AGRUPAMENTO DE ESCOLAS
ANADIA

Política de segurança digital

Documentos Orientadores

Equipa PTE e Direção

A segurança nos ambientes digitais apresenta-se como um desafio complexo. Na sociedade da informação, proteger e cuidar dos nossos dados é uma tarefa complexa. Quando lembramos que a Internet das Coisas[1] já é uma realidade, conectando não apenas pessoas, mas biliões de objetos como redes, o desafio de conectar-se com segurança exige cada vez mais atenção.

Dados pessoais "perdidos" nas redes sociais, nas pesquisas, nos milhões de emails e mensagens, sites de compras, nos programas de fidelidade, nos cartões de crédito e nos dispositivos móveis que concentram cada vez mais informações detalhadas sobre as nossas vidas. Toda a pessoa tem direito à liberdade e segurança[2].

Considerando o direito à segurança da informação como um dos direitos humanos que defendemos também na rede, a *eSafety Label*[3] oferece algumas dicas para preservar os direitos de proteção contra abusos e violações de privacidade ou das liberdades de expressão, e posicionamento sexual, religioso, político e de pensamento.

[1] https://www.cncs.gov.pt/ ı" Mas o que é isso da Internet das Coisas ou Internet de Tudo? A Internet das Coisas, também conhecida pelo acrónimo IoT, compreende todos os aparelhos e objetos que se encontram habilitados a estarem permanentemente ligados à Internet, sendo capazes de se identificar na rede e de comunicar entre si. Podem ter o seu estado alterado através daquele meio, com ou sem o envolvimento ativo do ser humanos e têm capacidade para recolher uma vasta quantidade de informação sobre os que o rodeia. A Internet Society define o IoT em sentido amplo como "a extensão da conectividade de rede e capacidade de computação para objetos, dispositivos, sensores e outros artefactos que normalmente não são considerados computadores". "

[2] Artigo 6º da Carta dos Direitos Fundamentais da UE

[3] Trata-se de um serviço europeu de certificação e de apoio às Escolas, que visa promover um ambiente seguro e enriquecedor e o acesso seguro às tecnologias digitais, como parte da experiência de ensino e aprendizagem.

Ficha Técnica: Título: Política de Segurança Digital do Agrupamento de Escolas de Anadia

Autores: Aníbal Marques, Catarina Simões, Luís Bandarra e João Lopes

Edição: Agrupamento de Escolas de Anadia, fevereiro de 2020 | Aprovado em Conselho Pedagógico do AEA em 19.02.2020, como parte integrante do Regulamento Interno.

O Coordenador da Política de Segurança Digital é o Responsável do equipamento informático e 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 sempre que assim se justifique.

O Coordenador da Política de Segurança Digital _____

O Diretor _____

Política aprovada pelo Conselho Pedagógico em 19 de fevereiro de 2020.

Vivemos na era da informação, numa época em que há uma enorme revolução digital, e em que os computadores já se encontram firmemente estabelecidos nas mais diversas áreas da vida moderna. As tecnologias da informação estão cada vez mais presentes, quer na vida dos adultos, quer na das crianças.

As crianças e jovens de hoje crescem com tecnologias, utilizando-as diariamente, acedendo numa idade cada vez mais jovem.

Progressivamente, a Internet é cada vez mais acessível para as crianças e jovens, na Escola, em bibliotecas, em casa e, na verdade, em qualquer lado. Com o crescimento e desenvolvimento das novas tecnologias, as crianças e jovens têm acesso cada vez mais fácil e mais rápido a qualquer informação e conteúdos online. Em grande medida, pelo facto de cada vez mais cedo terem também telemóveis com acesso online, o que facilita ainda mais a navegação nos mundos virtuais.

A Escola está ciente de que é impossível evitar totalmente que alunos e outros elementos da Escola sejam expostos a riscos, tanto quando utilizam a Internet, como noutras situações. As crianças e jovens devem ser sensibilizadas e ensinadas para que disponham das competências necessárias para tomar decisões seguras e responsáveis e para que sejam capazes de manifestar eventuais preocupações. Todos os professores devem ter consciência da importância de boas práticas de segurança digital na sala de aula com vista a educar e proteger as crianças sob o seu cuidado. Os elementos da Escola necessitam igualmente de saber como gerir a sua reputação profissional na Internet e de demonstrar uma conduta na Internet adequada e consonante com as suas funções.

