AGRUPAMENTO DE ESCOLAS
HENRIQUES NOGUEIRA

Política de Segurança Digital

Usar a Internet e os dispositivos digitais como recurso educativo em segurança

Ficha Técnica:

Título: Política de Segurança Digital do Agrupamento de Escolas Henriques Nogueira

Autores: Ana Almeida, Cristina Martins, Conceição Gonçalves, Sandra Ferreira

Edição: fevereiro de 2022

Agrupamento de Escolas Henriques Nogueira (AEHN)
Rua Henriques Nogueira
2560-241 Torres Vedras

Aprovado em Conselho Pedagógico em 23/02/2022

Preâmbulo

Nos dias que correm, crianças, jovens e adultos interagem diariamente com tecnologias (os telemóveis, as consolas de jogos, *tablets*, Internet…) 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 que daí decorrem apresentam benefícios significativos para todos; todavia, podem, por vezes, colocar crianças, jovens e adultos em risco.

A segurança digital abrange questões relacionadas não só com crianças e jovens, mas também com adultos, utilizadores da Internet e de dispositivos que permitem a comunicação eletrónica dentro e fora do ambiente escolar. Por conseguinte, assume grande relevância a regulamentação de procedimentos a adotar em meio escolar e a formação e a autoformação de todos os elementos da comunidade escolar, alertando para os riscos que as tecnologias encerram e responsabilidades que importa assumir. Neste contexto professores e educadores têm um papel fundamental.

A escola está ciente de que é impossível evitar totalmente que crianças, alunos e outros elementos da comunidade educativa sejam expostos a riscos, tanto quando utilizam a Internet, como noutras situações. As crianças e os jovens devem ser sensibilizados e ensinados para que disponham das competências necessárias para tomar decisões seguras e responsáveis e para que sejam capazes de manifestar eventuais preocupações. Os professores e educadores devem conhecer boas práticas de segurança digital dentro e fora da sala de aula com vista a educar e proteger as crianças e os jovens. Os elementos da escola necessitam igualmente de saber como gerir a sua reputação profissional na Internet e de demonstrar uma conduta *online* adequada e consonante com as suas funções.

Todos os professores e educadores devem, pois, ter consciência da importância das boas práticas de segurança digital, visando a proteção e a formação das crianças e dos jovens sob o seu cuidado, para o correto e adequado uso das tecnologias.

Este documento é, pois, essencial na definição de como o Agrupamento planeia abordara segurança digital e identificar os princípios nucleares que todos os elementos da comunidade escolar necessitam de conhecer e compreender. É também fundamental na definição de princípios nucleares de ação, que todos os elementos da comunidade escolar devem aplicar.

A Coordenadora da Política de Segurança Digital _____

A Diretora _____

Política aprovada pelo Conselho Pedagógico em 23/02/2022

Índice

1. Política de Segurança Digital (eSafety)

O Agrupamento de Escolas Henriques Nogueira, adiante designado apenas por AEHN, acredita que a Segurança Digital (*eSafety*) é um elemento essencial de salvaguarda das crianças, jovens e adultos no mundo digital, ao usar tecnologias, como computadores, portáteis, *tablets*, telemóveis ou consolas de jogos. 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*. O AEHN 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. O AEHN reconhece que há uma clara necessidade de garantir que todos os alunos e funcionários estejam protegidos dos potenciais perigos *online*. A política de segurança digital é, por isso, essencial na definição de princípios nucleares de ação, que todos os elementos da comunidade escolar devem aplicar. Este documento é complementado por outro intitulado "Política de Privacidade e Proteção de Dados Pessoais". Nesse documento são abordadas com maior pormenor as questões relativas à disponibilização dos dados pessoais dos alunos.

Os objetivos da Política de Segurança Digital (PSD) são:

- identificar claramente os princípios fundamentais, seguros e responsáveis esperados de todos os membros da comunidade em relação à tecnologia como forma de garantir que o AEHN seja um ambiente seguro no que concerne à utilização de equipamentos eletrónicos e da Internet;
- sensibilizar todos os membros do Agrupamento para os potenciais riscos, bem como dar a conhecer os benefícios das tecnologias;
- permitir que todos os funcionários possam trabalhar com segurança e responsabilidade, com vista a um modelo comportamental positivo *online*, estando cientes da necessidade de gerir os seus próprios padrões e práticas ao usar as tecnologias;
- identificar procedimentos claros a adotar de forma a responder às preocupações de segurança *online* que sejam conhecidos por todos os membros da comunidade.

