Paradis International College	Doc. Ref. :
	Date of Last Review: 2025
	Date of Next Review: 2028
Online Safety Policy	

	AUTHORS	APPROVED BY
Name	SAVA LOREDANA	ALBU OANA
Title	Teacher	Director of College

	Revision 2025	**APPROVED BY**
Name	Ionita Andreea	ALBU OANA
Title	Highschool teacher	Director of College

Introduction

Paradis International School is committed to promoting and safeguarding the welfare of all students and an effective online safety strategy is paramount to this. This is particularly important with regard to the Prevent strategy, as a large portion of cases of radicalization happen through the online medium.

Aims

1. To protect the whole Paradis International School community from illegal, inappropriate and harmful content or contact;
2. To educate the whole Paradis International School community about their access to and use of technology; and
3. To establish effective mechanisms to identify, intervene and escalate incidents where appropriate.

1. Aim

In considering the scope of the School's online safety strategy, the School will take a wide and purposive approach to considering what falls within the meaning of technology, networks and devices used for viewing or exchanging information including communications technology.

This policy applies to all members of the School community, including staff and volunteers, students, parents and visitors, who have access to the School's Technology whether on or off School premises, or otherwise use Technology in a way, which affects the welfare of other students or any member of the School community or where the culture or reputation of the School is put at risk.

The following policies, procedures and resource materials are also relevant to the School's online safety practices:

- Safeguarding and Child Protection Policy
- Anti-Bullying Policy
- Risk Assessment Policy for Student Welfare

2. Roles and responsibilities

2.1 Director of college and Senior Leadership and Management Team

- The Director of College has overall executive responsibility for the safety and welfare of members of the School community.

The Designated Safeguarding Leads (DSL) are senior members of staff from the Senior Leadership and School Management Team (SLMT) with lead responsibility for safeguarding and child protection. The responsibility of the DSL includes managing safeguarding incidents involving the use of Technology in the same way as other safeguarding matters, in accordance with the School's Safeguarding & Child Protection Policy.

2.2 All staff

- The School staff have a responsibility to act as a good role model in their use of Technology and to share their knowledge of the School's policies and of safe practice with the students.
- The School staff have a responsibility to act as a good role model in their use of Technology and to share their knowledge of the School's policies and of safe practice with the students.

- Educate students on digital risks, including trending scams and online challenges.

2.3 Parents

- The role of parents in ensuring that students understand how to stay safe when using Technology is crucial.
- Play a key role in monitoring and guiding their child's online activity.
- The School expects parents to promote safe practice when using Technology and to:

 (a) support the School in the implementation of this policy and report any concerns in line with the School's policies and procedures, according to the instructions they get in the parents brochure and during the meetings with the class teachers;

(b) talk to their child to understand the ways in which they are using the internet, social media and their mobile devices and promote responsible behaviour; and

(c) encourage their child to speak to someone if they are being bullied or otherwise are concerned about their own safety or that of another pupil or need support.

- If parents have any concerns or require any information about online safety, they should contact the DSL.

3. Education and training

3.1 Students

- Students are educated in an age appropriate manner about the importance of safe and responsible use of Technology, including the internet, social media and mobile electronic devices during the meetings with the class teacher and also in the brochure with the school rules
- Students are educated in the dangers of online scams, phishing, and fraud.
- children are guided to make sense of their physical world and their community through opportunities to explore, observe and find out about people, places, technology and the environment
- children are enabled to explore and play with a wide range of media and materials and provided with opportunities and encouragement for sharing their thoughts, ideas and feelings through a variety of activities in art, music, movement, dance, role-play, and design and technology
- The safe use of Technology is also a focus in all areas of the curriculum and key safety messages are reinforced as part of assemblies and tutorial/pastoral activities, teaching students

(a) about the risks associated with using the Technology and how to protect themselves and their peers from potential risks;

(b) to be critically aware of content they access online and guided to validate accuracy of information;

(c) how to recognize suspicious, bullying, radicalization and extremist behaviour;

(d) the definition of cyberbullying, its effects on the victim and how to treat each other's online identities with respect;

(e) the consequences of negative online behaviour; and

(f) how to report cyberbullying and/or incidents that make students feel uncomfortable or under threat and how the School will deal with those who behave badly.

(g) about the risks of participating in viral challenges (e.g., TikTok trends).

Any inappropriate online behavior, whether it occurs on school platforms or external apps (WhatsApp, Instagram, Snapchat, BeReal, etc.), will be sanctioned according to the School's Discipline Policy.

3.2. **Parents:**

- Parents and staff will be notified about trending online scams (e.g., phishing, fake payment portals) via WhatsApp groups.
- If any issues arise with online fee payments, parents will be informed directly via WhatsApp messages.

4. **Access to the School's Technology**

- The School provides the internet and an email system to staff as well as other Technology.
- Staff require individual usernames and passwords to access the School's internet sites and email system which must not be disclosed to any other person. Any student or member of staff who has a problem with their usernames or passwords must report it to the IT Department immediately
- Students and staff require individual usernames and passwords to access the School's internet and intranet sites and email system which must not be disclosed to any other person. Any student or member of staff who has a problem with their usernames or passwords must report it to the IT Department immediately
- The School's policies apply to the use of Technology by staff and students whether on or off School premises and appropriate action will be taken where such use affects the

welfare of other students or any member of the School community or where the culture or reputation of the School is put at risk.

● Kinderpedia is the official grading platform, ensuring that grades are only visible to the respective student, maintaining privacy. Kinderpedia is also used for payment administration.

● Strict security measures protect all student and staff email accounts.

ONLINE LEARNING RULES:

    o **WhatsApp groups are made, where the teacher posts the link to the online class, so only those in a restricted group have access to it,**

    o **The teachers grant access to online classes only to users they know, so students have to use their real names,**

    o **Students are not allowed to share links to classes with anyone outside the school, or they will get a notification from the Discipline and ethics committee,**

    o **Students must keep their cameras on during the lessons;**

    o **Students are not allowed to use inappropriate language in the chat box,**

    o **Students or their parents (family members, people in the house) are not allowed to record the online lessons without the teacher's consent.**

5. Procedures for dealing with incidents of misuse

Staff, students and parents are required to report incidents of misuse or suspected misuse to the School in accordance with this policy and the School's safeguarding and disciplinary policies and procedures.

5.1 Misuse by students

● Anyone who has any concern about the misuse of Technology by students should report it so that it can be dealt with in accordance with the School's behaviour and discipline policies, including the Anti-Bullying Policy where there is an allegation of cyberbullying.

- Anyone who has any concern about the welfare and safety of a pupil must report it immediately in accordance with the School's child protection procedures (see the School's Safeguarding & Child Protection Policy).

5.2 Misuse by staff

- If anyone has a safeguarding-related concern, they should report it immediately so that it can be dealt with in accordance with the procedures for reporting and dealing with allegations of abuse against staff set out in the School's Safeguarding & Child Protection Policy.

6   Monitoring and review

The DSL has responsibility for the implementation and review of this policy and will consider the record of incidents involving the use of Technology and the logs of internet activity (including sites visited) as part of the ongoing monitoring of safeguarding procedures, to consider whether existing security and online safety practices within the School are adequate.