

COMUNICAR EM **SEGURANÇA**

PLATAFORMAS DE ENSINO



2 À DISTÂNCIA



ZOOM ?!

! ? MICROSOFT
TEAMS

GOOGLE
MEET ?!

! ? CLASSROOM

ESCOLA
VIRTUAL ?!

COMO USAR
É SEGURO ?

O QUE SÃO?

PLATAFORMAS DE ENSINO À DISTANCIA



Não sendo algo novo, as plataformas que permitem a comunicação audio e video ganharam outra dimensão em 2020 com a situação de pandemia vivida a nível mundial.

Foram o recurso utilizado pelas escolas para continuarem as aulas, e o meio de comunicação, por excelência, entre professores e alunos, professores e pais.

De um dia para o outro, professores, alunos e pais tiveram de adaptar-se a uma nova realidade, conhecer uma enorme diversidade de plataformas, e aprender como a tecnologia podia ser uma mais valia no acesso à educação e conhecimento.

Não sendo uma novidade, estas plataformas foram sempre mais usadas por jovens adultos ou adultos, uma vez que um dos grandes desafios no ensino à distância é manter o interesse e o foco dos alunos. As plataformas digitais podem ser um complemento ao ensino tradicional, tendo sempre aspetos positivos e outros a melhorar.

As plataformas de ensino à distância permitem uma melhor gestão do tempo, aulas mais curtas e menos expositivas e com a possibilidade de uma interação diferente (questões, fóruns, atividades, etc). Por outro lado, é necessário garantir equipamentos (computador, tablet, telemóveis) e acesso a Internet com boa rede de forma a garantir uma comunicação eficaz.

Com a crescente utilização destas plataformas, umas das principais preocupações foi a segurança dos alunos, o respeito pela privacidade de cada um e a partilha de informação.

Na internet, em qualquer site ou plataforma, é sempre muito importante manter a segurança do computador e do utilizador.



DICAS/ SUGESTÕES

PLATAFORMAS À DISTANCIA

Ter os sistemas de proteção do computador atualizados

(firewall, antivírus, entre outros dispositivos).

Manter-se vigilante

em relação aos contactos dos seus filhos online.

Usar uma palavra-passe única

para cada plataforma.

