

Política de Segurança Digital

e-safety

Agrupamento de Escolas de Oliveira do Hospital



Índice

1.	Objetivos e âmbito da Política de Segurança Digital	4
1.1	Redação e revisão da Política de Segurança Digital.....	5
2.	Principais responsabilidades.....	5
2.1	Competências do Órgão de Gestão e da Equipa PTE.....	5
2.2	Competências do Coordenador PTE.....	6
2.3	Pessoal Docente, Pessoal Não Docente, Alunos, Prestadores de Serviços ou de Apoio.....	6
3.	Ensino, Avaliação e Aprendizagem.....	8
3.1	Importância da Internet.....	8
3.2	Benefícios da utilização da Internet no ensino	8
3.3	Formas de a Internet melhorar a avaliação e a aprendizagem	8
3.4	Avaliação de conteúdos digitais	9
3.5	Educação para a Segurança na Internet	9
4.	Comunicação <i>Online</i> e Utilização Segura da Tecnologia	10
4.1	<i>Website(s)</i>	10
4.2	Publicação de imagens, vídeos, atividades ou trabalhos dos alunos <i>online</i>	10
4.3	Administração do correio eletrónico	11
4.4	Utilização segura e adequada, em contexto de sala de aula, da Internet ou de quaisquer dispositivos associados.....	12
4.5	Telemóveis e equipamentos pessoais	12
4.6	Utilização de equipamentos pessoais pelos alunos.....	13
5.	Redes Sociais.....	13
5.1	Disposições gerais	13
5.2	Uso oficial das redes sociais.....	14
5.3	Uso pessoal das redes sociais	15
6.	Gestão de sistemas de informação.....	16
6.1	Sistemas de filtragem	16
7.	Reduzindo os riscos <i>online</i>	17
7.1	Tecnologias emergentes	17
7.2	Autorização e utilização da Internet no recinto escolar.....	17

7.3	Incidentes preocupantes.....	18
7.4	Denúncias relacionadas com a segurança digital.....	18
7.5	<i>Cyberbullying</i>	19
8.	Disposições finais.....	20

POLÍTICA DE SEGURANÇA DIGITAL (PSD)

A sociedade enfrenta atualmente novos desafios, decorrentes de uma globalização e desenvolvimento tecnológico em aceleração, tendo a escola de preparar os alunos, que serão jovens e adultos em 2030, para empregos ainda não criados, para tecnologias ainda não inventadas, para a resolução de problemas que ainda se desconhecem. (preâmbulo do DL 55/2018, de 6 de julho)

A segurança digital abrange questões relacionadas não só com crianças e jovens como também com adultos e com a utilização que todos fazem da Internet, maioritariamente através dos telemóveis, em ambiente escolar e fora dele. Isto exige a formação de todos os elementos da comunidade escolar sobre os riscos e responsabilidades de todos os que trabalham com crianças e jovens.

A escola está ciente de que é impossível evitar totalmente que alunos e outros membros da comunidade escolar sejam expostos a riscos quando utilizam a Internet. As crianças e jovens devem ser sensibilizados e ensinados a obter as competências necessárias para tomar decisões seguras e responsáveis. Todos os professores devem ter consciência da importância das boas práticas de segurança digital na sala de aula com vista a educar e proteger as crianças e jovens sob o seu cuidado.

A política de segurança digital (PSD) é essencial na definição do modo como o Agrupamento planeia desenvolver e estabelecer a sua abordagem à segurança digital.

Esta PSD vai ao encontro do Perfil dos alunos à Saída da Escolaridade Obrigatória (PASEO).

1. Âmbito e objetivos da Política de Segurança Digital

O Agrupamento de Escolas de Oliveira do Hospital considera a segurança digital um elemento essencial de salvaguarda das crianças, jovens e adultos no mundo digital, ao usar tecnologia, como computadores, *tablets*, telemóveis ou consolas de jogos; deve ser garantida a todos os alunos, professores e funcionários; o Agrupamento de Escolas de Oliveira do Hospital tem o dever, de acordo com os recursos humanos e técnicos, 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.

Os objetivos da PSD do Agrupamento de Escolas de Oliveira do Hospital são:

- Identificar claramente os princípios fundamentais, seguros e responsáveis, esperados de todos os membros da comunidade em relação à tecnologia, como forma de garantir um ambiente seguro no que concerne à utilização de equipamentos e da Internet.
- Sensibilizar todos os membros para os potenciais riscos, bem como para os benefícios da tecnologia.

