



---

# Política de Segurança Digital

---

Agrupamento de Escolas Dr. Manuel Gomes de Almeida

---

2018-2021

---

O uso das Tecnologias de Informação é inerente ao perfil dos alunos deste século XXI. O uso de tecnologias de informação e comunicação é uma mais-valia para o processo de ensino-aprendizagem, no entanto, este acesso deve ser seguro e eficaz. Assim, a Segurança na Internet e a consequente definição de uma Política de Segurança Digital vai permitir ajudar a garantir o uso adequado, eficaz e seguro das comunicações eletrónicas.

## Índice

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

<b>7.1. Tecnologias emergentes .....</b>	<b>16</b>
<b>7.2. Autorização e utilização da Internet no recinto escolar .....</b>	<b>17</b>
<b>7.3. Incidentes preocupantes .....</b>	<b>17</b>
<b>7.4. Denúncias relacionadas com a segurança digital .....</b>	<b>18</b>
<b>7.5. Cyberbullying .....</b>	<b>18</b>
<b>8. Disposições finais.....</b>	<b>19</b>
<b>9. Bibliografia/Webgrafia .....</b>	<b>21</b>

## **POLÍTICA DE SEGURANÇA DIGITAL (eSafety)**

Nos nossos dias, crianças, jovens e adultos interagem diariamente com tecnologias desde o simples telemóveis, a consolas de jogos e à Internet e vivenciam uma grande variedade de oportunidades, atitudes e situações. A troca de ideias, a interação social e as oportunidades de aprendizagem daí decorrentes apresentam enormes benefícios para todos, mas podem por vezes colocar crianças, jovens e adultos em perigo.

A segurança digital abrange questões relacionadas não só com crianças e jovens como também com adultos e com a utilização que todos fazem da Internet, dos telemóveis e outras tecnologias de comunicação eletrónica em ambiente escolar e fora dele. Isto exige a formação de todos os elementos da comunidade escolar sobre os riscos e responsabilidades envolvidos e faz parte do "dever de cuidado" aplicável a todos os que trabalham com crianças.

O agrupamento de escolas 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. Os alunos 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. Todos os professores devem ter consciência da importância de boas práticas de segurança digital na sala de aula com vista a educar e proteger os alunos sob o seu cuidado.

A política de segurança digital é essencial na definição de como o agrupamento 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. Objetivos e âmbito da Política de Segurança Digital**

Este agrupamento acredita que a segurança digital (eSafety) é um elemento essencial de salvaguarda de todos no domínio do mundo digital, ao usar tecnologia, sejam computadores, tablets, telemóveis, consolas de jogos,...

A Internet e as tecnologias de informação e comunicação são uma parte importante da vida quotidiana, pelo que todos, desde criança, devem ser apoiados/orientados para serem capazes de aprender a desenvolver estratégias de gestão e resposta ao risco online.

Este agrupamento, nas suas várias escolas, tem o dever de proporcionar à comunidade docente, de acordo com as suas possibilidades técnicas e disponibilidade de recursos, 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 agrupamento considera que há uma clara obrigação de garantir que todos os seus alunos e funcionários estão protegidos dos potenciais perigos online.

Os objetivos desta **Política de Segurança Digital (PSD)** do nosso agrupamento 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 nas várias escolas do agrupamento haja um ambiente seguro, também, no que concerne à utilização de equipamentos e da Internet.
- sensibilizar todos os membros das diversas escolas do agrupamento sobre os potenciais riscos, bem como dos 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.

Esta **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/agrupamento (coletivamente e adiante referidos como «**pessoal**» nesta Política), 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.

### 1.1. Redação e revisão da Política de Segurança Digital

A definição, coordenação e implementação da Política de Segurança Digital é da responsabilidade da Equipa de Segurança Digital constituída pelo Órgão de Gestão, representada pelo seu director e coordenadores de cada escola, e pelo Coordenador de Segurança Digital, representado pela Assessora TIC.

Esta Política de Segurança Digital é discutida e aprovada em Conselho Pedagógico.

A nossa Política de Segurança Digital foi redigida pelo agrupamento, tendo por base a Política do Selo de Segurança Digital, as orientações governamentais, o Perfil dos alunos para o século XXI e o Regulamento Interno deste agrupamento.

