POLÍTICA DE SEGURANÇA DIGITAL

ESCOLA SECUNDÁRIA ARQUITECTO OLIVEIRA FERREIRA

Orientações para o uso da Internet e dos dispositivos digitais em segurança e como recurso educativo.

Índice

1. Política de Segurança Digital (eSafety)

A segurança digital é um elemento de salvaguarda da confidencialidade, de integridade, de disponibilidade e da autenticidade de documentos e dados pessoais, informação pessoal de identificação sensível e não sensível (IPIS e IPINS) de crianças, jovens e adultos enquanto utilizadores do mundo digital, navegadores na internet, por meio de tecnologias e equipamentos diversos.

A troca de ideias, de opiniões, de experiências, a interação social online e as oportunidades de aprendizagem daí decorrentes apresentam enormes benefícios para todos, mas podem, por vezes, colocar crianças, jovens e adultos em perigo. A segurança digital abrange questões relacionadas não só com crianças e jovens, mas também com adultos e com a utilização que todos fazem da Internet e de todos os dispositivos que permitem a comunicação eletrónica em ambiente escolar e fora dele. Isto exige a atenção e a formação de todos os elementos da comunidade escolar sobre os riscos e as responsabilidades envolvidas e faz parte do cuidado inerente à função de cada educador. Todos os educadores e professores devem, pois, ter consciência da importância das boas práticas de segurança digital, visando a educação, a proteção e a formação das crianças e dos jovens sob o seu cuidado para o correto e adequado uso das tecnologias. 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.

O Coordenador da Política de Segurança Digital é designado pelo diretor e funciona como elemento de articulação com a Direção. A política de Segurança Digital, redigida com base na Política do Selo de Segurança Digital e na legislação aplicável, será revista anualmente.

2. Ensino e aprendizagem

2.1. A importância da utilização da Internet

- Devendo fazer parte integrante do currículo como uma ferramenta essencial na aprendizagem, a utilização da Internet na ESAOF deve elevar os padrões educativos, promover o sucesso dos alunos, apoiar o trabalho dos professores e reforçar a administração escolar.
- O acesso à Internet é um direito dos alunos e deverão demonstrar responsabilidade e maturidade na sua utilização.
- Os níveis de acesso à Internet são estabelecidos de acordo com os requisitos do currículo, idade e capacidades dos alunos.
- Todas as atividades escolares que impliquem o uso da Internet devem integrar a apresentação da *webgrafia*.

2.2. Benefícios da utilização da Internet no ensino

- Os benefícios da utilização da Internet no ensino incluem:
- Acesso a recursos pedagógicos e educativos.
- Intercâmbio cultural e educativo entre alunos de várias escolas, países e realidades.
- Utilização social, recreativa e de lazer nas bibliotecas, nos clubes e em casa.
- Acesso de alunos e professores a diferentes áreas de conhecimento.
- Maior acesso a apoio técnico, designadamente gestão remota de redes e atualizações automáticas de programas.
- Desenvolvimento profissional dos professores através do acesso a materiais pedagógicos e aplicações eficazes do currículo.
- Possibilidade de aprendizagem quando e onde for mais conveniente.
- Colaboração no âmbito de redes de escolas, serviços de apoio e associações profissionais.

2.3. Utilização da Internet com vista à melhoria da aprendizagem

- O acesso à Internet na ESAOF deve ser pensado com vista a alargar e a reforçar a educação.
- A cópia e a utilização subsequente de materiais obtidos na Internet, por alunos e professores, devem cumprir a legislação em matéria de direitos de autor, incluindo o conhecimento dos vários tipos de licenciamento disponíveis na Web e as regras de utilização dos recursos educativos abertos.
- A ESAOF assegurará que a utilização de materiais disponíveis na Internet e a sua forma de uso por professores e alunos vai ao encontro do que está presente na estrutura de licenciamentos dos recursos educativos abertos.
- Nas atividades de ensino e aprendizagem dever-se-á ensinar aos alunos o que é e o que não é uma utilização aceitável da Internet, e ser-lhes-ão indicados objetivo claros, quando utilizam a Internet, tendo em conta o currículo e a idade.
- Todas as atividades escolares que impliquem o uso da Internet devem permitir aos alunos aprender a pesquisar e a avaliar/validar informação, de acordo com a sua autoria, pertinência e rigor.