- 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 a tecnologia.
- Identificar procedimentos claros a adotar de forma a responder às preocupações de segurança *online* que são 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, visitantes, voluntários e outras pessoas que trabalham para ou prestam serviços em nome da escola (coletivamente e adiante referidos como «pessoal» neste documento), 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 Política de Segurança Digital é da responsabilidade do Coordenador PTE. Esta PSD é discutida e aprovada em Conselho Pedagógico e revista anualmente.

A Política de Segurança Digital foi redigida pelo Agrupamento, tendo por base a Política do Selo de Segurança Digital e as orientações governamentais.

Política de Segurança Digital proposta pelo Coordenador PTE: Hilário Russo

Revisão do documento *Política de Segurança Digital* pela docente : Isabel Cappelle

Design da Capa: Teresa Batista

Política aprovada pelo Diretor em: 22/06/2022

Política aprovada pelo Conselho Pedagógico em: ??/??/2022

Data da próxima revisão da Política: julho 2023

2. Principais responsabilidades

2.1 Competências do Órgão de Gestão e da Equipa PTE

- a) Desenvolver e promover uma visão e cultura de segurança *online* para todas as partes envolvidas, em linha com as recomendações nacionais e locais, apoiando e consultando adequadamente toda a comunidade escolar.

- b) Garantir que a segurança *online* é vista proativamente por toda a comunidade como uma questão de salvaguarda.
- c) Apoiar o Coordenador PTE, 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.

2.2 Competências do Coordenador PTE

- a) Agir como um ponto de contacto e ligação com outros membros do pessoal e outras agências, conforme apropriado, em relação a todas as questões de segurança *online*.
- b) Manter-se atualizado sobre 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 o agrupamento 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 do agrupamento e outras agências, conforme apropriado, em questões de segurança *online*.
- h) Facilitar a ligação com organismos locais e nacionais, conforme apropriado.
- i) Trabalhar com a Comissão Técnica na revisão e atualização da Política de Segurança Digital, Políticas de Utilização Aceitável (PUA) e outras políticas relacionadas numa base regular (pelo menos anualmente).
- j) Garantir que a segurança *online* é integrada noutras políticas e procedimentos do agrupamento de forma apropriada.

2.3 Pessoal Docente, Pessoal Não Docente, Alunos, Prestadores de Serviços ou de Apoio

As principais responsabilidades para **todos os membros** (pessoal) são:

- Contribuir para o desenvolvimento da Política de Segurança Digital.
- Ler as Políticas de Utilização Aceitável (PUA), aceitando-as, cumprindo-as e fazendo-as cumprir.

- Assumir a sua responsabilidade individual pela segurança dos sistemas eletrônicos da escola.
- Ter consciência de uma variedade de diferentes questões relacionadas com a segurança *online* e como elas podem afetar os alunos.
- Apresentar boas práticas na utilização das novas tecnologias.
- Incorporar a educação para a segurança *online* no currículo, sempre que possível.
- Identificar situações individuais de preocupação e tomar medidas apropriadas, seguindo as políticas e procedimentos de salvaguarda da escola.
- Ser capaz de sinalizar, para o apoio adequado disponível, as questões de segurança *online*, interna e externamente.
- Saber quando e como escalar questões de segurança *online*, interna e externamente.
- Manter um nível de conduta profissional no 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 (PUA) e respeitá-las.
- Respeitar os sentimentos e os direitos dos outros, tanto *online* como *offline*.
- Procurar a ajuda de um adulto de confiança, em caso de necessidade, e apoiar outros alunos que possam estar a enfrentar problemas de segurança *online*.

A um nível que é adequado à sua idade, capacidades e vulnerabilidades, o aluno deve:

- Assumir a responsabilidade de manter a sua segurança e a dos outros *online*.
- Assumir a responsabilidade, pela sua própria consciência e aprendizagem, em relação às oportunidades e riscos decorrentes das tecnologias novas e emergentes.
- 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:

- Ler a Política de Utilização Aceitável (PUA) da escola, incentivando os seus filhos ou educandos à sua adesão, e aderindo eles próprios, se for o caso.
- 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.
- Ser um modelo apropriado na utilização racional da tecnologia e na adoção de comportamentos seguros *online*.
- Identificar mudanças no comportamento que possam indicar que o seu filho ou educando está em risco de dano *online*.
- Procurar ajuda e apoio da escola, ou de outros órgãos competentes, se os seus filhos ou educandos encontrarem problemas ou preocupações *online*.

