



SeguraNet

# ESTUDO EM CASA

## RECOMENDAÇÕES no uso de plataformas que permitem a comunicação VÍDEO e ÁUDIO

Várias plataformas e serviços da Internet estão a ser usados pelas Escolas, como um meio educacional valioso, para que professores e alunos continuem conectados e a interagir. Promova um ambiente seguro no Estudo em Casa, tendo em atenção este conjunto de recomendações, quando utiliza plataformas que permitem a **comunicação vídeo e áudio**:

### 1 **Pense antes de publicar informação sensível**

Não partilhe informação com a sua localização ou dados pessoais (morada, contactos, fotos, etc). Estranhos podem facilmente descobrir a sua morada ou o local onde se encontra, bem como utilizar os seus dados pessoais de forma maliciosa. Algumas plataformas têm opções que permitem usar criptografia ponta-a-ponta, protegendo mais a informação trocada.

### 3 **Seja cuidadoso com a webcam e o microfone**

Ligue a webcam e o microfone no uso das plataformas apenas quando for estritamente necessário. Por vezes, as sessões são gravadas e deixamos de ter controlo sobre a privacidade dos nossos dados. Lembre-se também de que a webcam e o microfone podem ser acedidos remotamente. Desligue-os após a sua utilização! Para o fazer, aceda às configurações de privacidade do seu computador.

### 5 **Controle a partilha de ecrã**

Algumas destas plataformas permitem que qualquer pessoa partilhe o que está a ver no seu ecrã, com o grupo. O anfitrião pode impedir que isso aconteça, ao organizar reuniões em que apenas este possa partilhar o que vê no ecrã. Se possível, caso partilhe algum conteúdo no ecrã, utilize uma marca de água de modo a proteger a sua propriedade intelectual.

### 7 **“Tranque a porta”**

Algumas destas plataformas permitem impedir que novos utilizadores entrem numa reunião que já começou, mesmo que tenham o link de acesso ou a palavra-chave. Para isso basta “trancar a porta”. Assim impede que estranhos acessem à reunião depois do seu início.

### 9 **Escolha as opções de gravação mais adequadas**

Para reduzir riscos, o administrador da reunião, caso a plataforma ofereça essa opção, pode decidir que participantes podem gravar a mesma. No entanto, isto só o protege do uso indevido da aplicação, ou seja, o controle da privacidade total não é garantido, pois continua a existir a possibilidade de gravar a conversação, através de software externo.

### 2 **Mantenha o software atualizado**

É importante assegurar que está a usar a última versão disponível do software, devendo certificar-se de que está a proceder às devidas atualizações. Ao fazê-lo, não só obtém novas opções e funcionalidades, como também instala pacotes de segurança.

### 4 **Utilize formas seguras de convidar os participantes**

Estas plataformas oferecem formas distintas de convidar participantes, como partilhar o URL da chamada com qualquer contacto, o que dá poucas garantias de segurança. Deve utilizar sempre um método seguro, que inclui o envio de um identificador e de uma palavra-passe. Pode ainda exigir que os utilizadores sejam autenticados mediante um login nas plataformas antes de aceder a uma sessão.

### 6 **Crie uma sala de espera**

Certas plataformas permitem criar uma sala de espera virtual, antes de a reunião começar. Isso pode ajudar a monitorizar os convidados que vão chegando, selecionando os que podem ou não participar, e permitir apresentar as regras da reunião.

### 8 **Desligue a partilha nas mensagens**

Sempre que estas plataformas permitam impedir o envio de ficheiros no serviço de mensagens, por parte dos participantes, selecione essa opção. Esta funcionalidade é útil para impedir a difusão de conteúdo perigoso (vírus informáticos, por exemplo), durante conversas com grupos maiores.

### 10 **Não se esqueça de outros cuidados**

É importante manter outros cuidados de ciber-higiene que podem ser relevantes para a segurança no uso destas plataformas: use palavras-chave fortes, altere-as com frequência e tenham uma por cada plataforma; faça backups regulares; não abra emails ou clique em anexos e links desconhecidos; evite trabalhar em Wi-Fi públicos; e siga as regras para uma boa palavra-chave no seu Wi-Fi doméstico.