2.4. Avaliação de conteúdos

- Deve-se ensinar os alunos a serem críticos em relação aos materiais que leem e consequentemente validar uma informação antes de aceitar a sua exatidão.
- Deve-se orientar os alunos para o uso de ferramentas de pesquisa, adequadas à sua idade.
- A avaliação de materiais da Internet faz parte do processo de ensino e de aprendizagem de qualquer disciplina e é um requisito transversal à escola e ao currículo sendo, ainda, da responsabilidade do professor.

3. Gestão de sistemas de informação

3.1. Manutenção da segurança dos sistemas de informação

- A segurança dos sistemas informáticos da ESAOF é revista anualmente.
- A proteção antivírus é atualizada frequentemente.
- Os dados pessoais enviados através da Internet ou transferidos para fora da escola estão protegidos pelos sistemas de segurança dos programas utilizados.
- O/a gestor/a da rede analisará a capacidade e o funcionamento do sistema com regularidade.
- Os dispositivos amovíveis são utilizados de acordo com as autorizações específicas de cada serviço, estando os sistemas preparados para uma análise automática com antivírus.
- Os utilizadores não podem instalar qualquer software. A instalação de software para fins educativos deve ser autorizada pelo Coordenador PTE/Direção da ESAOF.
- Após a utilização, nomeadamente para atividades letivas, todos os ficheiros devem ser removidos.
- A capacidade e o funcionamento dos sistemas informáticos são analisados, pelo menos, uma vez por ano letivo.
- É obrigatória a autenticação para aceder à rede da escola.
- A página inicial de navegação de cada computador ao serviço dos utilizadores é definida pela ESAOF e não devem, em circunstância alguma, ser alteradas as páginas.

3.2. Gestão do correio eletrónico

- A administração da conta de correio eletrónico institucional da escola é da responsabilidade do Coordenador PTE/Direção.
- Todos os membros do pessoal docente, não docente e discente devem possuir um endereço de correio eletrónico institucional a ser usado para qualquer comunicação oficial.

- Qualquer comunicação eletrónica, que contenha conteúdo que possa violar a legislação de proteção de dados (por exemplo, informações confidenciais ou pessoais), só será enviada como email seguro.
- Os membros da comunidade escolar devem avisar imediatamente o Coordenador PTE se receberem comunicação ofensiva e esta será gravada de forma a agir apropriadamente.
- As mensagens de correio eletrónico enviadas a organizações externas devem ter o mesmo rigor e formalidade, que uma comunicação oficial escrita em papel timbrado da escola.
- O(s) endereço(s) de correio eletrónico da escola e outros detalhes de contacto oficiais não poderão ser utilizados para a criação de contas pessoais em redes sociais.
- Os alunos têm de informar imediatamente o professor designado para o efeito caso recebam mensagens de email ofensivas.
- Os alunos não podem revelar dados pessoais sobre eles próprios ou outros numa mensagem eletrónica, nem combinar encontrar-se com alguém sem autorização expressa de um adulto.
- O acesso a contas de email pessoais dentro da escola pode ser bloqueado.
- A utilização excessiva do email para fins sociais pode interferir com a aprendizagem e será restringida
- A comunicação com alunos, pais / encarregados de educação e com instituições para tratamento de assuntos oficiais da ESAOF deve ser preferencialmente realizada a partir de endereços eletrónicos institucionais.
- O reencaminhamento de mensagens em cadeia deve ser evitado e a difusão de informação em grupo dever ser cuidadosa, de modo a evitar ser objeto de spam.

3.3. Gestão dos conteúdos publicados

- A página da ESAOF deve conter o endereço físico da escola, as hiperligações autorizadas, o endereço de correio eletrónico oficial e o número de telefone e/ou fax. Não deve ser publicada qualquer informação pessoal de alunos ou professores.