- Assumir a responsabilidade, pela sua própria consciência e aprendizagem, em relação às oportunidades e riscos decorrentes das tecnologias novas e emergentes.

3. Ensino, Avaliação e Aprendizagem

3.1 Importância da Internet

A utilização da Internet faz parte integrante do currículo formal sempre que possível e é uma ferramenta essencial na aprendizagem.

A Internet faz parte do dia-a-dia no ensino.

Os alunos utilizam a Internet amplamente dentro e fora da escola e devem saber como avaliar a informação que obtêm na Internet e como se podem proteger.

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.

3.2 Benefícios da utilização da Internet no ensino

Os benefícios da utilização da Internet no ensino incluem:

- Acesso a recursos pedagógicos e educativos de todo o mundo, incluindo visitas virtuais a museus e galerias de arte.
- Intercâmbio cultural e educativo entre alunos de várias escolas e realidades.
- 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.
- Possibilidade de aprendizagem quando e onde for mais conveniente.

3.3 Formas de o recurso à Internet melhorar a avaliação e a aprendizagem

O acesso à Internet no agrupamento é pensado com vista a alargar e reforçar a educação.

Ensinar-se-á aos alunos o que é uma utilização correta da Internet, e ser-lhes-ão indicados objetivos claros quando a utilizam.

O agrupamento 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 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.

Os níveis de acesso à Internet serão revistos de modo a corresponderem aos requisitos do currículo e à idade e capacidades dos alunos.

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.

Os alunos aprenderão 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.

3.4 Avaliação de conteúdos digitais

Deve ensinar-se os alunos a serem críticos em relação aos materiais que leem e a validar uma informação antes de aceitar a sua exatidão.

Deve orientar-se os alunos para o uso de ferramentas de pesquisa, adequadas à sua idade.

A avaliação de materiais da Internet faz parte do processo de ensino e de aprendizagem de qualquer disciplina e é considerada um requisito transversal à escola e ao currículo e uma responsabilidade do professor.

3.5 Educação para a Segurança na Internet

O Agrupamento de Escolas de Oliveira do Hospital disponibiliza um currículo de segurança *online* através das aulas de AEOH On no 2º CEB e TIC no 3º CEB. Para além do currículo, este assunto é explorado no projeto Biblioteca Digital, na participação dos alunos nos projetos Erasmus+, *eTwinning*, Clube de Robótica, de forma a aumentar a consciencialização sobre a importância da utilização segura e responsável da Internet entre os alunos.

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.

A educação sobre o uso seguro e responsável deverá anteceder o acesso à Internet.

Os alunos serão apoiados na leitura e compreensão da **Política de Utilização Aceitável** para que esta se adapte à sua idade e capacidades.

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

A escola deve estar consciente de que algumas crianças e jovens podem ser considerados mais vulneráveis *online*, devido a uma variedade de fatores.

Os utilizadores deverão ser informados 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.

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.

Os membros do pessoal com a responsabilidade de gerir sistemas de filtragem ou monitorizar o uso das TIC serão supervisionados pelo Coordenador PTE e terão procedimentos claros para relatar problemas ou preocupações.

4. Comunicação *Online* e Utilização Segura da Tecnologia

4.1 Websites

Os detalhes de contacto no(s) *site(s)* escolares apenas poderão ser o endereço físico do agrupamento, hiperligações autorizadas, endereço de correio eletrónico oficial e número de telefone e/ou fax. Nenhuma informação pessoal dos alunos deverá ser publicada.

O Órgão de Gestão assumirá a responsabilidade editorial global pelo conteúdo *online* publicado e garantirá que as informações são precisas e adequadas, de acordo com a política de comunicação que consta da página da Escola.

O(s) *site(s)* cumprirão as orientações da escola para publicações, incluindo a acessibilidade, o respeito pelos direitos de propriedade intelectual, políticas de privacidade e de direitos de autor.

Os trabalhos, imagens ou vídeos dos alunos serão publicados com a permissão dos pais ou encarregados de educação.

A conta de administrador para o sítio oficial da escola será salvaguardada com uma senha apropriadamente forte.

O agrupamento irá postar informações sobre a salvaguarda, incluindo a segurança *online*, no sítio oficial da escola, para os membros da comunidade, incluindo esta PSD.