A política de segurança digital é essencial na definição de como a Escola planeia desenvolver e estabelecer a sua abordagem à segurança digital e na identificação dos princípios nucleares que todos os elementos da comunidade Escolar necessitam de conhecer e compreender.

1. Principais responsabilidades

1.1. Competências do Órgão de Gestão e da Equipa de Segurança Digital.

a) Desenvolver e promover uma visão e cultura de segurança online para toda a comunidade Escolar.
b) Garantir que a segurança online é vista proactivamente por toda a comunidade como uma questão de salvaguarda.
c) Apoiar o Coordenador de Segurança Digital, garantindo que tenha tempo e recursos suficientes para cumprir o seu papel de segurança online e demais responsabilidades.
d) Assegurar que todos os membros da equipa recebem formação regular e adequada quanto à segurança e responsabilidades online e orientações relativas a comunicações seguras e adequadas.
e) Tomar conhecimento e decidir acerca de quaisquer incidentes de segurança online.
f) Assegurar que são realizadas avaliações de risco adequadas sobre a utilização segura da tecnologia, incluindo a garantia de uma utilização responsável dos dispositivos.

1.2. Competências do Coordenador de Segurança Digital

a) Agir como um ponto de contacto e ligação com outros membros do pessoal e outras entidades, conforme apropriado, em relação a todas as questões de segurança online.
b) Manter-se atualizado com a pesquisa atual, legislação e tendências em matéria de segurança online.
c) Coordenar a participação em eventos locais ou nacionais para promover o comportamento online positivo, por exemplo, o Dia da Internet Segura.
d) Garantir que a segurança online é promovida para os pais e encarregados de educação e a comunidade em geral, através de uma variedade de canais e de abordagens.
e) Trabalhar com a Escola para a proteção e segurança de dados, de forma a garantir que a prática está de acordo com a legislação vigente.
f) Monitorizar as definições de segurança online para identificar as lacunas e usar esses dados para atualizar a resposta da Escola a essas necessidades.
g) Informar a equipa de gestão da Escola e outras entidades, conforme apropriado, em questões de segurança online.
h) Facilitar a ligação com organismos locais e nacionais, conforme apropriado.

i) Trabalhar com a Equipa de Liderança na revisão e atualização da Política de Segurança Digital, Políticas de Utilização Aceitável (PUAs), Política de Privacidade e outras políticas relacionadas, numa base regular.
j) Garantir que a segurança online é integrada noutras políticas e procedimentos da Escola de forma apropriada.

1.3. Pessoal Docente, Pessoal Não Docente, Alunos, Prestadores de Serviços ou de Apoio.

As principais responsabilidades para todos são:

a) Contribuir para o desenvolvimento da Política de Segurança Digital.
b) Ler as Políticas de Utilização Aceitável (PUAs), aceitando-as, cumprindo-as e fazendo-as cumprir.
c) Assumir a sua responsabilidade individual pela segurança dos sistemas eletrónicos da Escola.
d) Ter consciência de uma variedade de diferentes questões relacionadas com a segurança online e como elas podem afetar os alunos sob os seus cuidados.
e) Apresentar boas práticas na utilização das novas tecnologias.
f) Incorporar a educação para a segurança online no currículo, sempre que possível.
g) Identificar situações individuais de preocupação e tomar medidas apropriadas, seguindo as políticas e procedimentos de salvaguarda da Escola.
h) Ser capaz de sinalizar para o apoio adequado disponível as questões de segurança online, interna e externamente.
i) Saber quando e como escalar questões de segurança online, interna e externamente.
j) Manter um nível de conduta profissional no seu uso pessoal da tecnologia, dentro e fora do local de trabalho.