---

Política aprovada pelo diretor em \_\_\_\_\_

Política aprovada pelo Conselho Pedagógico em \_\_\_\_\_

A data da próxima revisão da Política é setembro de 2021.

---

## 2. Principais responsabilidades

### 2.1. Competências do Órgão de Gestão e da Equipa de Segurança Digital

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.

Garantir que a segurança online é vista proativamente por toda a comunidade como uma questão de salvaguarda.

Apoiar o Coordenador de Segurança Digital, garantindo que tenha tempo e recursos suficientes para cumprir o seu papel de segurança online e demais responsabilidades.

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.

Tomar conhecimento e decidir acerca de quaisquer incidentes de segurança online.

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 de Segurança Digital

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.

Manter-se atualizado com a pesquisa atual, legislação e tendências em matéria de segurança online.

Em colaboração com o grupo de docência de Informática, promover a participação em eventos locais ou nacionais para promover o comportamento online positivo, por exemplo, o Dia Europeu da Internet Segura.

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.

Trabalhar com a(s) escola(s) para a proteção e segurança de dados, de forma a garantir que a prática está de acordo com a legislação vigente.

Monitorizar as definições de segurança online para identificar as lacunas e usar esses dados para atualizar a resposta da escola a essas necessidades.

Informar a equipa de gestão da escola e outras agências, conforme apropriado, em questões de segurança online.

Facilitar a ligação com organismos locais e nacionais, conforme apropriado.

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 (pelo menos anualmente).

Garantir que a segurança online é integrada noutras políticas e procedimentos da escola 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 (PUAs), aceitando-as, cumprindo-as e fazendo-as cumprir.
- Assumir a sua responsabilidade individual pela segurança dos sistemas eletrónicos da escola.
- Ter consciência de uma variedade de diferentes questões relacionadas com a segurança online e como elas podem afetar os alunos sob os seus cuidados.
- 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 seu uso pessoal da tecnologia, dentro e fora do local de trabalho.

As principais responsabilidades dos alunos são:

- Contribuir positivamente para o desenvolvimento das políticas de segurança online.
- Ler ou pedir que lhes sejam lidas as Políticas de Utilização Aceitável (PUAs) e respeitá-las.
- Respeitar os sentimentos e os direitos dos outros, tanto online como offline.
- Procurar a ajuda de um adulto de confiança, se as coisas correrem mal, e apoiar outros que podem estar enfrentando problemas de segurança online.

De acordo com o adequado ao seu nível etário, capacidades e vulnerabilidades:

- Assumir a responsabilidade por manter-se a si e aos outros seguros 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 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.
- 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 e Aprendizagem

### 3.1. Importância da Internet

A utilização da Internet é 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 fora da escola e devem saber como avaliar a informação que obtêm na Internet e como se devem 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 não só nacionais mas de todo o mundo;
- Alargar horizontes e aprofundar aprendizagens;
- Possibilidade de aprendizagem quando e onde for mais conveniente
- 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.

### 3.3. Formas da Internet melhorar a aprendizagem

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

Aos alunos são ensinadas regras e orientações para o que é ou não uma utilização aceitável da Internet, e indicados objetivos claros quando utilizam a Internet.

A escola assegura que o software utilizado na escola é licenciado e que os 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 assegura 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 definidos 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 aprendem 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-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.

Deve-se mostrar-lhes ferramentas de pesquisa da Internet que sejam adequadas à sua idade.

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.

### **3.5. Educação para a Segurança na Internet**

O agrupamento disponibiliza um currículo de segurança online, inicialmente através atividades de enriquecimento curricular na área das TIC, evoluindo para disciplinas específicas do grupo de Informática, de forma a aumentar a consciencialização sobre a importância da utilização segura e responsável da Internet entre os alunos e de acordo com o seu nível etário.

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.

Pretende-se que a educação sobre o uso seguro e responsável anteceda 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 que o uso da Internet será monitorizado.

Considera-se relevante que haja consciência de que algumas crianças/jovens podem ser consideradas mais vulneráveis online, devido a uma variedade de fatores.

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.

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.

## 4. Comunicação Online e Utilização Segura da Tecnologia

### 4.1. Website(s)

Os detalhes de contacto no(s) site(s) escolares e diferentes contas oficiais em plataformas de redes sociais, apenas poderão ser o endereço físico da escola, 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.

O(s) site(s) e outras plataformas 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.