4.2 Publicação de imagens, vídeos, atividades ou trabalhos dos alunos *online*

O Agrupamento tem uma política clara relativamente à utilização de imagens de alunos onde se definem regras e procedimentos (Política de Utilização de Imagem). No início do ano, todos os EE assinam a permissão para o efeito.

Todas as imagens e vídeos compartilhados *online* serão utilizados de acordo com a Política de Utilização de Imagem do Agrupamento.

O Agrupamento garantirá igualmente que todo o uso de imagens, vídeos ou outro material digital se realizará em conformidade com outras políticas e procedimentos, incluindo a segurança e proteção dos dados, Políticas de Utilização Aceitável e códigos de conduta.

Em linha com a política de imagem, a autorização por escrito dos pais e encarregados de educação será sempre obtida antes das imagens/vídeos de alunos serem publicados *online*.

Os nomes completos dos alunos não serão utilizados em parte alguma do(s) *site(s)* da escola, em especial junto a fotografias.

4.3 Administração do correio eletrónico

A administração da conta de correio eletrónico institucional do agrupamento é da responsabilidade da direção do AEOH.

Todos os membros do pessoal docente, não docente e discente devem possuir um endereço de correio eletrónico a ser usado para qualquer comunicação oficial.

Qualquer comunicação eletrónica, que contenha conteúdo que possa violar a legislação de proteção de dados (por exemplo, informações confidenciais ou pessoais), só será enviada como *email* seguro e criptografado.

Os membros da comunidade escolar devem avisar imediatamente o Coordenador PTE se receberem comunicação ofensiva e esta será gravada de forma a agir apropriadamente.

Os professores e o Órgão de Gestão serão incentivados a desenvolver um equilíbrio adequado às suas responsabilidades profissionais ao iniciar ou responder a mensagens de correio eletrónico, especialmente se a comunicação ocorrer com os alunos e/ou pais e encarregados de educação.

As mensagens de correio eletrónico enviadas a organizações externas devem ter o mesmo rigor e formalidade, que uma comunicação oficial escrita em papel timbrado da escola.

O(s) endereço(s) de correio eletrónico da escola e outros detalhes de contacto oficiais não poderão ser utilizados para a criação de contas pessoais em redes sociais.

Os alunos têm de informar imediatamente o professor designado para o efeito caso recebam mensagens de email ofensivas.

Os alunos não podem revelar dados pessoais sobre eles próprios ou outros numa mensagem eletrónica, nem combinar encontrar-se com alguém sem autorização expressa de um adulto.

O acesso a contas de email pessoais dentro da escola pode ser bloqueado.

A utilização abusiva do email para fins sociais pode interferir com a aprendizagem e será restringida.

4.4 Utilização segura e adequada, em contexto de sala de aula, da Internet ou de quaisquer dispositivos associados

A utilização da Internet é fundamental no acesso à educação e todos os alunos 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.

Os níveis de acesso à Internet serão revistos para refletir as exigências curriculares e a idade e capacidade dos alunos.

Todos os professores devem estar cientes de que não podem contar exclusivamente com os sistemas de filtragem para proteger os alunos e que a supervisão, gestão de sala de aula e educação sobre uso seguro e responsável é essencial e da sua responsabilidade.

Os alunos deverão desenvolver atividades *online/offline*, com recurso a ferramentas adequadas, de acordo com a sua idade, e sempre com a supervisão do professor.

Todos os dispositivos da escola serão utilizados de acordo com a respetiva Política de Utilização Aceitável e com a segurança apropriada.

Os professores deverão, previamente, analisar e avaliar os *sites*, ferramentas e aplicativos de uso em sala de aula ou a recomendar para uso em casa.

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.

A escola tomará todas as medidas necessárias para que a utilização da Internet seja realizada num ambiente seguro.

4.5 Telemóveis e equipamentos pessoais

A utilização de telemóveis e outros equipamentos pessoais por parte de professores apenas é permitida em contexto de sala de aula, baseada numa utilização pedagógica fundamentada, de acordo com o ponto 5 do artigo 87.º do Regulamento Interno. Excetua-se a sua utilização no(s) período(s) de descanso devidamente autorizado(s) e nos locais reservados.

A utilização de telemóveis e outros equipamentos pessoais por parte do restante pessoal no recinto escolar é proibida. Excetua-se a sua utilização no(s) período(s) de descanso devidamente autorizado(s) e nos locais reservados.

O envio de mensagens ou conteúdos abusivos ou inadequados, através de telemóveis ou equipamentos pessoais por parte de qualquer elemento da escola, é desaconselhável.