As principais responsabilidades dos alunos são:

a) Contribuir positivamente para o desenvolvimento das políticas de segurança online.
b) Ler ou pedir que lhes sejam lidas as Políticas de Utilização Aceitável (PUAs) e respeitá-las.
c) Respeitar os sentimentos e os direitos dos outros, tanto online como offline.
d) Procurar a ajuda de um adulto de confiança, se as coisas correrem mal, e apoiar outros que podem estar enfrentando problemas de segurança online.
e) Avaliar os riscos pessoais do uso de qualquer tecnologia específica, e comportar-se de forma segura e responsável, para limitar esses riscos.

As principais responsabilidades dos pais e encarregados de educação são:

a) Ler as Políticas de Utilização Aceitável (PUAs) da Escola, incentivando os seus filhos ou educandos à sua adesão, e aderindo eles próprios, se for o caso.
b) Discutir questões de segurança online com os seus filhos, apoiando a Escola nas suas abordagens sobre o tema, reforçando comportamentos online seguros e adequados em casa.
c) Ser um modelo apropriado na utilização racional da tecnologia e na adoção de comportamentos seguros online.
d) Identificar mudanças no comportamento que possam indicar que o seu filho ou educando está em risco de dano online.
e) Procurar ajuda e apoio da Escola, ou de outros órgãos competentes, se os seus filhos ou educandos encontrarem problemas ou preocupações online.
f) Assumir a responsabilidade pela sua própria consciência e aprendizagem em relação às oportunidades e riscos decorrentes das tecnologias novas e emergentes.

2. Ensino e Aprendizagem.

2.1. Importância da Internet.

a) A utilização da Internet fará parte integrante do currículo formal sempre que possível e é uma ferramenta essencial na aprendizagem.
b) Os alunos utilizam a Internet amplamente fora da Escola e devem saber como avaliar a informação que obtêm na Internet e como se podem proteger.
c) A finalidade da utilização da Internet na Escola é elevar os padrões educativos, promover o sucesso dos alunos, apoiar o trabalho dos professores e reforçar a administração Escolar.

2.2. Benefícios da utilização da Internet no ensino.

Os benefícios da utilização da Internet no ensino incluem:

a) Acesso a recursos pedagógicos e educativos de todo o mundo, incluindo museus e galerias de arte.
b) Intercâmbio cultural e educativo entre alunos de várias Escolas e realidades.
c) Utilização social, recreativa e de lazer nas bibliotecas, nos clubes e em casa.
d) Acesso de alunos e professores a peritos em inúmeras áreas.
e) Desenvolvimento profissional dos professores através do acesso a informação, materiais pedagógicos e aplicações eficazes do currículo.
f) Colaboração no âmbito de redes de Escolas, serviços de apoio e associações profissionais.
g) Maior acesso a apoio técnico, designadamente gestão remota de redes e atualizações automáticas de programas.
h) Possibilidade de aprendizagem quando e onde for mais conveniente.

2.3. Formas da Internet melhorar a aprendizagem

a) O acesso à Internet na Escola será pensado com vista a alargar e reforçar a educação.
b) Ensinar-se-á 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.
c) 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.
d) A Escola 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.
e) Os níveis de acesso à Internet serão revistos de modo a corresponderem aos requisitos do currículo e à idade e capacidades dos alunos.
f) Os professores atribuirão aos alunos atividades com recurso à Internet que estejam de acordo com os objetivos de aprendizagem e com a sua idade e capacidades.
g) 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.

2.4. Avaliação de conteúdos digitais

a) 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.
b) Deve-se mostrar-lhes ferramentas de pesquisa da Internet que sejam adequadas à sua idade.
c) 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 e uma responsabilidade do professor.

2.5. Educação para a Segurança na Internet

a) O AEAnadia disponibiliza um currículo de segurança online (eSafety), através da atividade de enriquecimento curricular de TIC, de forma a aumentar a consciencialização sobre a importância da utilização segura e responsável da Internet entre os alunos.
b) A utilização segura e responsável da Internet e da tecnologia em geral deverá, no entanto, ser reforçado em todo o currículo e em todas as áreas.
c) A educação sobre o uso seguro e responsável deverá anteceder o acesso à Internet.
d) Os alunos serão apoiados na leitura e compreensão da Política de Utilização Aceitável para que esta se adapte à sua idade e capacidades.