Os endereços de email online deverão ser publicados com cuidado, para evitarem serem recolhidos por spam, sugerindo-se o uso do Bcc (cópia oculta) sempre que o destinatário seja um grupo.

No início do ano letivo, é solicitada aos pais e encarregados de educação a permissão de uso de imagem dos alunos, pelo que os trabalhos, imagens ou vídeos dos alunos serão publicados apenas quando existe essa permissão.

A conta de administrador para todos os sítios oficiais da escola será salvaguardada com senhas apropriadamente fortes.

A escola irá postar informações sobre a salvaguarda, incluindo a segurança online, no página oficial da escola, para todos os membros da comunidade, incluindo esta Política de Segurança Digital.

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

O agrupamento garantirá que todas as imagens e vídeos compartilhados online serão utilizados de acordo com a Política de Utilização de Imagem da escola.

A escola terá uma política clara relativamente à utilização de imagens de crianças/jovens onde se definem regras e procedimentos (Política de Utilização de Imagem).

A escola 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.

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

Em cada ano letivo, e mediante as atividades do plano anual de atividades, em que cada aluno participe, será obtida autorização por escrito dos pais ou encarregados de educação, para utilização da imagem dos seus educandos.

### 4.3. A gestão do correio eletrónico

A gestão da conta de correio eletrónico institucional da escola é da responsabilidade do Órgão de Gestão.

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

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.

Os membros da comunidade escolar devem avisar imediatamente a Equipa de Segurança Digital se receberem comunicação ofensiva, sendo esta objecto de análise de forma a agir apropriadamente.

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

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.

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 e-mail 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 e-mail pessoais dentro da escola pode ser bloqueado.

A utilização excessiva do e-mail 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 quaisquer dispositivos associados**

A utilização da Internet é uma característica fundamental de acesso à educação e todas os alunos recebem 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 são revistos para refletir as exigências curriculares e a idade e capacidade dos alunos.

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

As atividades online dos alunos são supervisionadas. Os alunos devem utilizar ferramentas online/offline e atividades online/offline adequadas à sua idade e devem ter sempre 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 devem sempre analisar e avaliar os sites, ferramentas e aplicativos antes do uso em sala de aula ou da sua recomendação para uso em casa.

A escola garante 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.

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 alunos durante as aulas é proibido, exceptuando-se as aulas em que seja considerada a sua importância pedagógica e um instrumento didático.

Também no caso dos professores, a utilização de telemóveis e outros equipamentos pessoais em contexto de sala de aula apenas é permitido baseado numa utilização pedagógica. 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 proibido. 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 proibido e quaisquer violações deste princípio serão tratadas em conformidade com a política de disciplina e de conduta da escola.

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 Coordenador de Segurança Digital ou o Órgão de Gestão podem 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.

Cabe a cada indivíduo a responsabilidade pelos dispositivos electrónicos pessoais trazidos 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. Os telemóveis e outros equipamentos pessoais serão entregues aos pais ou encarregados de educação, em conformidade com as políticas da escola.

Se um aluno necessitar de contactar os pais, deverá informar um professor ou funcionário que realizará o contacto utilizando, preferencialmente, os meios oficiais da escola.

Os alunos devem proteger os seus números de telefone, dando-os a conhecer apenas a amigos e familiares de confiança. Os alunos são instruídos quanto à utilização segura e adequada de telemóveis e outros equipamentos pessoais e sensibilizados para os limites e consequências dos seus atos.

#### **4.7. Utilização de equipamentos pessoais pelos professores**

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.

Sempre que for necessário contactar alunos ou pais/encarregados de educação, devem usar o telefone oficial da escola.

Durante o período letivo, os telemóveis e outros equipamentos devem estar desligados ou em modo de "silêncio". Os referidos equipamentos não devem ser utilizados em períodos letivos exceto em situações de emergência autorizadas pelo Órgão de Gestão.

## **5. Os Media 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 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.

Todo o pessoal do agrupamento será incentivado a envolver-se em *media* sociais de uma maneira positiva, segura e responsável, em todos os momentos.

Todo o pessoal do agrupamento, 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.

O agrupamento 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.

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).

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 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.

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 só acontecerá com objetivos do trabalho educacional, 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 ouvido o Coordenador de Segurança Digital.

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 *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.

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.

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.

