Escola Secundária de Caldas das Taipas

# POLÍTICA DE SEGURANÇA DIGITAL DA ESCT


JANEIRO DE 2023

# ÍNDICE

# 1. OBJETIVOS E ÂMBITO DA POLÍTICA DE SEGURANÇA DIGITAL

A Escola Secundária de Caldas das Taipas, adiante designada apenas por ESCT, acredita que a Segurança Digital (*eSafety*) é um elemento essencial de salvaguarda das crianças, jovens e adultos no mundo digital, ao usar tecnologia, como computadores, *tablets*, telemóveis, entre outros.

A ESCT reconhece que a Internet e as tecnologias de informação e comunicação são uma parte importante da vida quotidiana, pelo que os alunos devem ser apoiados para serem capazes de aprender a desenvolver estratégias de gestão e resposta ao risco *online*.

A ESCT tem o dever, de acordo com as suas possibilidades técnicas e disponibilidade de recursos, de proporcionar à comunidade docente pontos de acesso à Internet de qualidade para elevar os padrões de educação, promover a realização de atividades, apoiar o trabalho profissional e melhorar as funções de gestão.

A ESCT identifica que há uma clara necessidade de garantir que todos os alunos e funcionários estão protegidos dos potenciais perigos *online*.

A Política de Segurança Digital é, por isso mesmo, essencial na definição de princípios nucleares de ação, que todos os elementos da comunidade escolar devem aplicar.

Os objetivos da Política de Segurança Digital são:

1. Identificar claramente os princípios fundamentais, seguros e responsáveis esperados de todos os membros da comunidade em relação à tecnologia como forma de garantir que a Escola seja um ambiente seguro no que concerne à utilização de equipamentos eletrónicos e da Internet;
2. Sensibilizar todos os elementos da comunidade Escolar sobre os potenciais riscos, bem como dos benefícios da tecnologia;
3. Permitir que todos os elementos da comunidade Escolar possam trabalhar com segurança e responsabilidade;

4. Identificar procedimentos claros a adotar de forma a responder às preocupações de segurança online que são conhecidos por todos os membros da comunidade escolar.

A Política de Segurança Digital aplica-se a todos os elementos da comunidade escolar.

Esta Política aplica-se a todos os dispositivos de acesso à Internet e utilização de dispositivos de comunicação e informação, incluindo dispositivos pessoais, ou outros que tenham sido fornecidos a alunos, funcionários ou outras pessoas.

A Política de Segurança Digital, redigida pela ESCT e aprovada pelos órgãos próprios, tem por base a Política do Selo de Segurança Digital (*eSafety*) e a legislação em vigor.

## 1.1.A IMPORTÂNCIA DA UTILIZAÇÃO DA INTERNET

Fazendo a Internet parte integrante do currículo e ferramenta essencial no processo de ensino-aprendizagem e de administração escolar, deve (in)formar-se todos os elementos da comunidade escolar sobre a utilização responsável da mesma (nomeadamente no que concerne ao respeito pelos direitos de autor), bem sobre o que é e o que não é uma utilização aceitável da Internet, em consonância com as boas práticas relativas à segurança digital.

O acesso à Internet, pelos alunos, faz-se única e exclusivamente pela VLAN[1] reservada para esse efeito na rede minedu, de modo a não pôr em causa a segurança dos dados dos professores, dos serviços administrativos e da Direção.

[1] A infraestrutura de rede da ESCT é constituída por várias VLAN's de trabalho, diferenciando-se o acesso às mesmas por tipologia de utilizador (Alunos, Clientes Alunos Salas TIC, Clientes Professores, Clientes Administrativos e outras de segurança)

# 2. GESTÃO DE SISTEMAS DE INFORMAÇÃO

## 2.1. DIRETRIZES PARA A MANUTENÇÃO DA SEGURANÇA DOS SISTEMAS DE INFORMAÇÃO

- A segurança dos sistemas informáticos da ESCT e dos utilizadores será revista regularmente.
- Os antivírus, nomeadamente os dos servidores, serão atualizados automaticamente e as licenças renovadas sempre que necessário.
- Os dados pessoais enviados através da Internet ou transferidos para fora da ESCT estão protegidos pelos sistemas de segurança dos programas utilizados, tendo em conta as recomendações da Comissão Nacional de Proteção de Dados.
- Os dispositivos amovíveis serão utilizados de acordo com as autorizações específicas de cada serviço, devendo ser feita uma análise com o antivírus.
- A instalação de software para fins educativos nos Desktop e portáteis deve ser autorizada pelo Coordenador da Segurança Digital e supervisionada, preferencialmente, por um dos assessores/professores de TIC.
- Os utilizadores não devem colocar / deixar ficheiros de uso pessoal nos PCs ou nos dispositivos móveis. Após a utilização, nomeadamente para atividades letivas, todos os ficheiros devem ser removidos. Nos dispositivos móveis, os utilizadores também devem ter o cuidado de remover todas as contas pessoais associadas a aplicações.
- A capacidade e o funcionamento dos sistemas informáticos deverão ser analisados, pelo menos, uma vez por ano letivo.
- É obrigatória a utilização de nomes de utilizador e palavras-passe para aceder à rede da ESCT.

