Mission Statement: Creating tomorrow's successful and caring citizens today.



Policy Updated By	Latest Publish Date	Monitoring Cycle
Akram Tarik	January 2022	Annually

Schedule for Development / Monitoring / Review

Schedule for Development / Monitoring / Review		
This policy was approved by the Governing Body	January 2022	
on;		
The implementation of this policy will be monitored by the:	Principal and Senior Leadership Team	
The Policy will be reviewed annually, or more regularly in the light of any significant new developments. The next anticipated review date will be:	January 2023	
Should serious incidents take place, the following external persons/agencies should be informed:	Akram Tarik (Principal) and in his absence Jeremy Hallum (Vice Principal)	

Parents & Students CYBERSECURITY Guide

Vision

'At GFM we empower students to have the heart to celebrate uniqueness and the mind to be innovative, creative problem solvers, bringing a positive change to the world in which we live.'



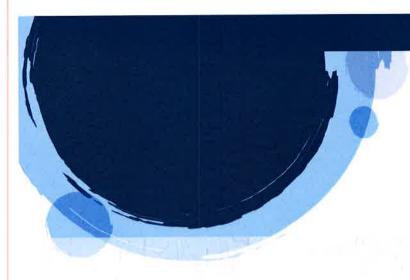


TABLE OF CONTENTS

I	ntro	oduction	3
Ţ	op 1	tips for Parents to keep children safe online	3
٨	1aj	ior Cybersecurity guidelines	
	1.	User Accounts & Passwords	4
	2.	Email & Phishing	5
	3.	Internet Browsing	6
	4.	Social Media &Online Communication	7
	5.	Audio/Video Conferencing	8
	6.	Device & Online Services Security	9
	7.	Cyberbullying	. 10





Vision

'At GFM we empower students to have the heart to celebrate uniqueness and the mind to be innovative, creative problem solvers, bringing a positive change to the world in which we live.'



INTRODUCTION

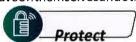
The Internet is an incredible platform for children to learn, express themselves and have fun, but it also has its dark side. Not everything on the Internet is safe and can be trusted. Even though the benefits outweigh the potential dangers, parents and guardians must be aware of the real risks that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

This guide contains an illustrative list of scenarios and general recommendations to parents on how to protect themselves and their children against most common cybersecurity threats.

Top tips for Parents to keep children safe online



It is important that you are aware of your child's Internet activities including the social media channels they utilise, 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, to day and in the future.



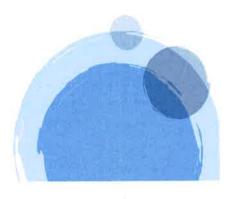
There are parental control tools available to help protect your children from harmful and inappropriate online content. Phones, tablets, game consoles and other devices that connect to the Integnet have parental control settings. Technology can be effective, butnosystem is 100 proof, so education remains key.



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.



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 "reportabuse" buttons where you can report in appropriate behaviour. For any GEMS Education related concerns, you are always welcome to contact your school directly.





Select a strong password

Your password should include a combination of upper case, lower case, number and special characters.

Change your password regularly

Update your password from time to time, especially if you suspect that the password may have become known to someone.

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.



All activities performed using your account are attributed to you, including all activities performed by a cybercriminal with access to your account.



Reuse password

Always create a new unique password for every account you create online.

Share your username/password

Don't tell your password to anyone including your family members, friends and peers.

Write down your password

They can be easily spotted and used by other people.

Use your personal data in a password

Never include your name, birth date, spouse name, pet name etc. as a part of your password

Use other user's credentials to log in Justlike you would not want anyone to use your credentials to send messages on your behalf, don't log in under someone else's account, even if you know the password.





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.



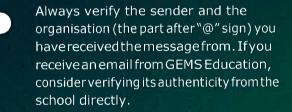


2. Email & Phishing

Nowadays, cyber-criminals may try to trick you into evealing your personal information and provided by means of email, messengers, SMS lls. This is called phishing. You may evive inshing messages that will request you erform an action or share some valuable data about yourself (that you would not do in normal circumstances).

DOS

Verify the sender



Verify the links

Always verify the link before clicking it. You can understand the real link destination by hovering your mouse cursor over it.

Mark suspicious emails as Spam

This will protect you from similar messages in the future.

DON'TS

Open attachments

Do not open attachments in emails you were not expecting to receive.

Click the links

If a message seems suspicious, do not click the links embedded in it.

Reveal your personal information

Do not respond to messages that request your usernames/password or personal information about yourself, your friends and family.



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. You should never respond to such messages or act on their instructions.







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.

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.



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.

Save your passwords in the browser

Doing this could leave you more vulnerable to being hacked.