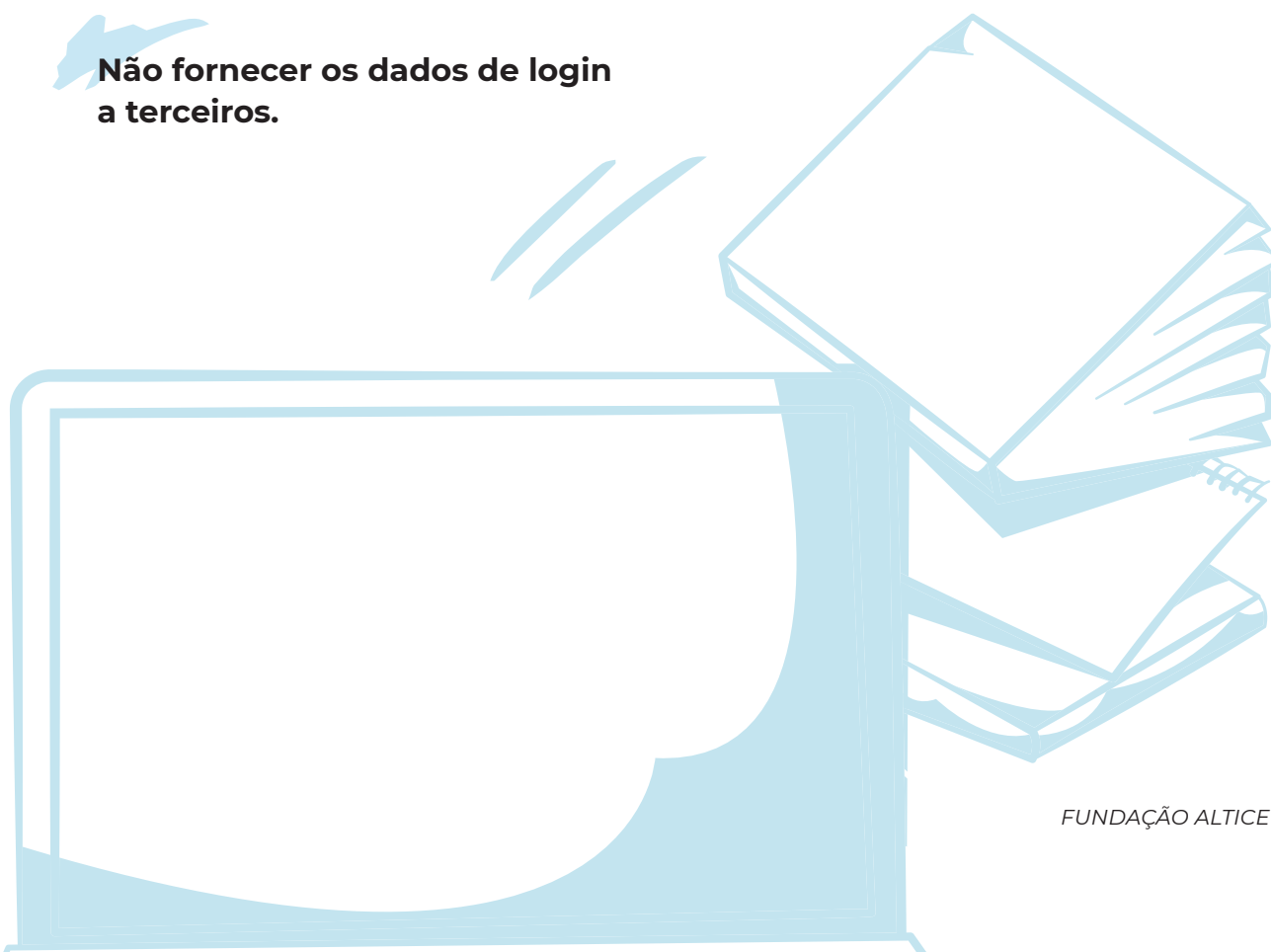
Evitar trabalhar através de WI-FIS públicos

ou nesse caso, usar uma VPN.

Não aceitar videochamadas de fontes/ligações /remetentes desconhecidos.

Não abrir links ou anexos de origem desconhecida, ou suspeita.

Não fornecer os dados de login a terceiros.



PENSAR ANTES DE PUBLICAR

Ter atenção ao partilhar dados pessoais (localização, fotografias, vídeos) que podem ser usados para outros fins.

SOFTWARE ATUALIZADO

É muito importante que o sistema operativo esteja atualizado, pois caso contrário, não será uma proteção para as ameaças que podem acontecer. Atualizar regularmente o software.

WEBCAM E MICROFONES

A comunicação online ganha com a utilização de uma câmara. No entanto, lembre-se que as câmaras e micros são de fácil acesso, e que podem ser ligados remotamente.

Ter sempre a câmara desligada ou tapada. Usar a câmara e o microfone apenas quando é necessário.

CONVIDAR PARTICIPANTES

Pode ser enviado apenas um link que dá poucas garantias de segurança, pois qualquer pessoa que tenha conhecimento do link, acede à reunião.

Uma alternativa mais segura é criar-se uma password de acesso à reunião, ou aceitar na reunião pessoas que devem estar na reunião (sala de espera).

