Ministry of Education
CURRICULUM DEVELOPMENT UNIT
St. Vincent and the Grenadines

#GoCyberSmart

# INTERNET SAFETY GUIDELINES

EMU
Education Media Unit
S.V.G Ministry of Education

# RATIONALE

Technology is an integral component of the lives of both young and old in today's world. Although the worldwide web provides a wealth of information and has become an essential resource in teaching and learning, it is unfortunately being used to destroy the lives of many persons, particularly children. It is therefore critical that protocols be established to ensure the protection of our children and young people. Cyber safety is defined as the safe and responsible use of information and communication technologies, such as the internet, social media, online games, smart phones, tablets, and other connected devices. Cyber safety education provides students with the knowledge and skills they need to stay safe within online environments. It involves acknowledging the benefits and opportunities offered by the online world, while understanding the risks and avoiding potential harms. This document provides guidelines for the safe use of the internet at home, in the classroom and at school by both students and teachers.

If the following policy is to be effective, each school must develop a Cyber Safety and Acceptable Use Policy. These will help to keep users safe and further in the management of the school's soft and hardware. Also, it is advisable that whenever students log on to the school's internet, they do not enter under the name of a device so that the teacher knows that it's the student who is actually on the device and not someone else.

# “SMART”

## INTERNET SAFETY GUIDELINES FOR CHILDREN

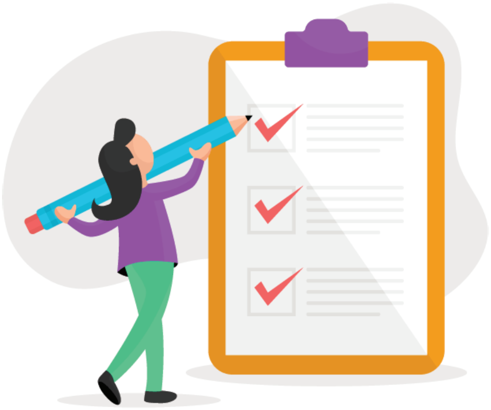
**SAFE** – Keep safe by being careful not to give out personal information such as your full name, email address, phone number, home address, photos, or school name to persons online.

**MEETING** – Meeting someone you have only been in touch with online can be dangerous, only do so with your parents’ permission and even then, only when they can be present.

**ACCEPTING** – Accepting emails, messages, or opening files, pictures, or texts from people you do not know, and trust can lead to problems – they may contain viruses or may be nasty messages.

**RELIABLE** – Information you find on the internet may not be true, or someone online may be lying about who they are.

**TELL** – Tell your parent, teacher, or trusted adult if someone makes you feel uncomfortable or worried, or if you or someone you know is being bullied online.



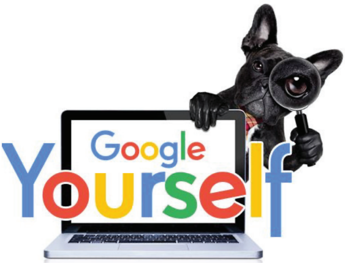
**Source:**
https://st-anne-stanley-school.co.uk/information/sickness/e-safety-for-children/

**Video sources on Cyber Safety:**
https://www.youtube.com/watch?v=euc-WcN5IkY&t=107s
https://www.youtube.com/watch?v=xl6AiyWA39w
https://www.youtube.com/watch?v=OgOzSPCaHnU
https://www.youtube.com/watch?v=ottnH427Fr8
https://www.youtube.com/watch?v=-tiUDjn7-as

# SAFE USE OF TECHNOLOGY

## AT HOME

### *Managing your Reputation*

- 

 – review online content which relates to you and take steps to secure or remove any private or unwanted content.
- **Choose profile pictures wisely** – even with a private account the profile picture and bios are usually visible. So, think carefully about what you share and what it might say/reveal about you.
- **Think before you post** – be mindful of how pupils; parents; and employers may view you and your online content.
- **Act according to your school's policy** – your school may have a policy about anything which can cause harm or distress to others or brings the name of the school into disrepute, including content shared out of school hours.

### *Securing your Content*

- **Privacy settings** – setting these to private will allow you to control who can see the content you share. They can usually be found within the settings of the account. Although remember that content can easily be screenshotted and shared more publicly.
- **Pin/passcode on devices** – always set devices up with a strong pin/passcode lock to ensure personal data and images are secure.
- **Strong passwords** – make sure you use a mixture of lower- and upper-case letters, symbols, and numbers within a password as this will make it stronger. Also remember to change them regularly and keep them to yourself.
- **Logging out** – always log out of online accounts when leaving a device to secure the content.

### *What to do if you are the Target of Cyber bullying*

- **Do not retaliate/respond** – this will often aggravate the situation further.
- **Keep the evidence** – screenshot or print all content and keep a record of any incidences you are unable to capture content of.
- **Report and seek advice** – you can report online content directly to the site as well as to your parents, Principal, School Counselor, or teachers who should support you in handling cases of cyber bullying.