e) Todos os utilizadores deverão ser informados e estar conscientes que o uso da Internet será monitorizado.
f) A Escola deve estar consciente de que algumas crianças podem ser consideradas mais vulneráveis online, devido a uma variedade de fatores.
g) O pessoal deverá ser informado de que o tráfego de Internet pode ser monitorizado e rastreado. A descrição e conduta profissional são essenciais ao utilizar os sistemas e dispositivos da Escola.
h) Todos os membros do pessoal devem estar cientes de que o seu comportamento online fora da Escola pode ter um impacto sobre o seu papel e reputação dentro da Escola. Ações civis, judiciais ou disciplinares podem ser tomadas se forem encontrados motivos de descrédito ou ofensa à profissão ou à instituição.
i) Os membros do pessoal com a responsabilidade de gerir sistemas de filtragem ou monitorizar o uso das TIC serão supervisionados pela Equipa de Segurança digital e terão procedimentos claros para relatar problemas ou preocupações.

3. Comunicação Online e Utilização Segura da Tecnologia.

3.1. Utilização segura e adequada em contexto de sala de aula da Internet ou quaisquer dispositivos associados.

a) A utilização da Internet é uma característica fundamental de acesso à educação e todas as crianças receberão orientação adequada à sua idade e capacidades de forma a apoiar e permitir desenvolver estratégias de aquisição de um currículo Escolar integral e inclusivo.
b) Todos os professores devem estar cientes de que não podem contar totalmente com os sistemas de filtragem para proteger as crianças e jovens, pelo que a supervisão, gestão de sala de aula e educação sobre uso seguro e responsável, é essencial e da sua responsabilidade.
c) As atividades online dos alunos serão supervisionadas. Os alunos deverão utilizar ferramentas online/offline e atividades online/offline adequadas à sua idade e deverão ter sempre a supervisão do professor.
d) Todos os dispositivos da Escola serão utilizados de acordo com a respetiva Política de Utilização Aceitável e com a segurança apropriada.
e) Os professores deverão sempre analisar e avaliar os sites, ferramentas e aplicativos antes do uso em sala de aula ou da sua recomendação para uso em casa.
f) A Escola irá garantir que a utilização de materiais derivados da Internet pelo pessoal e alunos está em conformidade com a lei de direitos de autor e reconhecimento da fonte de informação.
g) A avaliação dos materiais disponíveis online é uma parte do processo de ensino e aprendizagem em todas as disciplinas e será visto como um requisito em todo o currículo.
h) A Escola tomará todas as medidas necessárias para que a utilização da Internet seja realizada num ambiente seguro.

3.2. Gestão de telemóveis e equipamentos pessoais

a) Em sessões de sensibilização e atividades dirigidas a alunos do 1.º aos 12.º anos, dinamizadas, quando possível, em articulação entre o Serviço das Bibliotecas do Agrupamento e 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.
b) 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.
c) A função de Bluetooth dos telemóveis deve estar sempre desligada e não pode ser utilizada para enviar imagens ou ficheiros para outros telemóveis ou para interferir com o funcionamento de outros dispositivos.
d) 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.
e) Não é autorizado o uso de telemóveis e equipamentos pessoais em determinadas áreas dentro da Escola, como vestiários, casas de banho...
f) Os professores podem confiscar um telemóvel ou equipamento, conforme o estabelecido no RI do AEA. O Coordenador de Segurança Digital pode fazer uma pesquisa ao telemóvel ou equipamento, com o consentimento do aluno ou dos pais / encarregados de educação. Caso se suspeite que o equipamento pessoal contém materiais que podem constituir prova de uma ação ilícita, o telemóvel será entregue à Polícia para averiguações.
g) No caso de apreensão, os telemóveis e outros equipamentos pessoais serão entregues aos pais / encarregados de educação, de acordo com o estipulado no RI.
h) 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.
i) Se um aluno 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.
j) 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.
k) A utilização de telemóveis e outros equipamentos pessoais por parte de alunos na sala de aula é proibido.
l) A utilização de telemóveis e outros equipamentos pessoais por parte de professores apenas é permitido em contexto de sala de aula, baseada numa

utilização pedagógica fundamentada. Excetua-se a sua utilização no(s) período(s) de descanso devidamente autorizado(s) e nos locais reservados.

m) O envio de mensagens ou conteúdos abusivos ou inadequados através de telemóveis ou equipamentos pessoais por parte de qualquer elemento da Escola é proibido e quaisquer violações deste princípio serão tratadas em conformidade com a política de disciplina e de conduta da Escola.
n) Os professores podem confiscar um telemóvel ou equipamento se se considerar que está a ser utilizado de modo contrário às políticas da Escola em matéria de conduta ou bullying.
o) Os professores e restante pessoal são responsáveis pelos dispositivos eletrónicos de todos os tipos 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.

