

POLÍTICA DE SEGURANÇA DIGITAL



**Agrupamento de Escolas
Dr. Carlos Pinto Ferreira**

Política de Segurança Digital

Usar a Internet e os dispositivos digitais em segurança.



Este documento foi elaborado a partir do modelo disponibilizado pela European Schoolnet (www.eun.org) e desenvolvido com recursos do Kent County Council. Está licenciado com uma Licença Creative Commons - Atribuição- Compartilha Igual 3.0.

Índice

1. Política de segurança digital

A segurança digital visa proteger a confidencialidade, integridade e disponibilidade de autenticidade de documentos e dados pessoais. Atualmente, crianças, jovens e adultos interagem diariamente com as mais diversas tecnologias (os telemóveis, as consolas de jogos, a Internet, etc...) e contactam, experimentam e vivenciam uma infindável variedade de oportunidades, atitudes e situações. A troca de ideias, opiniões, 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 formação de todos os elementos da comunidade escolar sobre os riscos e 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 do Agrupamento.

A política de Segurança Digital, redigida com base na Política do Selo de Segurança Digital e na legislação aplicável, será revista anualmente.

O/A Coordenador/a da Política de Segurança Digital _____

Política aprovada pelo Diretor _____

em 15 de março de 2017

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 no Agrupamento 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 que demonstrem responsabilidade e maturidade na sua utilização.
- Os níveis de acesso à Internet serão 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 das referências bibliográficas.

2.2. Benefícios da utilização da Internet no ensino

- Acesso a recursos pedagógicos e educativos.
- Intercâmbio cultural e educativo entre alunos de vários países.
- Desenvolvimento profissional dos professores através do acesso a materiais pedagógicos e aplicações eficazes do currículo.
- Maior acesso a apoio técnico, designadamente gestão remota de redes e atualizações automáticas de programas.
- Possibilidade de aprendizagem quando e onde for mais conveniente.

2.3. Utilização da Internet com vista à melhoria da aprendizagem

- O acesso à Internet no Agrupamento deve ser pensado com vista a alargar e 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 licenciamentos disponíveis na Web e as regras de utilização 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 objetivos

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 aos alunos a serem críticos em relação aos materiais que leem e a saber como validar uma informação antes de aceitar a sua exatidão.
- A avaliação de materiais da Internet faz parte do processo de ensino e de aprendizagem de qualquer disciplina e será considerada um requisito transversal à escola e ao currículo.

3. Gestão de sistemas de informação

3.1. Manutenção da segurança dos sistemas de informação

- A segurança dos sistemas informáticos do Agrupamento e dos utilizadores será revista anualmente.
- A proteção antivírus será 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 serão 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 da Segurança Digital e feita, preferencialmente por ele mesmo ou por quem ele designe
- Após a utilização, nomeadamente para atividades letivas, todos os ficheiros devem ser removidos.

- A capacidade e o funcionamento dos sistemas informáticos serão 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 será definida pela de acordo com as necessidades / interesses dos serviços. Os utilizadores não devem, em circunstância alguma, alterar as páginas de navegação pré-definidas.

3.2. Gestão do correio eletrónico

- A comunicação com alunos, pais / encarregados de educação e com instituições para tratamento de assuntos oficiais do Agrupamento deve ser preferencialmente 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.
- O reencaminhamento de mensagens em cadeia deve ser evitado e a difusão de informação em grupo deve ser cuidadosa, de modo a evitar ser objeto de spam.

3.3. Gestão dos conteúdos publicados

- As informações de contacto no sítio do agrupamento devem ser a morada, os números de telefone e o email do agrupamento. Não deve ser publicada qualquer informação pessoal de alunos ou professores.
- O responsável editorial geral pelos conteúdos digitais publicados pelo Agrupamento 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 do Agrupamento devem respeitar os direitos de propriedade intelectual, as políticas de privacidade e os direitos de autor.

3.4. Publicação de fotografias e trabalhos de alunos

- Na publicação de imagens e/ou gravações 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 sítio do Agrupamento, 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 serão 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.

3.6. Gestão dos sistemas de filtragem

- O acesso à Internet fornecido pelo Agrupamento inclui sistemas de filtragem adequados à idade e à maturidade dos alunos.
- 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, de acordo com o RI.
- 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

- O Agrupamento manterá um registo atualizado de todos os alunos e professores que são autorizados a aceder às comunicações eletrónicas da escola.
- Todos os elementos da comunidade terão conhecimento da Política de Segurança Digital e dos recursos para a utilização segura da Internet, disponíveis no sítio Web do Agrupamento e serão incentivados a analisá-los com os seus educados.

4.2. Resolução de incidentes relativos à Segurança Digital

- Todos os elementos da comunidade escolar deverão informar o Coordenador da Segurança Digital 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 serão 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, o Agrupamento contactará a Equipa de Proteção de Menores, através da Direção e / ou Coordenador da Segurança Digital, 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 / ou Coordenador da Segurança Digital 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.

- Todos os elementos da escola serão sensibilizados para a importância de manterem uma conduta adequada na Internet e de não publicarem comentários, conteúdos, imagens ou vídeos na Internet que possam causar dano, prejuízo ou sofrimento a outros elementos da comunidade escolar.
- As sanções para os envolvidos em cyberbullying podem incluir:
 - eliminação de todo o material considerado inapropriado pelo(a) autor(a) dos atos ou, caso se recuse ou não seja capaz de o fazer, eliminação realizada pelo fornecedor do serviço para que apague os conteúdos em questão;
 - os pais / encarregados de educação serão informados da sanção aplicada;
 - a Polícia será contactada, caso se suspeite de ação ilícita.

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 autorizado o uso de telemóveis e equipamentos pessoais em determinadas áreas dentro da escola, como vestiários, casa de banho ou outras devidamente comunicadas, de acordo com o Regulamento Interno.
- Os professores ou outros responsáveis podem confiscar um telemóvel ou outros equipamentos eletrónicos, conforme o estabelecido no RI se suspeitar que o equipamento pessoal contém materiais que podem constituir prova de uma ação ilícita.
- No caso de apreensão, cumprir-se-á o estipulado no Regulamento Interno.
- 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.
- Sempre que for necessário contactar alunos ou pais/encarregados de educação, deverão usar um telefone da escola.
- A captura de imagem e / ou vídeo deverá ser feita com equipamentos disponíveis no Agrupamento.
- Se um docente violar as políticas da escola, podem ser tomadas medidas disciplinares.

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 está disponível, para conhecimento e consulta, no sítio Web do Agrupamento.
- O Agrupamento ministrará, a todos os elementos da escola, formação atualizada e adequada sobre a utilização segura e responsável da Internet, tanto ao nível profissional como pessoal.
- No sítio Web do Agrupamento são disponibilizados recursos de apoio para uma utilização segura e responsável da Internet e de equipamentos informáticos.