O(s) responsável(eis) 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 oficial direta com pais, encarregados de educação ou alunos através de qualquer canal de *media* social ou rede social.

Os membros do pessoal serão incentivados a gerenciar 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 de Segurança Digital 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 um pai e/ou responsável ou a permissão de outro adulto responsável e só quando eles podem estar presentes.

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.

Qualquer atividade de *media* social oficial envolvendo alunos no recinto escolar deverá ser sempre moderada pela escola.

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 sua 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, 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.

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 do *firewall* devem ser conhecidas e atualizadas de acordo com as ameaças de cyberssegurança.

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.

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

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.

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 pela escola 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 de Segurança Digital que, por sua vez, documentará o incidente e fá-lo-á chegar ao Órgão de Gestão, conforme adequado.

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

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.

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.

A escola irá tomar todas as precauções razoáveis para garantir que os usuários acessem 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.

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.

Os métodos para identificar, avaliar e minimizar os riscos online serão revistos regularmente pela Equipa de Segurança Digital da escola.

## **7. Reduzindo os riscos online**

### **7.1. Tecnologias emergentes**

O agrupamento 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 de Segurança Digital.

De acordo com o Regulamento Interno e a Política de Segurança Digital, os dispositivos móveis estão proibidos no recinto 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 aos alunos é fornecido acesso supervisionado à Internet que é apropriado para a sua idade e capacidades.

Os pais e encarregados de educação são convidados a ler a Política de Utilização Aceitável para o acesso dos alunos e discuti-lo com os seus filhos ou educandos, se for o caso.

Ao considerar o acesso para os membros vulneráveis da comunidade (como com as crianças com necessidades educativas especiais) a escola tomará as decisões com base nas necessidades específicas e compreensão do(s) aluno(s).

Todos os elementos da escola são responsáveis pela leitura da Política de Utilização Aceitável das TIC em vigor e aceitar as suas regras antes de utilizar quaisquer recursos informáticos da escola.

O acesso à rede de Internet da escola está vedado aos visitantes, exceto em caso de necessidade extrema e solicitada a devida autorização ao Órgão de Gestão ou ao 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 se comunicar situações preocupantes do ponto de vista da segurança digital (tais como violações do sistema de filtragem, "cyberbullying", conteúdos ilícitos, etc).

O Coordenador de Segurança Digital 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.

A escola gerirá os incidentes relacionados com a segurança digital em conformidade com as políticas da escola em matéria de disciplina/conduta.

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

Depois de concluídas eventuais investigações, a escola fará o ponto da situação, retirará ilações do ocorrido e, se necessário, tomará outras medidas.

Sempre que houver razões para crer ou recear que ocorreu ou está a ocorrer alguma atividade ilegal, a escola contactará a Equipa de Proteção de Menores, a Escola Segura ou outro responsável pelas questões de segurança digital.

#### 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 pela escola.

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

A escola 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.

Os professores e os alunos trabalharão em conjunto com a escola com vista à resolução dos problemas.

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

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

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

#### 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”.

O *cyberbullying* (assim como todas as outras formas de *bullying*) de qualquer elemento da escola não será tolerado.

De uma forma geral, os procedimentos formais adotados pela escola para dar apoio a qualquer elemento da comunidade escolar que seja alvo de *cyberbullying* serão os mesmos que o registo de ocorrências de incidentes preocupantes.

Todos os incidentes de *cyberbullying* comunicados à escola serão registados.

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

A escola 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 polícia, se necessário.

Será solicitado a alunos, professores e pais ou encarregados de educação que trabalhem em conjunto com a escola de modo a apoiarem a abordagem da escola em relação ao *cyberbullying* e à segurança digital.

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

- O autor poderá ter de retirar todo o material considerado inapropriado ou, caso se recuse ou não seja capaz de o fazer, poderá ser contactado o fornecedor do serviço para que elimine os conteúdos em questão.

- O autor poderá ver o seu direito de acesso à Internet na escola suspenso durante um determinado período de tempo. 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 polícia será contactada caso se suspeite de ação ilícita.

## 8. Disposições finais

O agrupamento 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.

Deverá ser incentivada uma abordagem de parceria para a segurança online em casa e na escola com os pais e encarregados de educação.

O agrupamento disponibiliza-se, através dos seus responsáveis, a disponibilizar informação e orientação para os pais e encarregados de educação sobre segurança online.