3.3 Publicação de fotografias, de gravações de voz e de trabalhos de alunos

a) A Escola garantirá que todas as imagens e vídeos compartilhados online serão utilizados de acordo com a Política de Utilização de Imagem da Escola.
b) Antes da publicação de imagens ou de gravações vídeo que incluam alunos, deve ser garantida a autorização expressa e informada, de acordo com a legislação aplicável.
c) A captação de imagens dos alunos deve, preferencialmente, ser executada de longe ou de ângulos que reduzam significativamente a possibilidade de identificação.
d) 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.
e) 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.
f) Em linha com a política de imagem, a autorização por escrito dos pais ou encarregados de educação será sempre obtida antes das imagens/vídeos de alunos serem publicados online.
g) Os trabalhos de alunos só serão publicados com a autorização dos mesmos ou dos pais/encarregados de educação das crianças.
h) No início de cada ano letivo, será obtida autorização por escrito dos pais ou encarregados de educação.

3.4. Gestão do correio eletrónico

a) A gestão da conta de correio eletrónico institucional da Escola é da responsabilidade do Órgão de Gestão.
b) Todos os membros do pessoal docente devem possuir um endereço de correio eletrónico a ser usado para qualquer comunicação oficial.

c) O encaminhamento de qualquer cadeia de mensagens/emails, etc., não é permitido. Spam ou lixo eletrónico será bloqueado e relatado para o provedor de email.
d) Qualquer comunicação eletrónica que contenha conteúdo que possa violar a legislação de proteção de dados (por exemplo, informações confidenciais ou pessoais) só será enviado como email seguro e criptografado.
e) Os membros da comunidade Escolar devem avisar imediatamente a Equipa de Segurança Digital se receberem comunicação ofensiva e esta será gravada de forma a agir apropriadamente.
f) As mensagens de correio eletrónico enviadas a organizações externas devem ser escritas com cuidado antes de enviar, da mesma forma que uma comunicação oficial escrita em papel timbrado da Escola o seria.
g) 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.
h) Os alunos têm de informar imediatamente o professor designado para o efeito caso recebam mensagens de email ofensivas.
i) 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.
j) O acesso a contas de email pessoais dentro da Escola pode ser bloqueado.

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

a) 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
b) 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.
c) Os blogues ou wikis oficiais geridos pelos professores devem estar protegidos por palavra-passe.
d) Através da página Web do Agrupamento, são disponibilizados aos pais / encarregados de educação materiais relacionadas 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 as Associações de Pais e Encarregados de Educação do Agrupamento.

3.6. Websites

a) Os detalhes de contacto no(s) site(s) Escolares apenas poderão ser o endereço físico da Escola, hiperligações autorizadas e endereço de correio eletrónico oficial. Nenhuma informação pessoal dos alunos deverá será publicada.
b) O Órgão de Gestão assumirá a responsabilidade editorial global pelo conteúdo online publicado e garantirá que as informações são precisas e adequadas.
c) O(s) site(s) cumprirão com as orientações da Escola para publicações incluindo a acessibilidade, o respeito para com os direitos de propriedade intelectual, políticas de privacidade e de direitos de autor.
d) Os endereços de email online deverão ser publicados com cuidado, para evitarem serem recolhidos por spam (por exemplo, substituindo '@' com 'AT').
e) Os trabalhos, imagens ou vídeos dos alunos serão publicados com a permissão dos pais ou encarregados de educação.
f) A conta de administrador para o sítio oficial da Escola será salvaguardada com uma senha apropriadamente forte.
g) A Escola irá publicar informações sobre a salvaguarda, incluindo a segurança online, no sítio oficial da Escola, para os membros da comunidade, incluindo este PSD.

