Crianças e jovens

Pais

Professores

Escolas

Estudo em Casa: Recomendações de Segurança

A Direção-Geral da Educação em articulação com o Centro Nacional de Cibersegurança e a Comissão Nacional de Proteção de Dados, disponibiliza um conjunto de recomendações e de orientações, a ter em conta na utilização das tecnologias de suporte ao ensino a distância.

Recomendações no uso de plataformas que permitem a comunicação áudio e vídeo

A Direção-Geral da Educação, no âmbito do Centro de Sensibilização SeguraNet, e o Centro Nacional de Cibersegurança disponibilizam um conjunto de recomendações no uso de plataformas que permitem a comunicação áudio e vídeo dirigidas a professores e a pais/encarregados de educação.

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.

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.

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.

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.

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.

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.

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 acedam à reunião depois do seu início.

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.

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.

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.

(ver modo de impressão)

Recomendações de segurança CNCS

O Centro Nacional de Cibersegurança disponibiliza também recomendações de segurança específicas para um conjunto de plataformas, nomeadamente:

Estudo em casa: Recomendações de segurança- Plataforma ZOOM

Estudo em Casa

Recomendações de segurança

Plataforma ZOOM

ZOOM - Versão: 4.6.10 (20033.0407)

Acesso à plataforma

A preparação da videoconferências pode ser feita através da plataforma ZOOM em linha (Figura 1) ou através da aplicação cliente instalada no dispositivo (Figura 2).

Em qualquer das situações, no momento da autenticação do utilizador, recomenda-se a inativação da opção "Continuar conectado" (*"Keep me signed in"*).

Fig.1

Efetuar Login

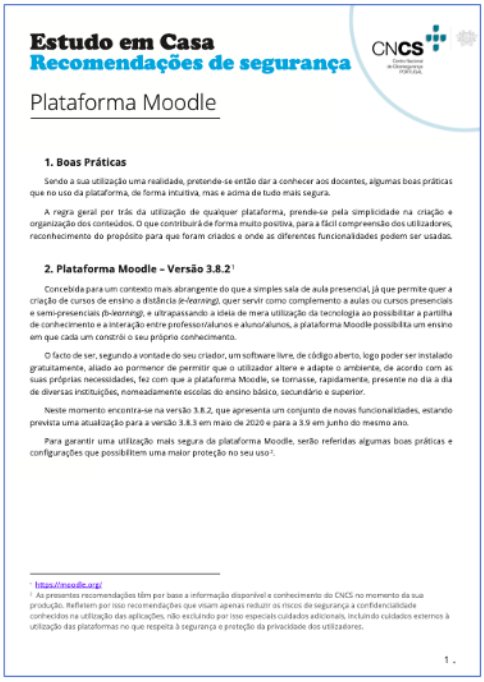
Fig.2

Sign In

1 .

(ver modo de impressão)

Estudo em casa: Recomendações de segurança - Plataforma Moodle



Estudo em Casa
Recomendações de segurança

Plataforma Moodle

1. Boas Práticas

Sendo a sua utilização uma realidade, pretende-se então dar a conhecer aos docentes, algumas boas práticas que no uso da plataforma, de forma intuitiva, mas e acima de tudo mais segura.

A regra geral por trás da utilização de qualquer plataforma, prende-se pela simplicidade na criação e organização dos conteúdos. O que contribuirá de forma muito positiva, para a fácil compreensão dos utilizadores, reconhecimento do propósito para que foram criados e onde as diferentes funcionalidades podem ser usadas.

2. Plataforma Moodle – Versão 3.8.2[1]

Concebida para um contexto mais abrangente do que a simples sala de aula presencial, já que permite quer a criação de cursos de ensino a distância (*e-learning*), quer servir como complemento a aulas ou cursos presenciais e semi-presenciais (*b-learning*), e ultrapassando a ideia de mera utilização da tecnologia ao possibilitar a partilha de conhecimento e a interação entre professor/alunos e aluno/alunos, a plataforma Moodle possibilita um ensino em que cada um constrói o seu próprio conhecimento.

O facto de ser, segundo a vontade do seu criador, um software livre, de código aberto, logo poder ser instalado gratuitamente, aliado ao pormenor de permitir que o utilizador altere e adapte o ambiente, de acordo com as suas próprias necessidades, fez com que a plataforma Moodle, se tornasse, rapidamente, presente no dia a dia de diversas instituições, nomeadamente escolas do ensino básico, secundário e superior.

Neste momento encontra-se na versão 3.8.2, que apresenta um conjunto de novas funcionalidades, estando prevista uma atualização para a versão 3.8.3 em maio de 2020 e para a 3.9 em junho do mesmo ano.

Para garantir uma utilização mais segura da plataforma Moodle, serão referidas algumas boas práticas e configurações que possibilitem uma maior proteção no seu uso[2].

[1] https://moodle.org/

[2] As presentes recomendações têm por base a informação disponível e conhecimento do CNCS no momento da sua produção. Refletem por isso recomendações que visam apenas reduzir os riscos de segurança a confidencialidade conhecidos na utilização das aplicações, não excluindo por isso especiais cuidados adicionais, incluindo cuidados externos à utilização das plataformas no que respeita à segurança e proteção da privacidade dos utilizadores.

1 .