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

A escola chamará a atenção dos pais e encarregados de educação para a sua Política de Segurança Digital através de boletins informativos, do prospeto da escola ou do seu sítio na Internet.

Será incentivada uma abordagem de parceria pais/escola em relação à segurança digital em casa e na escola. Para esse efeito, poderão ser organizadas sessões para os pais com demonstrações e sugestões para uma utilização segura da Internet em casa ou ser aproveitados outros eventos em que os pais participam para abordar a segurança digital.

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

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

A escola deve ter uma Política de Utilização Aceitável consubstanciada num documento claro e conciso, que indique claramente a alunos, professores e todos aqueles que utilizam as novas tecnologias dentro da escola o que podem e o que não podem fazer na Internet ou aquando da utilização de equipamentos tecnológicos.

Todos os membros da escola deverão estar informados sobre o processo de comunicação das preocupações de segurança online (eSafety), tais como violações de filtragem, *sexting*, *cyberbullying*, conteúdo ilegal, etc.

A Equipa de Segurança Digital deverá ser informada de qualquer incidente de segurança online envolvendo preocupações de proteção da criança.

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

Todos os elementos do agrupamento devem estar sensibilizados para o facto de que a sua conduta na 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.

A escola deverá informar os pais ou encarregados de educação de quaisquer incidentes ou preocupações relativas aos alunos, como e quando necessário.

Depois de identificados os possíveis incidentes, a escola deve implementar as alterações, conforme necessário.

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

Serão disponibilizadas informações aos alunos e pais ou 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 da escola.

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/>).

## **9. Bibliografia/Webgrafia**

- Perfil dos alunos para o século XXI
- Resolução do Conselho de Ministro nº 41/2018
- European Schoolnet ([www.eun.org](http://www.eun.org))
- EB1/PE da Marinheira (Licença Creative Commons Attribution-ShareAlike 3.0)



# Política de Utilização Aceitável

## das TIC (alunos)

Ao ler esta Política de Utilização Aceitável (PUA) declaro que:

- Compreendo que estas regras se aplicam quando utilizo a rede de Internet ou qualquer equipamento da escola, seja no seu interior ou exterior.
- Qualquer equipamento, dispositivo ou ferramenta relacionados com as Tecnologias de Informação e Comunicação, incluindo a Internet, apenas pode ser utilizado para fins escolares e quando autorizados pelo professor responsável.
- Estou proibido de realizar downloads ou instalar software em equipamento da escola, exceto com autorização expressa do professor responsável.
- Não irei revelar as minhas senhas a ninguém, exceto aos meus encarregados de educação ou a alguém responsável por mim.
- Ao utilizar as TIC, irei comunicar com alunos, professores ou outras pessoas de modo responsável, respeitoso e sensato, sendo responsável pela correção do meu comportamento ao utilizar a Internet, incluindo os sites a que acedo e a linguagem que utilizo.
- De acordo com o Regulamento Interno estou proibido de trazer para a escola telemóvel ou outro dispositivo móvel.
- Não vou deliberadamente navegar, fazer download, upload ou partilhar material que possa ser considerado ofensivo ou ilegal. Ao me deparar com esse tipo de material irei comunicar o facto imediatamente ao professor responsável.
- Irei respeitar os direitos de autor e a propriedade intelectual do trabalho de outros.
- Não darei nenhuma informação pessoal, como nome, número de telefone ou endereço, nem vou marcar encontros com alguém conforme consta da Política de Segurança Digital.
- Vou garantir que a minha atividade online, tanto na escola como fora desta, não desrespeite ou ofenda de algum modo a minha escola, funcionários, alunos, professores ou outros.
- Estou proibido e serei penalizado se publicar fotos não autorizadas de colegas, funcionários, professores ou outros membros da escola.
- Caso seja vítima de *cyberbullying* ou tenha conhecimento que alguém que o seja é meu dever e obrigação informar um professor, funcionário ou o órgão de gestão.
- Utilizarei a Internet respeitando os filtros existentes e as regras gerais definidas, sabendo que a minha utilização será monitorizada pelo responsável pela rede.
- Entendo que estas regras foram criadas para minha segurança e que se as não cumprir serei responsabilizado e penalizado de acordo com a gravidade das minhas ações, além de ser dado conhecimento ao meu encarregado de educação.
- Entendo que estas são as regras gerais a adotar na escola, mas que cada espaço pode ter regras específicas pelo que devo consultar o regulamento de utilização de cada sala.
- Em caso de dúvidas sobre assuntos relacionados com a segurança na internet e a utilização responsável e segura dos equipamentos, irei procurar informação ou ajuda junto dos professores, através da Política de Segurança Digital ou em sites adequados como, por exemplo:  
<http://www.internetsegura.pt/> <http://seguranet.pt/> <http://www.esafetylabel.eu/>