3.7 Gestão dos sistemas de filtragem

a) O acesso à Internet fornecido pelo Agrupamento incluirá sistemas de filtragem adequados à idade e à maturidade dos alunos.
b) 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.
c) Serão feitas verificações regulares, para comprovar a eficácia dos métodos de filtragem adotados.

3.8 Gestão dos casos de cyberbullying

a) 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.
b) Os alunos do 5.º ano terão sessões, dinamizadas pelo grupo 550, se necessário, em que serão sensibilizados para as questões do cyberbullying.
c) Todos os incidentes de cyberbullying comunicados serão registados e serão investigados, aplicando-se, quando necessário, os procedimentos de inquirição usados nos processos disciplinares, tal como estabelecido no RI.
d) As sanções para os envolvidos em cyberbullying podem incluir: a eliminação de todo o material considerado inapropriado pelo autor 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; o autor poderá ver o seu direito de

acesso à Internet na Escola suspenso durante um período de tempo a determinar pela Direção, em articulação com o Coordenador da Segurança Digital; o os pais / encarregados de educação serão informados da sanção aplicada; a Polícia será contactada, caso se suspeite de ação ilícita.

3.9 Utilização de equipamentos pessoais pelos alunos.

a) Se um aluno violar as políticas da Escola, o seu telemóvel ou equipamento será apreendido e guardado em local seguro na Escola. Os telemóveis e outros equipamentos pessoais serão entregues aos pais ou encarregados de educação, em conformidade com as políticas da Escola.
b) Se um aluno necessitar de contactar os pais, deverá informar um professor ou funcionário que realizará o contacto utilizando os meios oficiais da Escola.
c) Os alunos devem proteger os seus números de telefone, dando-os a conhecer apenas a amigos e familiares de confiança. 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.

4.0 Utilização de equipamentos pessoais pelos professores

a) Os professores não estão autorizados a utilizar os seus telemóveis ou equipamentos pessoais para contactar crianças, jovens ou seus familiares dentro ou fora da Escola na sua qualidade de profissionais.
b) Sempre que for necessário contactar alunos ou pais/encarregados de educação, deverão usar um telefone da Escola.
c) Durante o período letivo, os telemóveis e outros equipamentos deverão estar desligados ou em modo de "silêncio". Os referidos equipamentos não serão utilizados em períodos letivos exceto em situações de emergência autorizadas pelo Órgão de Gestão.
d) Se, por motivos pedagógicos, os professores pretenderem que os alunos utilizem telemóveis ou outros equipamentos pessoais numa atividade educativa, isso será feito com a aprovação da Equipa de Segurança Digital e de acordo com esta Política de Segurança Digital.

5. Os Media Sociais

5.1. Disposições gerais

a) A utilização segura e responsável dos meios de comunicação social, nomeadamente as redes sociais, será preocupação de todos os membros do AEA como forma de proteger tanto a Escola como a comunidade em geral, online e offline. Exemplos de media sociais podem incluir blogues, wikis, sites de redes sociais, fóruns, painéis de mensagens, jogos multiplayer online, aplicativos de vídeo/sites de partilha de fotos, chats, mensagens instantâneas e outros.

b) Todo o pessoal do AEA será incentivado a envolver-se em media sociais de uma maneira positiva, segura e responsável, em todos os momentos.
c) Todo o pessoal do AEA, incluindo alunos, é aconselhado a não publicar detalhes específicos e privados, pensamentos, preocupações, imagens ou mensagens em quaisquer serviços de media social, especialmente conteúdo que possa ser considerado ameaçador, prejudicial ou difamatório aos outros ou para com a instituição.
d) O AEA reserva-se o direito de controlar e/ou vedar o acesso de alunos e restante pessoal aos diversos media sociais e sites de redes sociais, enquanto tal for realizado no local e se resultar do uso de dispositivos ou sistemas Escolares.
e) O uso de aplicações de redes sociais durante o horário Escolar para uso pessoal não é permitido (excetua(m)-se o(s) período(s) de descanso devidamente autorizado(s) e nos locais apropriados).
f) O uso inadequado ou excessivo das redes sociais durante o horário de trabalho ou através do uso de dispositivos Escolares pode resultar em ação disciplinar ou legal e/ou remoção de recursos da Internet.
a) Quaisquer preocupações relativas à conduta online de qualquer membro do AEA em sites de media sociais devem ser comunicadas ao Órgão de Gestão ou ao Coordenador de Segurança Digital e serão geridas em conformidade com as políticas da Escola.
b) Quaisquer violações das políticas explícitas da Escola podem resultar em ações criminais, disciplinares ou civis, tendo em consideração a idade e a função dos envolvidos e as circunstâncias do erro cometido.