CONTROLAR CHATS E ÁUDIOS

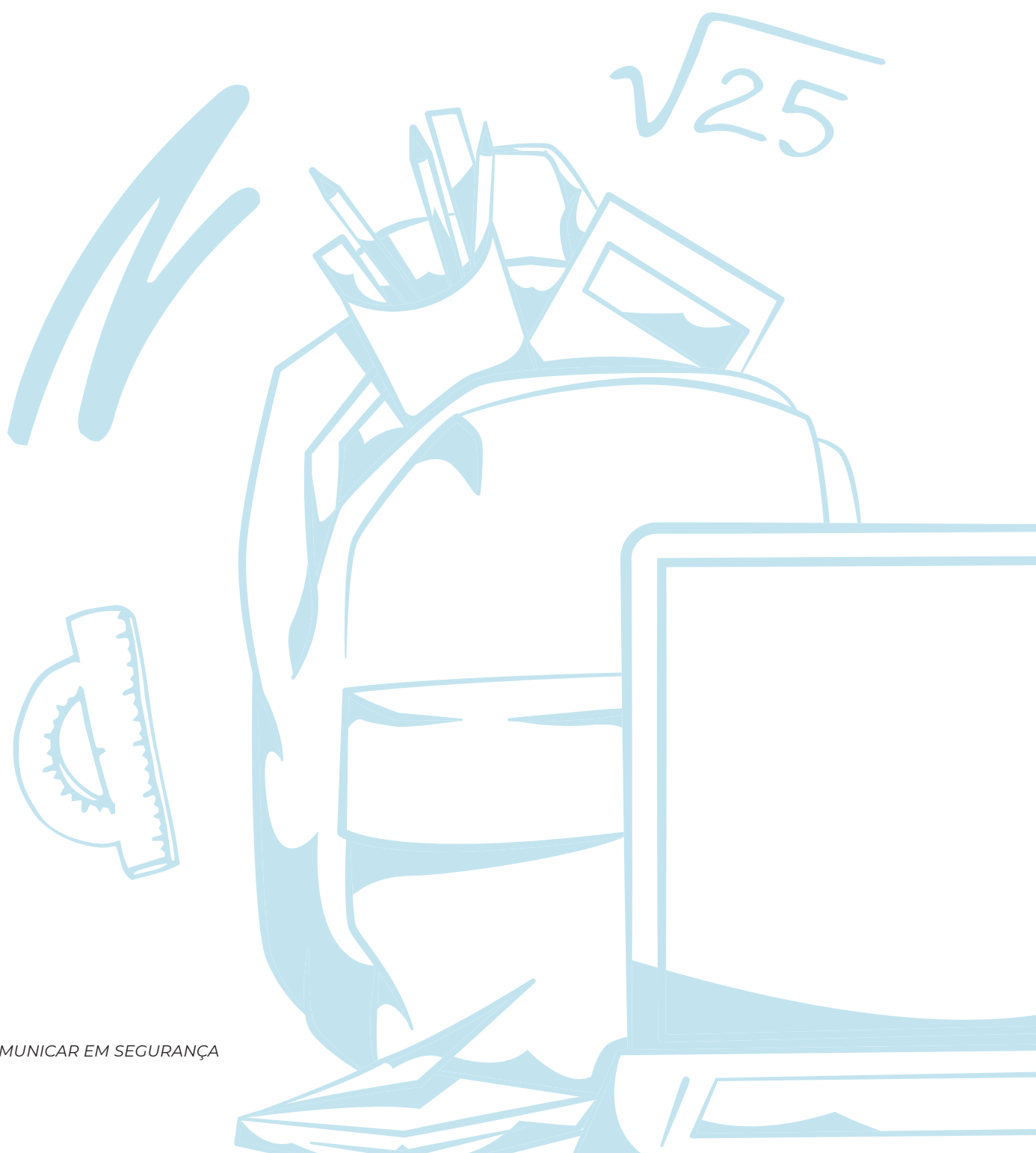
A gestão de aulas, reuniões ou trabalhos de grupo/equipa pode ser dificultada quando os microfones dos participantes estão ligados, ou quando não existe moderação no chat.

As plataformas podem ser configuradas para que esta situação não aconteça. A restrição de partilha de mensagens em grupos maiores pode ser uma mais valia para impedir a difusão de conteúdos maliciosos.

É da responsabilidade do organizador da reunião virtual gerir estas opções.

TRANCAR A PORTA

Algumas plataformas permitem “trancar a porta” após o início da reunião. Desta forma, pessoas estranhas não conseguem aceder à reunião, mesmo que saibam o link da reunião.



EDUCAÇÃO SEGURA

LINHA **INTERNET SEGURA**

800 21 90 90

PROJETO



PROMOTOR



COFINANCIADOR



Centro
Internet
Segura