## *Using Technology and the Internet Safely (For Teachers)*

- **Use school devices** – where possible try to use school devices which should already have appropriate filters applied at device level or across the school internet.
- **Set rules for use of personal devices** – If using personal devices is appropriate then set clear rules for use in class. This could include what apps to use or whether image taking would be appropriate for the activity.
- **Guide pupils to appropriate sites** – you may consider selecting sites for younger pupils or discussing with older ones what content they may be looking for when carrying out an online search.
- **Model good behavior** – consider the pupil's privacy when sharing their images online. Regardless of whether you have obtained media consent, model best practice by asking their permission before posting an image of them online.
- **Act according to school policy** – schools will have acceptable use policies for all members of the school community. Familiarize yourself and your pupils with these rules frequently.

### *Children Viewing Online Content*

- **Check online content first** – always try to check online content first either by fully exploring any webpages you may show in class or by watching videos in their entirety.
- **Check search results first** – if you are going to search for content with the class, perform a ‘dry run’ first to ensure the content is appropriate. Sometimes the most innocent of searches can return unexpected content.
- **Capture content** – you may wish to save content or take screen shots to ensure adverts/comments have not changed since you last checked.
- **Apply safety modes** – where available use the settings of the site/app to filter the content they search for. Google offer a ‘safe search’ setting which can be found in the top right corner and YouTube offer a ‘safety mode’ which can be found at the bottom of the screen or within the settings of the app.
- **Check school policy** – be clear on your school’s policy for viewing inappropriate content in class and share this with the pupils. Ensure that they are aware of the different policies and sanctions, e.g., if it is viewed on purpose or by accident.

## *Incorporating Online Safety into the Curriculum*

- **Whole school approach** – online safety messages should be embedded in all areas of the curriculum as many subjects now frequently use technology or ask pupils to conduct online searches. Ensure pupils are reminded of online safety messages whenever using technology and the internet.
- **Use a range of resources/teaching methods** – there are a wealth of online resources to support you in delivering online safety messages in a range of ways.
- **Stay up to date** – technology and online content can change rapidly. Ensure you are teaching about the current risks and trends by researching or speaking to pupils.
- **Give advice or routes to get help** – ensure pupils know what to do if something goes wrong online. This could include speaking to an adult, saving evidence or reporting.

## AT SCHOOL

### *Best Practice for Using Technology and the Internet*

- **Review policy regularly** – ensure the school's cyber safety policy is up to date and has been shared/communicated with all members of the school community.
- **What to do if…** – consider how your school will put your policy into practice. Outline how staff should react in different situations, e.g., where a pupil has misused technology and the internet on purpose or by accident.
- **Review school procedures** – as online issues evolve it is important to review school procedures and ensure teaching and responding procedures are effective.
- **Use appropriate methods of contact** – only contact pupils and their families through school channels, e.g., a school social networking page or online teaching platform.
- **Secure school devices** – ensure devices have up to date firewalls and safety modes in place and are secured with passcodes.

### *Using Technology Safely and Social Media Safely Offsite*

- **Use school devices** – to secure images and contact details it is best to use school devices for communication with young people and families or to take images.
- **Avoid sharing personal details** – most schools specify that staff should not give out personal mobile numbers or email addresses to pupils or parents as these details could easily be shared with others.

- **Review school policies and AUP beforehand** – schools will have clear policies on the use of technology and social media, and this should include offsite usage as well. Familiarize yourself and the pupils with this. This may include appropriate communication with others, taking/sharing images and sharing location details online.
- **Consider online risk** – where necessary remember to include possible online risks when completing risk assessment forms.
- **Set rules for personal devices** – pupils may bring personal devices on trips, so it is important to communicate whether this is allowed and the appropriate rules for use of a personal device during the school trip.

### *Using Children's Images*

- **Obtain consent** – before videoing or photographing pupils ensure you are clear about the school's policy and that parents have completed relevant consent forms.
- **Use school devices** – It is advisable to only use school devices when capturing images or videos of students as it is then stored on that device.
- **Consider where it will be stored and for how long**– when saving a file ensure this is on a secure school network or encrypted USB and deleted when no longer required.
- **No names** – it is best practice not to share the image with the child's full name to safeguard their welfare.
- **Consider appropriateness of the image before sharing** – not all images which may be taken are

appropriate to be shared online. Caution may be needed in taking photos at sporting events, for example during swimming lessons or events. It is also best practice to ask the child before sharing an image in a public space as it may embarrass of upset them.

**Adapted from:**
https://www.childnet.com/ufiles/Using-technology-safely-checklist.pdf

**Resource videos for teaching online safety:**
https://www.youtube.com/watch?v=6jMhMVEjEQg&list=PLaSegn4AdJAwh4zgUZAvowur_DwMkr14l
https://www.youtube.com/watch?v=rzoIgNrIilo

*A production of*
***The Curriculum Development Unit***
*in collaboration with*
***The Education Media Unit***
*Ministry of Education and National Reconciliation*
*St. Vincent and the Grenadines*

Ministry of Education
CURRICULUM DEVELOPMENT UNIT
St. Vincent and the Grenadines

EMU
Education
Media Unit
S.V.G Ministry of Education

# #GoCyberSmart