

POLÍTICA DE SEGURANÇA DIGITAL



*Usar a Internet e os dispositivos
digitais em segurança*



ÍNDICE

ENQUADRAMENTO

I ENSINO E APRENDIZAGEM

- A. Utilização da Internet – sua importância
- B. Benefícios da utilização da Internet no ensino
- C. Educação para a segurança na Internet
- D. Avaliação de conteúdos digitais

II GESTÃO DE SISTEMAS DE INFORMAÇÃO

- A. **Manutenção** e segurança dos sistemas de informação
- B. Gestão de correio eletrónico
- C. Gestão dos conteúdos publicados
- D. Publicação de fotografias e trabalhos de alunos
- E. Gestão de comunidades sociais virtuais, redes sociais e publicações pessoais
- F. Gestão dos sistemas de filtragem
- G. Autorização no acesso à Internet
- H. Resolução de incidentes relativos à segurança digital
- I. Gestão de casos de cyberbullying
- J. Gestão de telemóveis e equipamentos pessoais

III NOTA FINAL

ENQUADRAMENTO

A Internet é hoje uma realidade presente no dia a dia de todos enquanto ferramenta que promove a comunicação, ultrapassa barreiras físicas, expande a nossa educação, colocando-nos em contacto com o mundo, abrindo janelas ao nosso conhecimento.

Sendo, indiscutivelmente, um meio essencial e do qual todos nós dependemos, direta ou indiretamente, expõe-nos também a enormes ameaças que é preciso ter presente aquando da sua utilização, tornando imperativo a criação de mecanismos e estratégias de minimização de eventuais abusos e ilegalidades possibilitados pela sua utilização.

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 com a utilização que todos fazem da Internet, dos telemóveis e de outras tecnologias de comunicação eletrónica em ambiente escolar e fora dele, exigindo o conhecimento por parte de todos os elementos da comunidade escolar dos os riscos e responsabilidades envolvidos. - Todos devem ser sensibilizados e dotados das competências necessárias para tomar decisões seguras e responsáveis. Assim sendo, uma política de segurança digital é essencial na definição de como o Agrupamento de Escolas de St^a Bárbara planeia desenvolver e estabelecer a sua abordagem à segurança digital e na identificação dos princípios nucleares que todos os elementos da comunidade escolar necessitam conhecer e compreender.

Este plano, alinhado com o Plano de Ação para a Transição Digital da Escola, assenta na capacitação e inclusão digital de toda a comunidade escolar e visa assegurar que toda a comunidade escolar segue determinadas regras básicas no que concerne à utilização da internet e das TIC em geral.

A. Utilização da Internet – sua importância

O acesso à Internet na escola está pensado com vista a alargar e reforçar a educação.

- Ensinar-se-á aos alunos a reconhecer uma utilização segura e responsável da Internet e ser-lhes-ão indicados objetivos claros aquando da sua utilização.
- A escola assegurará que a cópia e a utilização subsequente de materiais obtidos na Internet por alunos e professores cumprem a legislação em matéria de direitos de autor, incluindo o conhecimento dos vários tipos de licenciamentos disponíveis na web.
- A escola assegurará, igualmente, 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.
- A Rede Internet nas Escolas continuará a garantir que os níveis de acesso à Internet serão revistos de modo a corresponderem aos requisitos do currículo e à idade e competências dos alunos.
- A atribuição aos alunos de atividades com recurso à Internet, quer seja por parte dos docentes quer por entidades externas ao Agrupamento, respeitará os mesmos princípios.
- A escola assegurará que os alunos aprendem a utilizar eficazmente a Internet para fins de pesquisa, designadamente desenvolver competências de procura, obtenção e avaliação de informações.
- Os alunos devem aprender como indicar as fontes das informações utilizadas e a respeitar os direitos de autor quando utilizam material obtido na Internet nos seus trabalhos escolares.