- O responsável editorial geral pelos conteúdos digitais publicados pela ESAOF na Internet é nomeado pelo Diretor e deve assegurar que os conteúdos publicados são corretos e adequados.
- Todas as publicações em formato digital da responsabilidade de membros da ESAOF devem respeitar os direitos de propriedade intelectual, as políticas de privacidade e os direitos de autor.
- A conta de administrador da página oficial da escola será salvaguardada com uma senha
- apropriadamente forte.
- A escola irá postar informações sobre a salvaguarda, incluindo a segurança online, no sítio oficial da escola, para os membros da comunidade, incluindo esta PSD.

3.4. Publicação de fotografias e trabalhos de alunos

- A ESAOF tem uma política clara relativamente à utilização de imagens de alunos onde se definem regras e procedimentos (Política de Utilização de Imagem). No início do ano, todos os EE assinam a permissão para o efeito.
- A escola garantirá que todas as imagens e vídeos compartilhados online serão utilizados de acordo com a Política de Utilização de Imagem da ESAOF.
- A ESAOF garante igualmente que todo o uso de imagens, vídeos ou outro material digital se realiza em conformidade com outras políticas e procedimentos, incluindo a segurança e proteção dos dados, Políticas de Utilização Aceitável e códigos de conduta.
- Na publicação de imagens e/ou gravações de vídeo que incluam alunos, deve ser garantida a proteção da imagem dos alunos, de acordo com a legislação aplicável.
- Os nomes completos dos alunos não serão utilizados em parte alguma do página da ESAOF, em especial junto a fotografias.
- A publicação de qualquer imagem e/ou vídeo de alunos, será feita apenas, depois de obtida autorização por escrito dos pais e /ou encarregados de educação.
- Os trabalhos de alunos podem ser publicados, desde que não estejam identificados, ou após obtida autorização por escrito dos pais e /ou encarregados de educação.

3.5. Gestão de comunidades sociais virtuais, redes sociais e publicações pessoais

- Através de atividades dinamizadas pelos professores em sala de aula e pelo Serviço das Bibliotecas Escolares, os alunos são ensinados a usar a Internet e as redes sociais, de modo a protegerem a sua privacidade, 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.
- O uso oficial das redes sociais pela escola visa exclusivamente o trabalho educacional, através da divulgação ou comunicação destinada, por exemplo, a aumentar o envolvimento dos pais e encarregados de educação.
- Qualquer publicação online em sites oficiais ou de rede social deverá cumprir os requisitos legais, incluindo a Lei de Proteção de Dados, o direito à privacidade ou a obrigação em proteger informação privada Política de Segurança Digital 17 e não deverá violar qualquer dever de direito comum de confidencialidade, direitos de autor, Cyberbullying, etc.

3.6. Gestão dos sistemas de filtragem

- O acesso à Internet fornecido pela ESAOF inclui sistemas de filtragem adequados à idade e à maturidade dos alunos.
- A ESAOF deve garantir que os sistemas adequados de filtragem e controlo estão implementados, de forma a evitar que a comunidade escolar não possa aceder a conteúdo inadequado ou ilegal.
- Todos os membros da comunidade escolar que violarem os sistemas de filtragem ou acederem a sítios com conteúdos inadequados ao espaço escolar serão alvo de procedimento disciplinar.
- Serão feitas verificações regulares, para comprovar a eficácia dos métodos de filtragem adotados.