A PSD aplica-se a todos os funcionários, incluindo o órgão de gestão, professores, pessoal de apoio, prestadores de serviços, voluntários e outras pessoas que trabalham para o agrupamento ou prestam serviços em nome deste (coletivamente e adiante referidos como pessoal), bem como alunos e pais ou encarregados de educação.

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. Esta Política deve ser divulgada em conjunto com outras políticas escolares relevantes.

1.1. Redação e revisão da Política de Segurança Digital

- A definição, coordenação e implementação da PSD é da responsabilidade da Direção, a qual deve nomear um Coordenador de Segurança Digital.
- O AEHN reserva-se o direito de alterar, sem aviso prévio, a PSD, que será discutida e aprovada em Conselho Pedagógico.
- A PSD foi redigida pelo AEHN, tendo por base a Política do Selo de Segurança Digital e a legislação em vigor e orientações governamentais.

2. Ensino e aprendizagem

2.1. A importância da correta utilização da Internet

• Devendo ser parte integrante do currículo como uma ferramenta essencial no apoio à aprendizagem, a utilização da Internet no AEHN 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 proporcionado aos alunos, sempre que possível, e estes deverão utilizá-la de forma responsável.

• 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, considerando o currículo e a idade.

• A cópia, e a utilização subsequente de materiais obtidos na Internet, por crianças e jovens, professores e educadores e restante comunidade escolar, 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.

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

• 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 (direitos de

[1]A infraestrutura de rede do AEHN 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).

autor), pertinência e rigor, devem integrar a apresentação das referências bibliográficas e devem ser adequadas, pelos professores, às diferentes faixas etárias.

2.2. Benefícios da utilização da Internet no ensino

A utilização da internet possibilitará:

- acesso à informação;
- 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 AEHN deve ser pensado com vista a alargar e reforçar a educação.
- 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 ensinar-se os 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 AEHN e dos utilizadores será revista anualmente.
- 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 escola estão protegidos pelos sistemas de segurança dos programas utilizados, tendo em conta as recomendações da Comissão Nacional de Proteção de Dados na Deliberação n.º 1495/2016 relativas as restrições de acesso a esses sistemas e à robustez das palavras chave e identificadas no nosso documento "Política de Privacidade e Proteção de Dados Pessoais."
- Os dispositivos amovíveis serão utilizados de acordo com as autorizações específicas de cada serviço, estando os sistemas preparados para uma análise automática com antivírus.
- A instalação de *software* para fins educativos nos PC de secretária e portáteis deve ser autorizada pelo Coordenador da Segurança Digital e feita por um membro da equipa TIC/PTE.
- A capacidade e o funcionamento dos sistemas informáticos serão analisados, pelo menos uma vez por ano letivo.
- É obrigatória a utilização de nomes de utilizador e palavras-passe para aceder à rede da escola.
- Os utilizadores devem fazer a sua autenticação, nos computadores, com as suas credenciais e trabalhar na sua área de trabalho.
- A página inicial de navegação de cada PC ao serviço dos utilizadores será definida pela Direção, 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

- O AEHN disponibiliza contas de correio eletrónico a professores, educadores e formadores, pessoal não docente e alunos/formandos e a comunicação institucional é feita por esta via.
    - A comunicação com instituições, Pais/Encarregados de Educação para tratamento de assuntos oficiais do AEHN será obrigatoriamente 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 os alunos deve ser feita preferencialmente através de contas que não identifiquem diretamente os alunos, ou seja, através da sua conta de *email* institucional.
- A troca de mensagens com encarregados de educação é feita para as suas contas pessoais.
- 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 na página *Web* do agrupamento devem ser a morada, os números de telefone e o *email* do AEHN. 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.
- A Diretora é a responsável editorial geral pelos conteúdos digitais publicados pelo AEHN na Internet e deve assegurar que os conteúdos publicados são corretos e adequados.
- Todas as publicações em formato digital da responsabilidade de membros do AEHN devem respeitar os direitos de propriedade intelectual, as políticas de privacidade e os direitos de autor.