Os professores podem confiscar um telemóvel ou equipamento se se considerar que está a ser utilizado de modo contrário às políticas do agrupamento em matéria de conduta ou *bullying*, de acordo com o artigo 96.º, alínea e), ponto 6 do Regulamento Interno. O Órgão de Gestão pode fazer uma pesquisa ao telemóvel ou equipamento com o consentimento dos pais ou 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.

Os professores, alunos 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.

4.6 Utilização de equipamentos pessoais pelos alunos

Se um aluno violar as políticas da escola, o seu telemóvel ou equipamento será apreendido e guardado em local seguro na escola, de acordo com o artigo 96.º, alínea e), ponto 6 do Regulamento Interno. Os telemóveis e outros equipamentos pessoais serão entregues aos pais ou encarregados de educação, em conformidade com as políticas da escola.

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.

Os alunos não estão autorizados a utilizar telemóveis nos locais onde decorram aulas ou outras atividades formativas, exceto quando a utilização de qualquer dos meios acima referidos esteja diretamente relacionada com as atividades a desenvolver e seja expressamente autorizada pelo professor ou pela direção (cf. artigo o artigo 96.º, alínea e), ponto 6 do Regulamento Interno).

Durante o período letivo, os telemóveis e outros equipamentos deverão estar desligados ou em modo de "silêncio", a comunicação Bluetooth e WiFi deverão estar desligadas. Os referidos equipamentos não serão utilizados em períodos letivos, exceto em emergências autorizadas pelo Órgão de Gestão.

Se, por motivos pedagógicos, os professores pretenderem que os alunos utilizem telemóveis ou outros equipamentos pessoais numa atividade educativa, isso será feito de acordo com esta Política de Segurança Digital.

5. Redes Sociais

5.1 Disposições gerais

A utilização segura e responsável dos meios de comunicação social, nomeadamente as redes sociais, será preocupação de todos os membros do Agrupamento de Escolas de Oliveira do Hospital, como forma de proteger tanto a escola como a comunidade em geral, *online* e *offline*. Podem incluir-se nas redes sociais: *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.

Todo o pessoal do Agrupamento de Escolas de Oliveira do Hospital será incentivado a envolver-se nas *redes* sociais de uma maneira positiva, segura e responsável, em todos os momentos.

Todo o pessoal do AEOH, incluindo alunos, é aconselhado a não publicar detalhes específicos e privados, pensamentos, preocupações, imagens ou mensagens em quaisquer serviços de *rede* social, especialmente conteúdo que possa ser considerado ameaçador, prejudicial ou difamatório aos outros ou para com a instituição.

O Agrupamento de Escolas de Oliveira do Hospital reserva-se o direito de controlar e/ou vedar o acesso de alunos e restante pessoal às diversas redes sociais e *sites* de redes sociais, quando realizado no local e se resultar do uso de dispositivos ou sistemas escolares.

O uso de aplicações de redes sociais durante o horário escolar para uso pessoal não é permitido (exceção(m)-se o(s) período(s) de descanso devidamente autorizado(s) e nos locais apropriados).

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.

Quaisquer preocupações relativas à conduta *online* de qualquer membro do Agrupamento de Escolas de Oliveira do Hospital em *sites* de *redes* sociais devem ser comunicadas ao Órgão de Gestão e serão geridas em conformidade com as políticas da escola (cf. PUA, Ponto 15).

Quaisquer violações das políticas explícitas do agrupamento 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

O uso oficial das redes sociais pelo agrupamento visa exclusivamente o trabalho educacional, através da divulgação ou comunicação destinada, por exemplo, a aumentar o envolvimento dos pais e encarregados de educação.

A utilização oficial das redes sociais como ferramentas de comunicação será avaliada e fundamentada formalmente pelo Órgão de Gestão, depois de ouvida a Equipa de Manutenção e Gestão de Recursos Tecnológicos.

Os canais oficiais do agrupamento 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.

Toda a comunicação nas plataformas oficiais deve ser clara, transparente e aberta ao escrutínio.

Qualquer publicação *online* em *sites* oficiais ou de *rede* social (Bibliotecas Escolares, do Clube Europeu e outros Clubes) 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.

Imagens, vídeos ou trabalhos de alunos só serão compartilhadas em *sites* de *rede* social, canais oficiais ou redes sociais de acordo com a Política de Utilização de Imagem.

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.