(ver modo de impressão)

Estudo em casa: Recomendações de segurança - Plataforma Microsoft Teams

Estudo em Casa
Recomendações de segurança

Plataforma Microsoft Teams

1. Microsoft Teams – Versão 1.3.00.4461

O Microsoft Teams é uma plataforma unificada de comunicação e colaboração que combina chat, videoconferências, armazenamento de arquivos (incluindo colaboração em arquivos) e integração de aplicativos no local de trabalho. Faz parte do pacote de produtividade do Office 365 e apresenta extensões para poderem ser integradas a produtos que não são da Microsoft.

Lançada em 2016 pela Microsoft, é considerado um software colaborativo e encontra-se disponível em 26 idiomas diferentes. Na página de início da plataforma, permite o início da sessão (Figura 1).

Fig 1

Para efeito deste documento, vão ser efetuadas um conjunto de recomendações, que que no uso da plataforma, de forma intuitiva, mas e acima de tudo mais segura [1], sendo que para a função a que se destina, será referida a versão para educação [2].

[1] As presentes recomendações têm por base a informação disponível e conhecimento do CNCS no momento da sua produção. Refletem por isso recomendações que visam apenas reduzir os riscos de segurança a confidencialidade conhecidos na utilização das aplicações, não excluindo por isso especiais cuidados adicionais, incluindo cuidados externos à utilização das plataformas no que respeita à segurança e proteção da privacidade dos utilizadores.

[2] https://www.microsoft.com/pt-pt/education/products/teams

1 .

(ver modo de impressão)

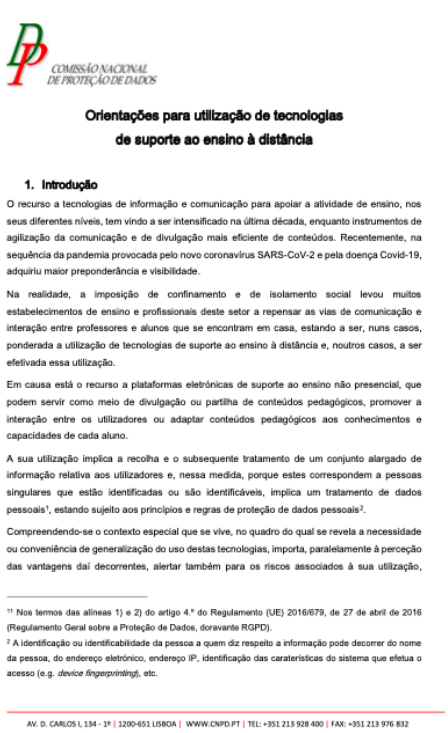
Estudo em casa: Recomendações de segurança - Plataforma Google Classroom

(a disponibilizar brevemente)

Orientações CNPD

A Direção-Geral da Educação destaca ainda as orientações emanadas pela Comissão Nacional de Proteção de Dados, com o objetivo de proteger os

dados pessoais e minimizar o impacto sobre os direitos dos respetivos titulares.



COMISSÃO NACIONAL DE PROTEÇÃO DE DADOS

Orientações para utilização de tecnologias de suporte ao ensino à distância

1. Introdução

O recurso a tecnologias de informação e comunicação para apoiar a atividade de ensino, nos seus diferentes níveis, tem vindo a ser intensificado na última década, enquanto instrumentos de agilização da comunicação e de divulgação mais eficiente de conteúdos. Recentemente, na sequência da pandemia provocada pelo novo coronavírus SARS-CoV-2 e pela doença Covid-19, adquiriu maior preponderância e visibilidade.

Na realidade, a imposição de confinamento e de isolamento social levou muitos estabelecimentos de ensino e profissionais deste setor a repensar as vias de comunicação e interação entre professores e alunos que se encontram em casa, estando a ser, nuns casos, ponderada a utilização de tecnologias de suporte ao ensino à distância e, noutros casos, a ser efetivada essa utilização.

Em causa está o recurso a plataformas eletrónicas de suporte ao ensino não presencial, que podem servir como meio de divulgação ou partilha de conteúdos pedagógicos, promover a interação entre os utilizadores ou adaptar conteúdos pedagógicos aos conhecimentos e capacidades de cada aluno.

A sua utilização implica a recolha e o subsequente tratamento de um conjunto alargado de informação relativa aos utilizadores e, nessa medida, porque estes correspondem a pessoas singulares que estão identificadas ou são identificáveis, implica um tratamento de dados pessoais[1], estando sujeito aos princípios e regras de proteção de dados pessoais[2].

Compreendendo-se o contexto especial que se vive, no quadro do qual se revela a necessidade ou conveniência de generalização do uso destas tecnologias, importa, paralelamente à perceção das vantagens daí decorrentes, alertar também para os riscos associados à sua utilização,

[1] Nos termos das alíneas 1) e 2) do artigo 4.º do Regulamento (UE) 2016/679, de 27 de abril de 2016 (Regulamento Geral sobre a Proteção de Dados, doravante RGPD).
[2] A identificação ou identificabilidade da pessoa a quem diz respeito a informação pode decorrer do nome da pessoa, do endereço eletrónico, endereço IP, identificação das características do sistema que efetua o acesso (e.g. *device fingerprinting*), etc.

AV. D. CARLOS I, 134 - 1º | 1200-651 LISBOA | WWW.CNPD.PT | TEL: +351 213 928 400 | FAX: +351 213 976 832

(ver modo de impressão)

ATIVIDADES FEVEREIRO	QUEM SOMOS
CONTACTOS	INTERNET SEGURA
LINHA INTERNET SEGURA	LINHA ALERTA