COMMUNICATE **SAFELY**

ONLINE LEARNING

PLATFORMS

COMUNICAR
EM SEGURANÇA

altice
fundação

ZOOM ?!

!? MICROSOFT TEAMS

GOOGLE MEET ?!

!? CLASSROOM

VIRTUAL SCHOOL ?!

HOW TO USE

IS IT SAFE?

WHAT ARE THEY?

Despite not being new, platforms that provide audio and video communication gained a bigger dimension in 2020, with the pandemic situation experienced worldwide.

They were the resource used by schools to continue classes, and the means of communication par excellence between teachers and students, teachers and parents.

From one day to the next, teachers, students and parents had to adapt to a new reality, get to know a huge diversity of platforms and learn how technology could be an added value in accessing education and knowledge.

Not being a novelty, these platforms have always been more used by young adults or adults, as one of the great challenges in online learning is maintaining students' interest and focus. Digital platforms can be a complement to traditional teaching, having positive aspects and others to be improved.

Online learning platforms allow for better time management, shorter and less expository lessons and the possibility of different interaction (questions, forums, activities, etc.). On the other hand, it is necessary to have equipment (computer, tablet, mobile phones), as well as Internet access with good network, in order to ensure effective communication.

With the increasing use of these platforms, one of the main concerns was the safety of students, respect for everybody's privacy and sharing information.

On the Internet, in any website or platform, it is always very important to keep both the computer and the user safe.

HINTS/ SUGGESTIONS

Keeping computer security systems up to date
(firewall, antivirus, among other devices).

Keeping vigilant
regarding your children's online contacts.

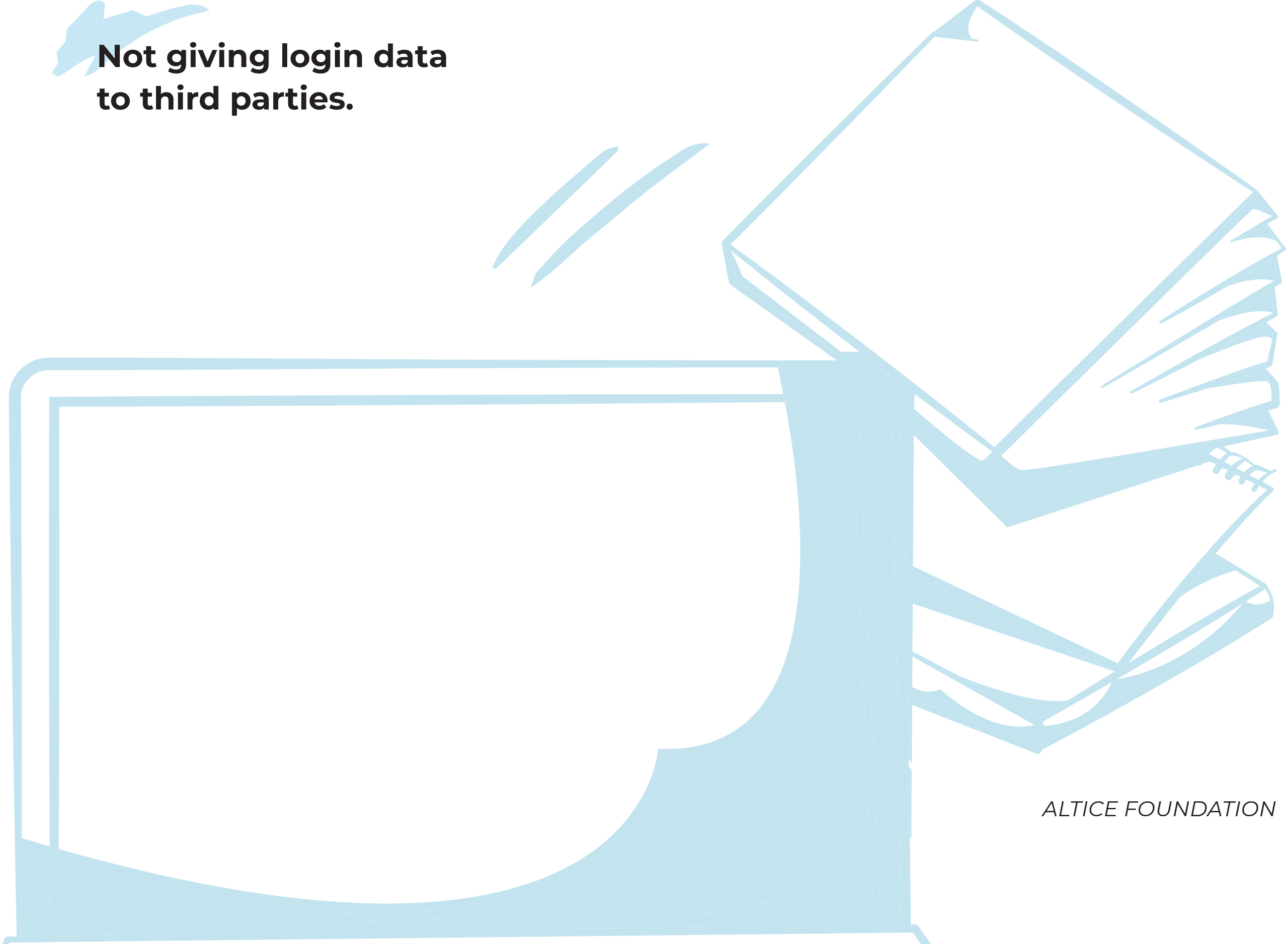
Using one single password
for each platform.

Avoiding work through public Wi-Fi
or, in that case, using a VPN connection.