Os responsáveis que gerem os canais oficiais do agrupamento, 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.

É proibida a comunicação direta com pais, encarregados de educação ou alunos através de qualquer canal de rede social.

Os membros do pessoal serão incentivados a gerir e controlar, de forma responsável, o conteúdo que partilharem e publicarem *online*.

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 PTE ou do Órgão de Gestão antes de utilizarem redes sociais na sala de aula.

As opiniões pessoais do pessoal não refletem nem vinculam a posição oficial da escola como instituição.

5.3 Uso pessoal das redes sociais

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.

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.

Os alunos serão aconselhados a não promover encontros *online* sem a permissão dos pais ou outro adulto responsável e apenas na sua presença.

Os alunos serão informados sobre a segurança adequada em sites de *rede* social e serão incentivados a utilizar em segurança senhas, negar o acesso a indivíduos desconhecidos e a aprender a bloquear e relatar comunicações não desejadas.

Qualquer atividade de *rede social* oficial, envolvendo alunos no recinto escolar ou em atividades escolares, deverá ser sempre moderada pela escola, nunca pelos professores ou funcionários através das suas contas pessoais.

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

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.

Os utilizadores devem assumir responsabilidade pela utilização da Internet.

Os computadores de trabalho devem estar protegidos contra determinadas ações inadvertidas ou deliberadas dos utilizadores.

Os computadores de trabalho deverão ter mais do que um navegador de Internet, contendo extensões que permitam bloquear publicidade e navegar de forma privada, incluindo o uso de motores de pesquisa com a inclusão de navegação em privado.

Toda a rede interna deve ter instalada e atualizada uma proteção antivírus e *firewall*.

O acesso por dispositivos sem fios deve ser administrado proativamente e estar sujeito a um nível de segurança mínimo com encriptação WPA2.

A segurança dos sistemas informáticos da escola e dos utilizadores será revista com regularidade.

A proteção antivírus será atualizada com regularidade.

As regras da *firewall* devem ser conhecidas e atualizadas de acordo com as ameaças de cibersegurança.

Os dispositivos amovíveis podem ser utilizados sem restrições, uma vez que todos os equipamentos dispõem de rastreio através do antivírus de rede.

Nenhum *Software* não aprovado será autorizado nas áreas de trabalho ou como anexo de mensagens eletrónicas.

Os ficheiros guardados na rede da escola ou nos postos de trabalho serão verificados com regularidade.

A utilização de nomes de utilizador e palavras-passe para aceder à rede da escola ou aos postos de trabalho deverá ser obrigatória (aplicações de gestão dos alunos e do correio eletrónico, entre outras).

Sempre que possível, serão integradas extensões de programas nos navegadores de Internet, (tais como o *Adblock Plus* ou outros semelhantes), o que permitirá a utilização de uma navegação mais privada e com menor índice de publicidade não desejada, durante o uso da *web*.

É aconselhada a configuração de um motor de pesquisa por defeito nos navegadores de Internet, com navegação privada.

6.1 Sistemas de filtragem

O acesso à Internet fornecido pelo agrupamento incluirá sistemas de filtragem adequados à idade e à maturidade dos alunos.

Se sítios indesejáveis chegarem ao conhecimento de alunos, professores ou outros, o endereço será comunicado ao Coordenador PTE que, por sua vez, documentará o incidente e fá-lo-á chegar ao Órgão de Gestão, conforme adequado.

Qualquer material que a escola considere ilegal será denunciado através dos mecanismos oficiais.

A estratégia de acesso à Internet do agrupamento deve ser delineada de forma a estar em consonância com a idade e o currículo dos alunos.

O Agrupamento 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.

O Agrupamento irá tomar todas as precauções razoáveis para garantir que os utilizadores acedam apenas a material apropriado. No entanto, devido à natureza global e conectividade 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.

O Agrupamento irá auditar o uso da tecnologia para determinar se a Política de Segurança Digital é adequada e que a sua implementação é apropriada.

Os métodos para identificar, avaliar e minimizar os riscos *online* serão revistos regularmente pelo Coordenador PTE.

7. Reduzindo os riscos *online*

7.1 Tecnologias emergentes

O Agrupamento de Escolas de Oliveira do Hospital está ciente de que a Internet é um ambiente em constante mudança, com novos aplicativos, ferramentas, dispositivos, *sites* e materiais a emergir a um ritmo rápido. Cabe a cada professor examinar e avaliar as tecnologias emergentes de acordo com o seu benefício educacional, solicitando, se necessário, o parecer ou opinião do Coordenador PTE.