4. Decisões quanto às políticas

4.1. Autorização do acesso à Internet

- A ESAOF mantém um registo atualizado de todos os alunos e professores que são autorizados a aceder às comunicações eletrónicas da escola.
- Todos os elementos da comunidade devem ter conhecimento da Política de Segurança Digital e dos recursos para a utilização segura da Internet, que estarão disponíveis na página da ESAOF.
- Os pais e encarregados de educação deverão serão informados que é fornecido aos alunos acesso supervisionado à Internet, apropriado para a sua idade e capacidades.
- Os pais e encarregados de educação serão convidados a ler/ analisar a Política de Utilização Aceitável para o acesso dos alunos, com os seus filhos/ educandos.
- Ao considerar o acesso para os membros vulneráveis da comunidade (nomeadamente, os alunos com necessidades educativas especiais), a escola tomará as decisões com base nas necessidades específicas e compreensão do(s) aluno(s).
- O acesso à rede de Internet da escola está vedado a todos os visitantes, exceto em caso de necessidade extrema e mediante autorização do Coordenador PTE/Direção.

4.2. Resolução de incidentes relativos à Segurança Digital

- Todos os elementos da comunidade escolar deverão informar o do Coordenador PTE/Direção caso tenham conhecimento 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).
- As queixas relativas à utilização indevida da Internet são tratadas no quadro dos procedimentos de apresentação de queixas ou denúncias adotadas pela escola.
- 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.

- Sempre que houver razões para crer ou recear que ocorreu ou está a ocorrer alguma atividade ilegal, a ESAOF contactará a Equipa de Proteção de Menores, através da Direção, encaminhando a situação para a Polícia.

4.3. Gestão dos casos de cyberbullying

- O cyberbullying (assim como todas as outras formas de bullying) não será tolerado e todos os incidentes detetados serão comunicados à Direção e às autoridades competentes, quando necessário.
- Alunos, professores e pais/encarregados de educação serão aconselhados a manter um registo do bullying como prova.
- Serão adotados procedimentos claros para investigar incidentes ou alegados casos de cyberbullying.
- Será solicitado a alunos, professores e pais/encarregados de educação que trabalhem em conjunto com a escola de modo a apoiarem a abordagem da escola em relação ao cyberbullying e à segurança digital.
- Toda a comunidade escolar será sensibilizada para a importância de manter uma conduta adequada na Internet e de não publicar comentários, conteúdos, imagens ou vídeos na Internet que possam causar dano, prejuízo ou sofrimento a outros elementos da comunidade escolar.

4.4. Gestão de telemóveis e equipamentos pessoais

- Os telemóveis ou equipamentos pessoais não podem ser utilizados durante as aulas ou tempos letivos formais (devendo, por isso, estar desligados), a não ser para efeitos pedagógicos devidamente autorizados, orientados e supervisionados pelo professor.
- Os utilizadores são responsáveis por qualquer tipo de dispositivos eletrónicos que tragam para a escola. A escola não assume qualquer responsabilidade pela perda, roubo ou dano de tais objetos, nem por quaisquer efeitos prejudiciais para a saúde causados por estes dispositivos, sejam eles reais ou potenciais.

- Não é permitido levar telemóveis e outros equipamentos para os exames e/ou outras provas de avaliação. Os alunos que tenham um telemóvel na sua posse durante um exame estarão sujeitos às normas estabelecidas pelo Júri Nacional de Exames.
- Se um(a) aluno(a) necessitar de contactar os pais ou encarregado de educação, deve usar, preferencialmente, o telefone da escola ou contactar os pais ou encarregado de educação através do seu telemóvel, em período não letivo e fora de espaços como salas de aula, biblioteca, zonas comuns dos blocos e outros espaços onde possa perturbar o funcionamento dos serviços.
- Os pais e encarregados de educação não devem contactar os filhos/educandos para os telemóveis durante o horário letivo. Em caso de necessidade de contacto urgente devem usar o número de telefone da Escola.
- Os professores e educadores não devem, preferencialmente, utilizar os seus telemóveis ou equipamentos pessoais para contactar crianças ou jovens dentro ou fora da escola na sua qualidade de profissionais, a não ser em situações de emergência e quando outros meios de contacto não estejam operacionais.

5. Conhecimento das políticas

5.1. Conhecimento das políticas pelo pessoal docente, não docente e pais e encarregados de educação

- A Política de Segurança Digital estará disponível, para conhecimento e consulta, na página da ESAOF.