# Política de Utilização Aceitável

## das TIC (pessoal docente)

É importante que todos os professores adotem, dentro do possível, todas as medidas necessárias para proteger os sistemas de dados e de informação contra acesso não autorizado, danos, perdas, abusos e roubo.

Ao ler esta Política de Utilização Aceitável (PUA) declaro que:

- Compreendo que os Sistemas de Informação e as TIC incluem as redes, os dados e o seu armazenamento, as tecnologias de comunicação digital online e offline e os dispositivos de acesso. Como exemplos temos os telemóveis, os PDA, as câmaras digitais, o correio eletrónico (email) e os sites de redes sociais.
- Os sistemas de informação da escola devem ser utilizados de forma adequada. Tenho conhecimento de que, ao abrigo da lei portuguesa e das diretivas europeias os seguintes atos constituem uma infração punível por lei: obter acesso não autorizado a material informático com o intuito de cometer ou facilitar outros atos ilícitos ou de alterar material informático sem autorização.
- Aceito que todos os equipamentos e programas informáticos disponibilizados pela escola só podem ser utilizados para fins relacionados com a escola e para uso educacional. Para impedir o acesso não autorizado a sistemas ou dados pessoais, esforçar-me-ei por não deixar qualquer sistema de informação com dados dos alunos ou de terceiros sem vigilância.
- A fim de evitar o acesso não autorizado a sistemas ou a dados pessoais dos alunos ou de terceiros, esforçar-me-ei por não deixar qualquer sistema informático ligado sem que seja necessário iniciar sessão com palavra-passe ou sem encerrar a minha sessão, consoante o caso.
- Comprometo-me a respeitar o sistema de segurança e a não divulgar qualquer palavra-passe ou informação de segurança.
- Comprometo-me a não tentar instalar qualquer software adquirido ou descarregado, sem permissão do responsável pelo sistema ou da direção da escola.
- Comprometo-me a assegurar que os dados pessoais de alunos, professores, funcionários ou pais/encarregados de educação são tratados de acordo com a legislação nacional, no que diz respeito à proteção de dados pessoais. Isto significa que todos os dados pessoais são obtidos e processados de forma adequada e de acordo com a lei, apenas são mantidos para os fins a que se destinam, não são guardados por mais tempo do que o necessário e é assegurada a sua privacidade e segurança por meio de medidas de proteção adequadas, quer sejam utilizadas nas instalações físicas da escola quer estejam alojados online ou sejam acedidos à distância. As fotografias ou os vídeos de alunos são utilizados exclusivamente para fins educativos ou de divulgação das atividades da escola e estão sempre sujeitas a autorização dos encarregados de educação de acordo com a Política de Utilização de Imagem.
- Comprometo-me a não guardar documentos profissionais que contenham informações pessoais ou sensíveis relacionadas com a escola em dispositivos pessoais (como computadores portáteis, tablets, telemóveis), salvo se estiverem protegidos por palavra-passe ou encriptados.
- Comprometo-me a não guardar no sistema informático da escola informações pessoais não relacionadas com as atividades escolares, tais como fotografias, ficheiros ou dados financeiros pessoais.
- Comprometo-me a respeitar os direitos de autor e propriedade intelectual.

Compreendo que em matéria de segurança digital quando trabalho com alunos devo promover a utilização segura das redes, a supervisão dos alunos na sala de aula e em outros espaços da escola, fazendo cumprir o disposto na Política de Segurança Digital da escola e na Política de Utilização Aceitável para os alunos.

Comprometo-me a reportar qualquer incidente preocupante relativo à segurança dos alunos na Internet ao coordenador de segurança digital ou ao órgão de gestão, assim que possível. Qualquer acesso accidental, receção de materiais inadequados, violações de filtros ou sítios web inadequados deverá ser reportado ao coordenador de segurança digital ou ao órgão de gestão da escola, assim que possível.