5.2. Uso oficial das redes sociais

a) O uso oficial das redes sociais pela Escola só acontecerá com objetivos do trabalho educacional, divulgação ou comunicação destinada, por exemplo, a aumentar o envolvimento dos pais e encarregados de educação.
b) A utilização oficial das redes sociais como ferramentas de comunicação será avaliada e fundamentada formalmente pelo Órgão de Gestão ouvido o Coordenador de Segurança Digital.
c) Os canais oficiais da Escola nas redes sociais deverão ser configurados de forma segura, sóbria e institucional, destinando-se exclusivamente a fins educativos e a uma utilização responsável, de acordo com a legislação local e nacional.
d) Toda a comunicação nas plataformas oficiais deve ser clara, transparente e aberta ao escrutínio.
e) Qualquer publicação online em sites oficiais ou de media social deverá cumprir os requisitos legais, incluindo a Lei de Proteção de Dados, o direito à privacidade ou a obrigação em proteger informação privada e não deverá violar qualquer dever de direito comum de confidencialidade, direitos de autor, cyberbullying, etc.
f) Imagens, vídeos ou trabalhos de alunos só serão compartilhadas em sites de media social, canais oficiais ou redes sociais de acordo com a Política de Uso de Imagem.

g) Pais e encarregados de educação, alunos, professores e restante pessoal, serão informados da existência dos diversos canais oficiais e da respetiva Política de Utilização de Imagem.
h) O(s) responsável(eis) que gerem os canais oficiais da Escola, nomeadamente as redes sociais, não devem divulgar informações, fazer compromissos ou participar em atividades em nome da Escola, a menos que estejam devidamente autorizados a fazê-lo.
i) É proibida a comunicação direta com pais, encarregados de educação ou alunos através de qualquer canal de media social ou rede social.
j) Os membros do pessoal serão incentivados a gerenciar e controlar de forma responsável o conteúdo que partilharem e publicarem online.
k) Os professores que pretendam utilizar ferramentas das redes sociais com os alunos em atividades curriculares avaliarão o risco dos sítios na Internet antes de os utilizar e verificarão os termos e condições dos mesmos de modo a garantir que são adequados às idades dos alunos. Adicionalmente, os professores poderão obter aconselhamento do Coordenador de Segurança Digital ou do Órgão de Gestão antes de utilizarem redes sociais na sala de aula.
l) As opiniões pessoais do pessoal não refletem nem vinculam a posição oficial da Escola como instituição.

5.3. Uso pessoal das redes sociais

a) A publicação pessoal em sites de media social será ensinada aos alunos como parte de uma abordagem incorporada e progressiva através de sites apropriados à sua idade, que foram alvo de uma avaliação de risco e aprovados como adequados para fins educativos.
b) Os alunos serão aconselhados a considerar os riscos de partilhar detalhes pessoais de qualquer tipo em sites de media social que possam identificá-los ou a sua localização. Exemplos incluem o nome real/completo, endereço, números de telefone móvel ou fixo, Escola frequentada, detalhes de contacto, endereços de correio eletrónico, nomes completos dos amigos/família, interesses específicos, etc.
c) Os alunos serão aconselhados a não promover encontros online sem um pai e/ou responsável ou a permissão de outro adulto responsável e só quando eles podem estar presentes.
d) Os alunos serão informados sobre a segurança adequada em sites de media social e serão incentivados a utilizar em segurança senhas, negar o acesso a indivíduos desconhecidos e em aprender a bloquear e relatar comunicações não desejadas.
e) Qualquer atividade de media social oficial envolvendo alunos no recinto Escolar deverá ser sempre moderada pela Escola.
f) Sempre que solicitado, serão abordadas com os pais ou encarregados de educação questões e preocupações relacionadas com a utilização de redes sociais, meios sociais e sítios de publicação pessoal (dentro ou fora da Escola), especialmente quando se trata de alunos mais novos.