Not accepting video calls from unknown sources/ links/senders.

Not opening links or attachments of unknown or suspicious origin.

Not giving login data to third parties.



THINK BEFORE PUBLISHING

Be careful when sharing personal data (location, photos, videos) that can be used for other purposes.

UPDATED SOFTWARE

It is very important to keep the operating system up-to-date, otherwise it won't protect you against possible threats. Update your software regularly.

WEBCAM AND MICROPHONES

Online communication will benefit from using a camera. However, remember that cameras and microphones are easily accessible and can be switched on remotely.

Always keep your camera switched off or covered. Use the camera and microphone only when necessary.

INVITE PARTICIPANTS

- You can send one link only, which provides little security, as anyone who knows the link can access the meeting.

- A more secure alternative is to create a password to access the meeting, or to accept people who have to be in the meeting (waiting room).

CONTROL CHATS AND AUDIOS

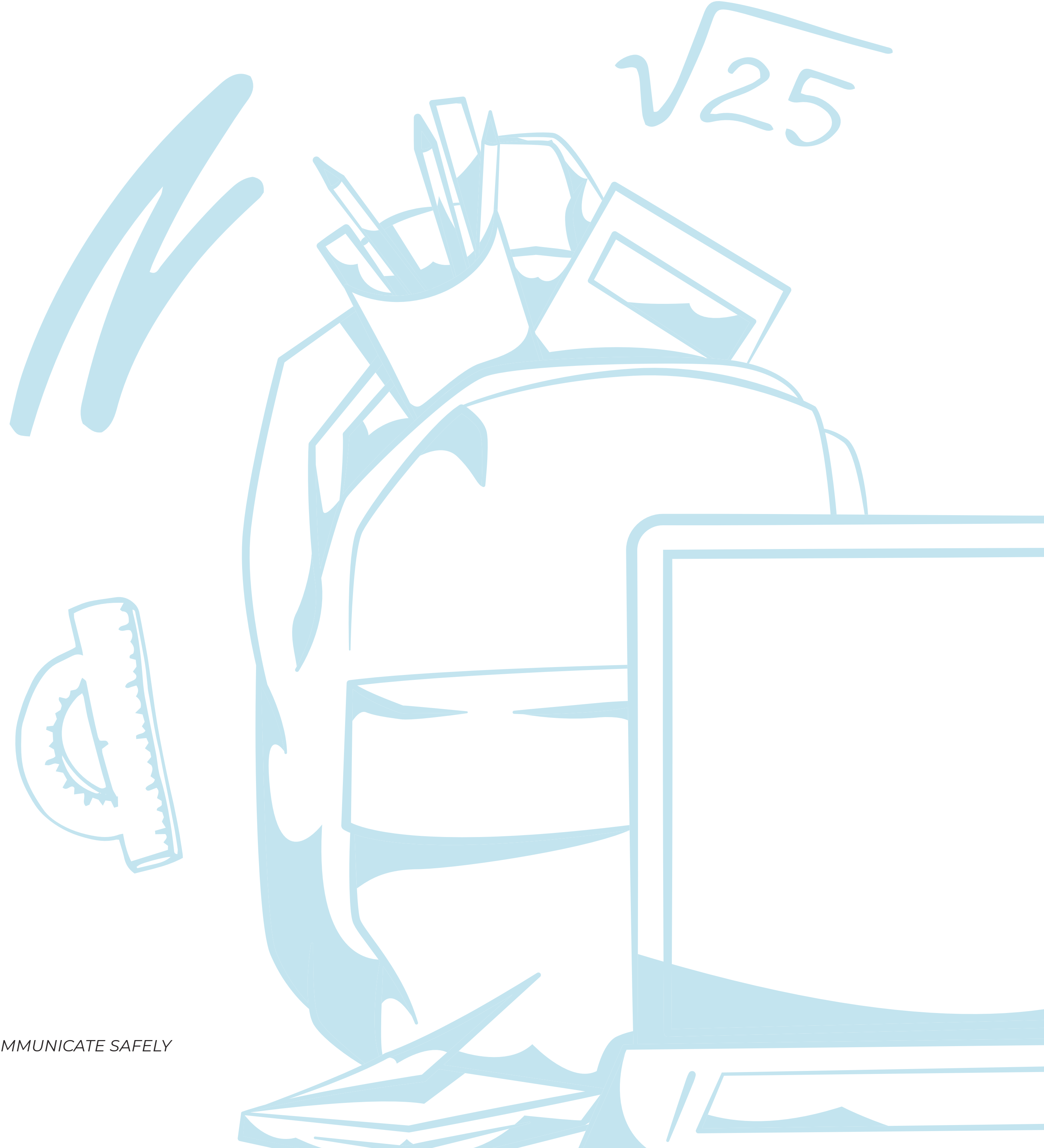
- Managing classes, meetings or group/team assignments can be difficult when participants' microphones are on or when there is no chat moderation.

- Platforms can be set up in order to avoid this situation. Restricting message sharing in larger groups can help prevent the dissemination of malicious content.

- It is the responsibility of the virtual meeting host to manage these options.

LOCK THE DOOR

Some platforms let you “lock the door” after the meeting is started. This way, outsiders cannot access the meeting, even if they know the link for the meeting.



SAFE EDUCATION

ONLINE **SAFETY HELPLINE**

800 21 90 90

PROJECT

COMUNICAR EM SEGURANÇA

SPONSOR

altice fundação

FUNDING PARTNER

Cofinanciado pelo Mecanismo Interligar a Europa - União Europeia

Centro Internet Segura

A COR LARANJA