As minhas comunicações eletrónicas com os alunos e pais ou encarregados de educação serão realizadas exclusivamente através de canais de comunicação aprovados.

A minha utilização das TIC e dos sistemas de informação será sempre consonante com as minhas funções profissionais, quer use sistemas pessoais quer da escola. Isto inclui a utilização de emails, mensagens de texto, redes sociais, jogos, publicações digitais e outros dispositivos ou sítios web. A minha utilização das TIC não interferirá com os meus deveres profissionais e estará em consonância com as Políticas de Utilização Aceitável, com a Política de Segurança Digital da escola e com a lei.

Comprometo-me a não criar, transmitir, apresentar, publicar ou encaminhar qualquer material suscetível de assediar e ofender alunos, encarregados de educação, funcionários, ou que possa trazer descrédito para a escola.

Estas políticas aplicam-se igualmente na utilização de equipamento pessoal na rede da escola.

Se tiver dúvidas ou perguntas relacionadas com práticas seguras e profissionais na Internet, responsabilizo-me por procurar ou solicitar esclarecimento.

Comprometo-me a cumprir com rigor o disposto na Política de Segurança Digital da escola.

## Política de Utilização Aceitável

### das TIC (pessoal docente)

Declaro que li, compreendi e aceito cumprir a Política de Utilização Aceitável das TIC destinadas ao pessoal docente do agrupamento.

Nome	Assinatura	Data



# Política de Utilização Aceitável

## das TIC (pessoal não docente e visitantes)

É importante que todos os membros da escola adotem, dentro do possível, todas as medidas necessárias para proteger os sistemas de dados e de informação contra acesso não autorizado, danos, perdas, abusos e roubo.

Ao ler esta Política de Utilização Aceitável (PUA) declaro que:

- Compreendo que os Sistemas de Informação e as TIC incluem as redes, os dados e o seu armazenamento, as tecnologias de comunicação digital online e offline e os dispositivos de acesso. Como exemplos temos os telemóveis, os PDA, as câmaras digitais, o correio eletrónico (email) e os sites de redes sociais.
- Os sistemas de informação da escola devem ser utilizados de forma adequada. Tenho conhecimento de que, ao abrigo da lei portuguesa e das diretivas europeias os seguintes atos constituem uma infração punível por lei: obter acesso não autorizado a material informático com o intuito de cometer ou facilitar outros atos ilícitos ou de alterar material informático sem autorização.
- Aceito que apenas posso aceder à rede sem fios da escola e nos meus momentos de pausa conforme definido na Política de Segurança Digital da Escola.
- Comprometo-me a respeitar o sistema de segurança e a não divulgar qualquer palavra-passe ou informação de segurança.
- Comprometo-me a não tentar instalar qualquer software adquirido ou descarregado, sem permissão do responsável pelo sistema ou da direção da escola.
- Comprometo-me a assegurar que os dados pessoais de alunos, professores, colegas ou pais/encarregados de educação são tratados de acordo com a legislação nacional, no que diz respeito à proteção de dados pessoais.
- Comprometo-me a não guardar documentos profissionais que contenham informações pessoais ou sensíveis relacionadas com a escola em dispositivos pessoais (como computadores portáteis, tablets, telemóveis), salvo se estiverem protegidos por palavra-passe ou encriptados.
- Comprometo-me a respeitar os direitos de autor e propriedade intelectual.
- Comprometo-me a reportar qualquer incidente preocupante relativo à segurança na Internet ao coordenador de segurança digital ou ao órgão de gestão, assim que possível.
- A minha utilização das TIC não interferirá com os meus deveres profissionais e estará em consonância com as Políticas de Utilização Aceitável, com a Política de Segurança Digital da escola e com a lei.
- Comprometo-me a não criar, transmitir, apresentar, publicar ou encaminhar qualquer material suscetível de assediar e ofender colegas, alunos, encarregados de educação, professores, ou que possa trazer descrédito para a escola.
- Estas políticas aplicam-se igualmente na utilização de equipamento pessoal na rede da escola.
- Se tiver dúvidas ou perguntas relacionadas com práticas seguras e profissionais na Internet, responsabilizo-me por procurar ou solicitar esclarecimento.
- Comprometo-me a cumprir com rigor o disposto na Política de Segurança Digital da escola.