B. 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 e países.
- Utilização social, recreativa e de lazer nas bibliotecas, nos clubes e em casa.
- Acesso de alunos e professores a peritos em inúmeras áreas.
- Desenvolvimento profissional dos professores através do acesso a informação, materiais pedagógicos e aplicações eficazes do currículo.
- Colaboração no âmbito de redes de escolas, serviços de apoio e associações profissionais.

- Maior acesso a apoio técnico, designadamente gestão remota de redes e atualizações automáticas de programas.
- Acesso às aprendizagens quando e onde for mais conveniente.

C. Educação para a segurança na Internet

A educação sobre o uso seguro e responsável da Internet deverá anteceder o acesso à mesma, não só em disciplinas especificamente relacionadas com as TIC, como noutras disciplinas ou atividades de enriquecimento curricular, de forma a aumentar a consciencialização sobre a importância da utilização segura e responsável da internet.

A utilização segura e responsável da Internet e da tecnologia em geral deverá, no entanto, ser reforçada em todo o currículo e em todas as áreas.

Todos os utilizadores deverão ser informados e estar conscientes de que o uso da Internet pode ser monitorizado e rastreado.

Todos os dispositivos da escola serão utilizados de acordo com a respetiva política de utilização e com a segurança apropriada.

D. Avaliação de conteúdos digitais

A avaliação de materiais da Internet faz parte do processo de ensino e de aprendizagem de qualquer disciplina e será considerada, no Agrupamento, um requisito transversal à escola e ao currículo.

Nesse sentido, os alunos ficarão a conhecer ferramentas de pesquisa da Internet adequadas à sua idade e serão ensinados a tomar posições críticas em relação aos materiais que leem e a saber como validar uma informação antes de aceitar a sua exatidão.

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. Manutenção e segurança dos Sistemas de Informação

A segurança dos sistemas informáticos do Agrupamento e dos utilizadores será revista anualmente.

1. A **equipa PTE** e/ou um técnico contratado assegurará a:

- Revisão anual da segurança dos sistemas de informação e dos utilizadores.
- Atualizações de segurança, regulares, dos equipamentos.
- Proteção antivírus.

2. Os **utilizadores** ficam obrigados a:

- Necessidade de autorização para a instalação de software para fins educativos por parte da equipa PTE ou serviços técnicos e levada a cabo por esses mesmos serviços.
- Remoção dos ficheiros do utilizador por parte do mesmo, após utilização do dispositivo, nomeadamente em atividades letivas.
- Autenticação obrigatória para aceder à rede da escola.

B. Gestão de correio eletrónico

A comunicação com alunos, pais / encarregados de educação e com instituições para tratamento de assuntos oficiais do Agrupamento deve ser obrigatoriamente realizada a partir de endereços eletrónicos institucionais. - A cada utilizador é atribuída uma palavra-passe pessoal e intransmissível, a qual deve ser atualizada periodicamente.

Apesar do correio eletrónico assumir um papel cada vez mais relevante na vida das organizações e das pessoas, o “direito a desligar” (ao descanso e ao lazer) é um direito fundamental que urge respeitar. Nesse sentido, toda a informação eletrónica, apenas, deve ser trocada no período compreendido entre as 08:00h e as 18:30h.

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.

C. Gestão dos conteúdos publicados

As informações de contacto na página Web do Agrupamento devem ter 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 designado pelo Diretor e deve assegurar que os conteúdos publicados são corre-

tos 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.

D. 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 da página do Agrupamento, em especial junto a fotografias.
- A publicação de qualquer imagem e/ou vídeo de alunos será feita, apenas, quando obtida autorização por escrito dos pais/encarregados de educação.
- Os trabalhos de alunos podem ser publicados, após obtida autorização por escrito dos pais/encarregados de educação.

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

Através de atividades dinamizadas pelos professores em sala de aula e pelas 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 verificarem os termos e condições dos mesmos, de modo a garantir que são adequados às idades dos alunos.