De acordo com o Regulamento Interno e a Política de Segurança Digital, os dispositivos móveis estão proibidos no contexto escolar e serão confiscados, exceto se devidamente autorizados por um responsável pedagógico.

7.2 Autorização e utilização da Internet no recinto escolar

Os pais e encarregados de educação deverão ser informados que é fornecido aos alunos acesso supervisionado à Internet, apropriado para a sua idade e capacidades.

Os pais e encarregados de educação são convidados a ler/ analisar a Política de Utilização Aceitável para o acesso dos alunos, com os seus filhos/ educandos.

Ao considerar o acesso para os membros vulneráveis da comunidade (nomeadamente, os alunos com necessidades educativas especiais), a escola tomará as decisões com base nas necessidades específicas de cada um.

A utilização de quaisquer recursos informáticos requer o conhecimento prévio e a assinatura da Política de Utilização Aceitável das TIC por todos os elementos da escola.

O acesso à rede de Internet do agrupamento está vedado a todos os visitantes, exceto em caso de necessidade extrema e mediante autorização do Órgão de Gestão ou do Coordenador de Segurança Digital, ficando sujeitos a esta Política de Segurança Digital e às restantes Políticas de Utilização Aceitável.

7.3 Incidentes preocupantes

A observação do comportamento dos alunos é essencial na deteção de situações preocupantes e na criação da confiança necessária à partilha, com os professores, de problemas.

Todos os elementos da escola serão informados sobre como proceder para comunicar situações preocupantes do ponto de vista da segurança digital (tais como, violações do sistema de filtragem, *Cyberbullying*, conteúdos ilícitos, etc.).

O Coordenador PTE deverá ser informado de todos os incidentes relacionados com segurança digital que envolvam preocupações ao nível da proteção de menores e fá-los-á chegar ao Órgão de Gestão que agirá em conformidade, nomeadamente através do contacto das entidades competentes.

O agrupamento gerirá os incidentes relacionados com a segurança digital em conformidade com as políticas da escola em matéria de disciplina/conduita. Depois de concluídas eventuais investigações, retirará ilações e, se necessário, tomará medidas.

O agrupamento informará os pais/encarregados de educação de quaisquer incidentes ou preocupações, quando e como considerar mais adequado.

Sempre que houver razões para crer ou recear que ocorreu alguma atividade ilegal, o AEOH contactará a Equipa de CPCJ, o responsável pelas questões de segurança digital ou outra pessoa competente e encaminhará a situação para a GNR.

7.4 Denúncias relacionadas com a segurança digital

As queixas relativas à utilização indevida da Internet serão tratadas no quadro dos procedimentos de apresentação de queixas ou denúncias adotadas pelo agrupamento, de acordo com o art.º 113.º do Regulamento Interno.

Quaisquer queixas que envolvam a utilização indevida da Internet por pessoal docente, não docente ou restante pessoal serão encaminhadas para o Órgão de Gestão.

O agrupamento manterá um registo de todos os incidentes ou queixas relacionadas com a segurança digital, assim como das medidas tomadas.

Os professores e os alunos serão informados dos procedimentos necessários para apresentação de queixas e trabalharão em conjunto com a escola, com vista à resolução dos problemas.

Todos os elementos do agrupamento necessitam de compreender a importância da confidencialidade e a necessidade de seguir os procedimentos oficiais da escola para comunicação de situações preocupantes.

Quaisquer situações (incluindo sanções) serão tratadas de acordo com os procedimentos do AEOH em matéria de conduta, disciplina e proteção de menores.

Todos os elementos do AEOH serão sensibilizados para a importância de manterem uma conduta adequada, durante a utilização da Internet, e de não publicarem comentários, conteúdos, imagens ou vídeos que possam causar dano, prejuízo ou sofrimento a outros elementos da comunidade escolar.

7.5 *Cyberbullying*

O *Cyberbullying* pode ser definido como “A utilização de uma tecnologia, em especial os telemóveis e a Internet, para deliberadamente causar dano ou incomodar alguém”, como tal não será tolerado por qualquer elemento do AEOH.

De uma forma geral, para dar apoio a qualquer elemento da comunidade escolar que seja alvo de *Cyberbullying*, o AEOH adotará procedimentos formais semelhantes ao registo de ocorrências de incidentes preocupantes, no netGIAE.