Use Virtual Private Networks (VPN)
Especially while accessing official GEMS
Education resources such as Online
Learning platform or
videoconferencing tools.





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.



Social Media & Online Communication

TAX INFO ADDRESS CITIZENSHIP IRTH DATE EDUCATION
RAVEL DOCUMENT TRAVEL LOUGHTH MARIN MATION LIBRATIVE MATIONALITY MARINAL STATUS INCOME INFO IDENTITY DOCUMENT BANK ACCOUNT NUMBER OCCUPATION VISA INFO

Fake social media profiles are increasingly prevalent. It is asy for cyber-criminals to create fake accounts and use them for illegal purposes. Remember, all people that you eet online are strangers, no matter how long you may ave known them or how friendly they appear to be.



Review your privacy settings

Ensure your social media accounts privacy settings are configured to be restrictive, so that your posts and your personal details are only revealed to your friends and not strangers. Review your privacy settings periodically.

Think before you post

Whether on social media website, mobile apps orany other online platforms. Always take a minute to think before hitting the "Send" button.

Try to utilise pseudonymized names

Including screen name / nick name and details on social media and other online platforms. Avoid sharing authentic personal details.

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. Make sure you share any worries or incidents with your school so they can provide support for the student.

Share your concerns with the school

If you have any GEMS Education related concerns or queries, reach out to your school directly.

> In social media networks, your online privacy can be affected by others and the privacy of others also depends on you



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.

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.

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.

Share your school information online

The school has dedicated people who are authorised to share any school related information online.

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.

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.

Posting offensive contentSome 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.

'In a world where you can be anything... be kind."



 $\label{lem:makesureyour} \textbf{Make sure your child is aware of all the recommendations listed above and follows them while browsing the web.}$

Parent Note



4. Audio/Video Conferencing



DOS 🔀



- 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, neighbourhood that you are
 in etc.
- 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.
- Keep your password in secret
 Avoid sharing your passwords with other
 people as they can use them to act on
 your behalf.

XDON'TS

Record/livestream people without their consent

This action is considered illegal law in some countries.

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.

Invite external participants

If you are having an online session with teachers/students/parents from your school do not invite students and parents from other schools.



Make sure your child consults with you before joining a new group within existing or new video conferencing





5. Device & Online Services Security

DOS

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.

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.

Makeuse of parental controls

Parental control settings are available in most of the modern smartphones and tablets.
Additionally, many parental control tools can be found online.



Turn off security software

Software such as anti-virus scanner or firewall should never be turned off.

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.

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.

Misuse GEMS provided devices/services

Devices/services are provided for educational purposes only. Do not use these devices for any malicious/illegal/hacking activities and do not share them with other students or parents.



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.





6. Cyberbullying

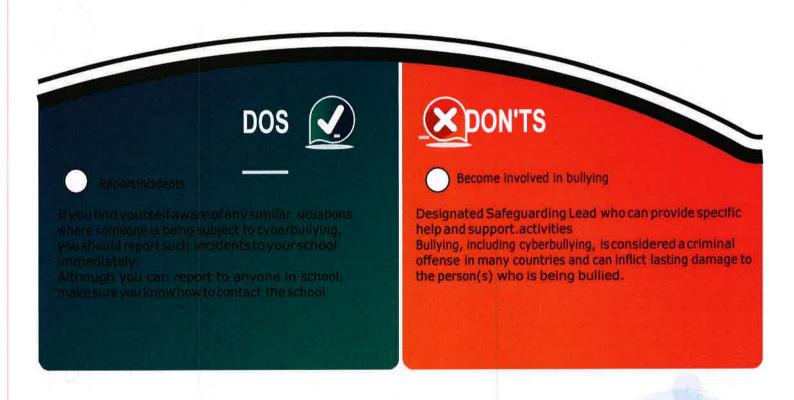
GFM IT Online Security Guidance for Parents Policy

Misuse of digital communication / technology to harass, humiliate, threaten or stalk an individual is termed as cyberbullying. Cyberbullying could happen over any digital channel such as text messages, email, social media, gaming or similar online forums.

Look out for the following sample scenarios where someone has been:

- Sending, sharing or posting nasty, hurtful or abusive messages
- Humiliating someone by posting/sharing embarrassing videos or images
- Tagging someone inappropriately in an image
- Spreading rumours or lies about someone online
- Trolling saying mean things to stir people up against someone

- Imitating someone online
- Making threats towards someone online
- Sending repeated harassment and threatening messages (cyberstalking)
- Deliberately excluding someone from a group/conversation





• Please teach your children the safeguards for the above scenarios and ensure they follow the below quidelines 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 / school Safeguarding Lead or other trusted adult as soon as possible.





Signed Date 7 | 22

Vice Principal

Principal/eEO

Signed Date 7/1/22

Policy review date: January 2023