F. Gestão dos sistemas de filtragem

O acesso à Internet fornecido pela escola inclui **sistemas de filtragem** adequados à idade e à maturidade dos alunos.

- Qualquer material que a escola considere ser ilegal será denunciado através dos mecanismos oficiais.
- Os métodos para identificar, avaliar e minimizar os riscos online serão revistos regularmente pelo encarregado de proteção de dados

G. Autorização no acesso à Internet

O acesso à Internet é efetuado por tipologia de utilizador, ou por utilizador específico, por forma a garantir a segurança e a adequação dos conteúdos e recursos a partilhar.

- O Agrupamento manterá um registo atualizado de todos os alunos e professores que são

autorizados a aceder às comunicações eletrónicas do Agrupamento.

- Todos os elementos da comunidade educativa devem ter conhecimento da Política de Segurança Digital e dos recursos para a utilização segura da Internet.

H. Resolução de incidentes relativos à segurança digital

Todos os elementos da comunidade escolar deverão informar o encarregado da proteção de dados 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/denúncias adotadas pelo Agrupamento.
- A aplicação de medidas para superação de problemas relativos à segurança digital, incluindo os de índole disciplinar, serão articulados com os responsáveis pelos serviços onde ocorram os problemas.

I. Gestão de casos de cyberbullying

O cyberbullying, tal como todas as outras formas de bullying, não será tolerado e todos os incidentes detetados serão participados ao coordenador de proteção de dados e às autoridades competentes, quando necessário.

O *cyberbullying* corresponde ao uso da tecnologia para assediar, ameaçar ou vitimizar outra pessoa de forma repetida. Não requer força física, não implica um contacto cara-a-cara nem está limitado a algumas testemunhas.

- É importante ter consciência que a partir do momento que a criança ou o adolescente tem um telemóvel/computador/tablet está em risco.
- Todos devem estar alerta para os sinais que podem indiciar *cyberbullying* (por ex. fazer da sua vida digital um segredo ou tentar protegê-la a todo o custo; isolar-se e evitar a família, os amigos, as atividades habituais; diminuição do desempenho escolar; mostrar-se nervoso e ansioso sempre que surge uma nova mensagem; parar de usar o telemóvel/computador/tablet).

J. 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 alunos devem proteger os seus números de telefone, dando-os a conhecer apenas a amigos e familiares de confiança.
- Os utilizadores são responsáveis por qualquer tipo de dispositivos eletrónicos que tra-

gam 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.



NOTA FINAL

Todos os elementos da comunidade terão conhecimento da política de Segurança Digital e dos recursos para a utilização segura da Internet, disponíveis na página Web do Agrupamento (www.seguranet.pt).

Os membros da comunidade escolar devem estar cientes sobre comportamentos seguros e adequados online e a importância de não publicar qualquer conteúdo, comentários, imagens ou vídeos que causem danos, angústia ou ofensa a quaisquer outros membros da comunidade escolar.

Qualquer situação omissa deverá ser analisada à luz da legislação nacional e das orientações da Comissão Nacional de Proteção de Dados (<http://www.cnpd.pt>).

A elaboração deste documento teve por base:

- ♣ Lei n.º 67/98, de 26 de outubro, sobre a proteção de dados e que define no seu artigo 3.º (<https://www.cnpd.pt/bin/legis/nacional/LPD.pdf>);
- ♣ Lei n.º 103/2015, de 24 de agosto (<https://dre.pt/application/file/a/70084427>) que altera a Lei n.º 67/98;
- ♣ Lei n.º 51/2012, de 5 de setembro (<https://goo.gl/4zEtyk>) - Estatuto do Aluno e Ética Escolar;
- ♣ Regulamento (UE) N.º 2016/679, de 27 de abril de 2016 (<https://goo.gl/p28FKU>), relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados;
- ♣ Deliberação n.º 1495/2016, de 6 de setembro (<https://goo.gl/Nfsqyz>)