## 2.2. DIRETRIZES PARA A GESTÃO DO CORREIO ELETRÓNICO

- A ESCT disponibiliza contas de correio eletrónico aos professores, alunos, funcionários e encarregados de educação, e a comunicação institucional é feita preferencialmente por esta via.
- Os grupos de contactos de correio eletrónico são geridos centralmente com o objetivo de facilitar o trabalho dos utilizadores.
- A comunicação com instituições para tratamento de assuntos oficiais da ESCT deve ser realizada a partir de endereços eletrónicos institucionais.

- As mensagens de correio eletrónico enviadas para organizações externas devem obedecer a procedimentos de escrita e de protocolo similares aos do envio de ofícios por correio físico.
- A troca de mensagens com vários destinatários deve ser feita preferencialmente em cópia oculta (Bcc - "blind carbon copy").
- A troca de mensagens com encarregados de educação é feita para as suas contas institucionais.
- O reencaminhamento de mensagens em cadeia deve ser evitado e a difusão de informação em grupo deve ser cuidadosa, de modo a evitar o *spam* (correio não desejado).

## 2.3. DIRETRIZES PARA A GESTÃO DOS CONTEÚDOS PUBLICADOS

- As informações de contacto no sítio da ESCT devem ser a morada, os números de telefone e o email da ESCT. Não deve ser publicada qualquer informação pessoal de alunos ou professores.
- A publicitação online de horários das turmas e a listagem dos alunos das turmas só será efetuada se os sistemas garantirem um acesso restrito a alunos e a pais e encarregados de educação, com palavras-passe robustas.
- Não serão publicadas pautas online e as pautas afixadas em papel nos locais de estilo seguirão as recomendações da Comissão Nacional sobre Proteção de Dados relativas a faltas e outros dados de natureza pessoal.
- O Diretor é o responsável editorial geral pelos conteúdos digitais publicados pela ESCT na Internet e deve assegurar que os conteúdos publicados são corretos e adequados.
- Todas as publicações em formato digital da responsabilidade de membros da ESCT devem respeitar os direitos de propriedade intelectual, as políticas de privacidade e os direitos de autor.

## 2.4. PUBLICAÇÃO DE FOTOGRAFIAS, DE GRAVAÇÕES DE VOZ E DE TRABALHOS DE ALUNOS

- Antes da publicação de imagens ou de gravações vídeo e audío que incluam alunos, deve ser garantida a autorização expressa e informada, de acordo com a legislação aplicável.
- A publicação em linha, em rede aberta ou circuito fechado, de imagens dos alunos ou de gravações contendo a sua voz só são admissíveis se não houver uma relação direta entre a imagem e o som e o nome dos alunos, reduzindo, assim, significativamente, a possibilidade de identificação dos alunos.

- A captação de imagens dos alunos deve, preferencialmente, ser executada de longe ou de ângulos que reduzam significativamente a possibilidade de identificação.
- Os professores não devem recolher imagens ou voz dos alunos com os seus dispositivos pessoais e não podem publicar diretamente imagens ou outros registos dos alunos nas suas redes sociais pessoais.
- O consentimento por escrito será mantido pela Escola, sempre que as imagens de alunos forem utilizadas para fins de publicidade, até as imagens em causa deixarem de ser usadas.
- Os trabalhos de alunos a publicar online devem ter em conta as referências bibliográficas e os direitos de autor.

## 2.5. GESTÃO DE COMUNIDADES SOCIAIS VIRTUAIS, REDES SOCIAIS E PUBLICAÇÕES PESSOAIS

- Através de atividades dinamizadas pelos professores em sala de aula e outros espaços e estruturas escolares, os alunos serão sensibilizados sobre o uso aceitável da Internet e das redes sociais, de modo a protegerem a sua privacidade e a dos outros, a evitarem a divulgação de dados pessoais, a negarem o acesso a desconhecidos e a bloquearem comunicações não desejadas.
- Os professores que pretendam utilizar ferramentas das redes sociais com os alunos em atividades curriculares devem avaliar o risco dos sítios na Internet, antes de os utilizarem e verificar os termos e condições dos mesmos, de modo a garantir que são adequados às idades dos alunos.
- A ESCT promoverá campanhas de sensibilização de pais/encarregados de educação sobre a utilização segura de redes sociais e outros sítios de publicação de dados pessoais. Estas ações de sensibilização para o uso seguro da Internet podem vir a ser organizadas em colaboração com a Associação de Pais e Encarregados de Educação da ESCT.