6. Gestão de sistemas de informação

a) Os utilizadores devem agir com razoabilidade – por exemplo, descarregar ficheiros de grande dimensão durante o horário de trabalho afeta a qualidade/velocidade da ligação à Internet das restantes pessoas.
b) Os utilizadores devem assumir responsabilidade pela sua utilização da Internet.
c) Os computadores de trabalho devem estar protegidos contra determinadas ações inadvertidas ou deliberadas dos utilizadores.
d) Os computadores de trabalho deverão ter mais do que um navegador de Internet, incluindo nestes, extensões que permitam bloquear publicidade e navegar de forma privada, incluindo o uso de motores de pesquisa com a inclusão de navegação em privado.
e) Toda a rede interna deve ter instalada e atualizada uma proteção antivírus e firewall.
f) O acesso por dispositivos sem fios deve ser administrado proactivamente e estar sujeito a um nível de segurança mínimo com encriptação WPA2.
g) A segurança dos sistemas informáticos da Escola e dos utilizadores será revista com regularidade.
h) A proteção antivírus será atualizada com regularidade.
i) As regras da firewall devem ser conhecidas e atualizadas de acordo com as ameaças de cybersegurança.
j) Os dispositivos amovíveis apenas poderão ser utilizados pelos professores e mediante uma autorização específica do Coordenador de Segurança Digital, seguida de uma análise antivírus/malware.
k) Nenhum Software não aprovado será autorizado nas áreas de trabalho ou como anexo de mensagens eletrónicas.
l) Os ficheiros guardados na rede da Escola ou nos postos de trabalho serão verificados com regularidade.
m) Sempre que possível, serão integradas extensões de programas nos navegadores de Internet.
n) É aconselhada a configuração de um motor de pesquisa por defeito nos navegadores de Internet, com navegação privada.

6.1. Sistemas de filtragem

a) O acesso à Internet fornecido pela Escola incluirá sistemas de filtragem adequados à idade e à maturidade dos alunos.
b) Se sítios indesejáveis chegarem ao conhecimento de alunos, professores ou outros, o endereço será comunicado ao Coordenador de Segurança Digital que, por sua vez, documentará o incidente e fá-lo-á chegar ao Órgão de Gestão, conforme adequado.
c) Qualquer material que a Escola considere ser ilegal será denunciado através dos mecanismos oficiais.
d) A estratégia de acesso à Internet da Escola deve ser delineada de forma a estar em consonância com a idade e o currículo dos alunos.

e) A Escola deverá garantir que os sistemas adequados de filtragem e controlo estão implementados de forma a evitar que pessoal e alunos possam aceder a conteúdo inadequado ou ilegal.
f) A Escola irá tomar todas as precauções razoáveis para garantir que os usuários acedam apenas a material apropriado. No entanto, devido à natureza global e conetividade do conteúdo disponível na Internet, nem sempre é possível garantir que o acesso a material inadequado nunca ocorrerá através de uma configuração ou dispositivo Escolar.
g) A Escola irá auditar o uso da tecnologia para determinar se a Política de Segurança Digital é adequada e que a sua implementação é apropriada.
h) Os métodos para identificar, avaliar e minimizar os riscos online serão revistos regularmente pela Equipa de Segurança Digital da Escola.

7. Conhecimento das políticas

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

a) A Política de Segurança Digital está disponível, para conhecimento e consulta, no sítio Web do Agrupamento,
b) 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.
c) No sítio Web do Agrupamento são disponibilizados recursos de apoio para uma utilização segura e responsável da Internet e de equipamentos informáticos.
d) O Agrupamento chamará a atenção dos pais para a sua Política de Segurança Digital, através de jornal Escolar, de informação a entregar no ato da matrícula, das reuniões regulares a realizar com os diretores de turma e do seu sítio Web na Internet.

Agrupamento de Escolas de Anadia, 19 de fevereiro de 2020