online:** The school has dedicated people who are authorized to share any school related information online
2. **DO NOT share your personal information**: This includes your home address, phone numbers, bank details or anything that should be known only to you or your family members.
3. **DO NOT accept friend requests from strangers**: Many requests are made from fake accounts and may be from people who have constructed fake personal profiles that do not reflect the reality.
4. **DO NOT meet someone you have come to know online: The** person may not be who they claim to be and meeting them offline can pose risks.

5. **DO NOT post, share, trade your pictures/videos:** This especially applies on embarrassing content or content you would not want others to see. Once you have shared the content on Social Media, online forums, website or anyone over the Internet it cannot be undone.
6. **DO NOT tag or post pictures of others without consent:** This includes your friends, just as you would not want someone posting or circulating pictures of you without your permission.
7. **DO NOT post offensive content:** Some topics such as someone's religion, race, organization or a community could upset people and may also be against the law or in breach of the social media platforms' usage terms – avoid posting such sensitive content.

Parent Note

Make sure your child is aware of all the recommendations listed above and follows them while browsing the web.

6. Guidelines for Sending and Receiving Email

Nowadays, cyber-criminals may try to trick you into revealing your personal information and passwords by means of email, messengers, SMS or voice calls. You should be suspicious of any messages that try to scare you into opening an attachment or logging into the website to verify your account or reset your account or request personal details etc. we request all our students and parents to not respond to such messages or act on their instructions.

DO's

1. **Verify Sender**: Always verify the sender and the organization (the part after "@" sign) you have received the message from. If you receive an email from Good Will Children Private School, consider verifying its authenticity from the school directly.
2. **Verify the links**: Always verify the link before clicking it. You can understand the real link destination by hovering your mouse cursor over it.
3. **Mark suspicious emails as Spam**: This will protect you from similar messages in the future.

DON'TS

1. **DO NOT click the links**: If a message seems suspicious, do not click the links embedded in it.
2. **DO NOT reveal your personal information**: Do not respond to messages that request your usernames/password or personal information about yourself, your friends and family.
3. **DO NOT open Attachments**: Do not open attachments in emails you were not expecting to receive.

Good Will Children Private School

7. Guidelines on User Accounts & Passwords

DO's

4. **Select a strong password:** Your password should include a combination of upper case, lower case, number and special characters.
5. **Change your password regularly**: Update your password from time to time, especially if you suspect that the password may have become known to someone.
6. **Always logout:** When you are finished with your activity don't forget to press "Logout". Especially while using public Wi-Fi networks. Remember, someone can misuse your account and send messages on your behalf.

DON'TS

1. **DO NOT Reuse Passwords:** Always create a new unique password for every account you create online.
2. **DO NOT Share your username/password**: Don't tell your password to anyone including your family members, friends and peers.
3. **DO NOT write down your password:** They can be easily spotted and used by other people.
4. **DO NOT use your personal data in a password**: Never include your name, birth date, spouse name, pet name etc. as a part of your password

Parent Note

Make sure you have your child's passwords for email, messengers and social networking sites. It's a good idea for you to review who is communicating with your child and in the event of trouble, you'll have important access.

8. Guidelines for Parents to Monitor their Children on Distance Learning

- Place the laptop or computer in a identified area in your home within your supervision.
- Frequently check the exchange of information like messages and materials between your child, their peers, and the school or third entity.
- In case of any wrong suspicion activity on internet or during Microsoft TEAMS and Zoom sessions, report it to school social worker.
- Have frequent conversations with your child regarding online session experiences.
- Install the parent control software to monitor your child's online activities.

- Use only your account for online sessions (Microsoft TEAMS and ZOOM) and Classe365 LMS.

9. Guidelines for Bring your own device from home (BYOD)

- Learning about and being held accountable for the responsible use of electronic and digital tools is an important part of preparing students to be successful in today's knowledge society. Personal electronic devices are the sole responsibility of the student owner. The school has no responsibility for these personal devices if they are lost, loaned, or stolen.
- Electronic devices must be used in a manner consistent with the Good Will Children Private School's Safe Internet Guidelines and the school reserves the right to limit use of electronic devices, especially when these devices are used to harass others or disrupt the learning environment
- Students must use their tablets and laptops from home in the ethical way.
- Students will obey all safe internet guidelines of school like behaviour and communication while using their own technological devices.
- **Students are not allowed to bring the devices other than their specific schedules.**