Todos os incidentes de *Cyberbullying* comunicados ao AEOH serão registados.

Alunos, professores e pais ou encarregados de educação serão aconselhados a manter um registo do *bullying* como prova.

O AEOH tomará medidas para identificar o responsável pela situação de *bullying*, sempre que possível e adequado. Isto poderá passar pela análise dos registos informáticos da escola, por identificar e entrevistar possíveis testemunhas e contactar o fornecedor do serviço e a GNR, se necessário.

Será solicitado a alunos, professores e pais ou encarregados de educação que trabalhem em conjunto com o AEOH, de modo a apoiarem a abordagem do agrupamento em relação ao *Cyberbullying* e à segurança digital.

As sanções para os envolvidos em *Cyberbullying* podem incluir o seguinte:

- O autor poderá ter de retirar a publicação de todo o material considerado inapropriado. Para o efeito, em caso de recusa ou incapacidade, poderá ser contactado o fornecedor do serviço.
- O autor poderá ver suspenso o seu direito de acesso à Internet na escola, durante um determinado período. Poderão ser previstas outras sanções para alunos e professores, em conformidade com as políticas da escola em matéria de conduta e antibullying ou as Políticas de Utilização Aceitável.
- Os pais/encarregados de educação serão informados.
- A GNR será contactada caso se suspeite de ação ilícita.

8. Disposições finais

O AEOH reconhece que os pais e encarregados de educação têm um papel essencial a desempenhar para permitir que as crianças se tornem utilizadores seguros e responsáveis da Internet e da tecnologia digital.

O Agrupamento de Escolas de Oliveira do Hospital disponibiliza-se, através dos seus responsáveis, a fornecer informação e orientação aos pais e encarregados de educação sobre segurança *online*.

Os pais e encarregados de educação deverão ser encorajados a ser um modelo de comportamento positivo para os alunos no que toca à segurança *online*.

O Agrupamento chamará a atenção dos pais e encarregados de educação para a sua Política de Segurança Digital através de boletins informativos ou da sua página web.

Será incentivada uma abordagem de parceria família/escola em relação à segurança digital em casa e na escola. Para esse efeito, poderão ser organizadas sessões com demonstrações e sugestões para uma utilização segura da Internet em casa ou outros eventos direcionados aos pais e encarregados de educação.

Será solicitado aos pais que leiam e debatam com os seus filhos a Política de Utilização Aceitável e a Política de Segurança Digital da escola e respetivas implicações.

O AEOH deve ter uma Política de Utilização Aceitável consubstanciada num documento claro e conciso, orientador do uso adequado e seguro das novas tecnologias na escola e da utilização de equipamentos tecnológicos.

O agrupamento implementará Políticas de Utilização Aceitável, com o intuito de proteger alunos, professores e outros elementos.

Todos os membros do agrupamento deverão estar informados sobre o processo de comunicação das preocupações de segurança *online* (eSafety), tais como violações de filtragem, *sexting*, *Cyberbullying*, conteúdo ilegal, entre outras.

O órgão de Gestão deverá ser informado de qualquer incidente de segurança *online* envolvendo preocupações de proteção da criança.

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

Todos os elementos do AEOH deverão estar sensibilizados para o facto de que a sua conduta, no uso da Internet fora da escola, pode afetar as suas funções e a sua reputação dentro da escola. Podem ser interpostas ações disciplinares, de responsabilidade civil ou outras previstas na lei, caso se considere que desonraram a profissão ou a instituição de ensino ou que a confiança na sua capacidade profissional ficou abalada. O agrupamento deverá informar os pais e encarregados de educação de quaisquer incidentes ou preocupações relativas aos alunos, como e quando necessário. Depois de identificados os possíveis incidentes, o AEOH deve implementar as alterações, conforme necessário.

Pais, encarregados de educação, alunos e restante pessoal têm a obrigação de trabalhar em parceria com o agrupamento de forma a resolver atempada e satisfatoriamente os problemas surgidos.

Serão disponibilizadas informações aos alunos e pais e encarregados de educação sobre recursos úteis e sítios na Internet, sistemas de filtragem e atividades pedagógicas e lúdicas, que abordem uma utilização positiva e responsável da Internet.

A Política de Segurança Digital será apresentada formalmente e discutida com todos os elementos do AEOH.

Este documento fará parte integrante do Plano de Ação de Desenvolvimento Digital Escolas (PADDE), integrando o campo das Infraestruturas.

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