3.4. Publicação de fotografias, de gravações de voz e de trabalhos de alunos

- Antes da publicação de imagens ou de gravações áudio e/ou vídeo 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 mesmos.

- 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 só serão publicados *online* com a autorização dos mesmos e dos pais/encarregados de educação das crianças e devem ter em conta os direitos de autor.

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

- Através de atividades dinamizadas pelos professores em sala de aula, nomeadamente nas aulas de TIC, 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, formadores e educadores 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. Os blogues ou *Wikis* oficiais geridos pelos professores devem estar protegidos por palavra-passe.
- Através da página *Web* do AEHN, são disponibilizados aos pais/encarregados de educação materiais relacionados com a utilização de redes sociais, meios sociais e sítios de publicação pessoal (dentro ou fora da escola), especialmente para os alunos mais novos. Ações de sensibilização para o uso seguro da Internet podem vir a ser organizadas em colaboração com a Biblioteca Escolar (BE) e/ou com Associação de Pais e Encarregados de Educação do AEHN.

3.6. Gestão dos sistemas de filtragem

- O acesso à Internet fornecido pelo AEHN inclui sistemas de filtragem de conteúdos impróprios, implementados centralmente pela Direção-Geral de Estatística da Educação e Ciência que fornece o acesso à Internet e garante a manutenção regular destes sistemas de filtragem.
- Os professores que encontrarem sítios bloqueados com interesse pedagógico ou sítios impróprios que estão desbloqueados devem fazer chegar essa informação à Direção de modo a poder fazer-se o pedido de atualização à Direção-Geral de Estatísticas da Educação e Ciência.

4. Decisões quanto às políticas

4.1. Autorização do acesso à Internet

- Pessoal docente, não docente e alunos / formandos 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 da Política de Privacidade e Proteção de Dados Pessoais, disponíveis no sítio *Web* do AEHN e serão incentivados a analisá-los com os seus educandos.

4.2. Resolução de incidentes relativos à Segurança Digital

- Todos os elementos do AEHN deverão informar o Coordenador da segurança digital se tiverem 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.
- O Coordenador da segurança digital registará todos os incidentes, bem como todas as medidas aplicadas, e 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.
- Alterações no acesso e nos serviços, decorrentes da aplicação de medidas no âmbito da segurança digital, devem ser comunicadas a alunos, docentes e pessoal não docente, ainda que com a devida proteção de confidencialidade das pessoas envolvidas.

- Sempre que houver razões para crer ou recear que ocorreu ou está a ocorrer alguma atividade ilegal, o AEHN contactará a Equipa de Proteção de Menores e/ou encaminhará a situação para as autoridades competentes.

4.3. 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 do AEHN, 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.
- As sanções, para os envolvidos em *cyberbullying*, poderão incluir:
  - O(a) autor(a) dos atos deverá eliminar todo o material considerado inapropriado. Caso este se recuse ou não seja capaz de o fazer, a eliminação dos referidos conteúdos deverá ser solicitada ao fornecedor do serviço.
  - O(A) autor(a) poderá ver o seu direito de acesso à Internet na escola suspenso durante um período de tempo a determinar pela Direção;
  - Os pais/encarregados de educação serão informados da sanção aplicada;
  - As autoridades competentes serão contactadas, 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.
- 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 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. 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 para os telemóveis durante o horário letivo. Em caso de necessidade de contacto urgente devem usar o número de telefone da Escola.
- Sempre que for necessário contactar alunos ou pais/encarregados de educação, dever-se-á usar, preferencialmente, o telefone da escola.
- Os telemóveis e outros equipamentos estarão desligados ou em modo de "silêncio" e os telemóveis e outros equipamentos não serão utilizados em períodos letivos, exceto em situações de emergência, ou em atividades pedagógicas.

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 AEHN.
- O AEHN 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 AEHN são disponibilizados recursos de apoio para uma utilização segura e responsável da Internet e de equipamentos informáticos.
- O AEHN dará a conhecer aos pais a sua Política de Segurança Digital, através dos canais que entender adequados, nomeadamente no ato de matrícula.