## 2.6. GESTÃO DOS SISTEMAS DE FILTRAGEM

- O acesso à Internet fornecido pela ESCT inclui sistemas de filtragem de conteúdos impróprios, geridos centralmente pelo organismo que gere a rede minedu escolar.
- Os professores que encontrarem sites bloqueados com interesse pedagógico ou sites impróprios que estão desbloqueados devem reportar essa informação ao responsável na ESCT pela rede minedu que através de plataforma própria solicitará o pedido de atualização à Direção-Geral de Estatísticas da Educação e Ciência.

# 3. DECISÕES QUANTO ÀS POLÍTICAS

## 3.1. AUTORIZAÇÃO DO ACESSO À INTERNET

- Pessoal docente, não docente e alunos estão autorizados a aceder à Internet, desde que o façam de forma responsável e no âmbito das suas funções.
- No ato da matrícula, os pais/encarregados de educação terão conhecimento da Política de Segurança Digital e das Políticas de Utilização Aceitável.

## 3.2. RESOLUÇÃO DE INCIDENTES RELATIVOS À SEGURANÇA DIGITAL

- Todos os elementos da ESCT deverão informar o Coordenador da Segurança Digital de situações preocupantes, do ponto de vista da segurança digital (tais como violações do sistema de filtragem, *cyberbullying*, conteúdos ilícitos, utilização inadequada de equipamento, etc.).
- O Coordenador da Segurança Digital tomará as providências necessárias para resolver os incidentes de segurança digital, nomeadamente nos casos de *cyberbullying*.
- A aplicação de medidas para superação de problemas relativos à segurança digital, incluindo os que possam implicar a aplicação de medidas disciplinares, deve ser articulada com os responsáveis pelos serviços onde ocorreram os problemas.

## 3.3. GESTÃO DOS CASOS DE *CYBERBULLYING*

- O *cyberbullying* não será tolerado e todos os incidentes detetados serão comunicados à Direção, ao Coordenador da Segurança Digital e às autoridades competentes, quando necessário.
- Aos alunos serão disponibilizadas atividades e sessões, dinamizadas por diferentes entidades da ESCT, de sensibilização para as questões do *cyberbullying*.
- Todos os incidentes de *cyberbullying* comunicados serão investigados, aplicando-se, quando necessário, os procedimentos de inquirição usados nos processos disciplinares e as sanções que se consideram adequadas, tal como estabelecido no Regulamento Interno.
- Nas situações que tenham origem fora da ESCT envolvendo elementos da comunidade educativa, deve informar-se a Direção, para a ESCT poder ter um papel ativo e desencadear os procedimentos entendidos como necessários.

### 3.4. GESTÃO DE TELEMÓVEIS E EQUIPAMENTOS PESSOAIS

- Em sessões de sensibilização e atividades dirigidas a alunos, dinamizadas, quando possível, em articulação com as atividades curriculares, os alunos serão instruídos quanto à utilização segura e adequada de telemóveis e outros equipamentos pessoais e serão sensibilizados para os limites e consequências dos seus atos.
- Os telemóveis ou equipamentos pessoais não podem ser utilizados durante as aulas ou tempos letivos formais e outras atividades dentro e fora da ESCT (devendo, por isso, estar desligados), a não ser para efeitos pedagógicos devidamente autorizados, orientados e supervisionados pelo professor.
- A utilização de telemóveis e outros equipamentos em períodos letivos está condicionada ao consentimento por parte do docente responsável.

## 4. CONHECIMENTO DAS POLÍTICAS

- A Política de Segurança Digital está disponível, para conhecimento e consulta, no sítio Web da Escola.
- A Escola incentiva os docentes da Escola a frequentar formações atualizadas e adequadas sobre a utilização segura e responsável da Internet, e promove atividades de esclarecimento junto do pessoal não docente, alunos e pais / encarregados de educação.

## 5. CASOS OMISSOS

- Nos casos omissos, aplicar-se-á o que consta no Regulamento Interno, e na lei geral.

Escola Secundária de Caldas das Taipas

# PLANO DE SEGURANÇA DIGITAL DA ESCT

JANEIRO DE 2023