

# Política de Segurança Digital



Usar a internet e os dispositivos digitais em segurança e como recurso educativo.

*“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)*



# Índice

<b>1. Introdução e Enquadramento</b>	<b>3</b>
<b>2. Ensino e Aprendizagem</b>	
2.1 – A importância da utilização da Internet	4
<b>3. Gestão de Sistemas de Informação</b>	
3.1 – Manutenção da segurança dos sistemas de informação	4
3.2 – A gestão do correio eletrónico	5
3.3 – Gestão dos conteúdos publicados	5
3.4 – Gestão dos conteúdos publicados	5
3.5 – Gestão de comunidades sociais virtuais, redes sociais e publicações pessoais	6
3.6 – Gestão dos sistemas de filtragem	6
<b>4. Decisões quanto às políticas</b>	
4.1 – Autorização do acesso à Internet	7
4.2 – Resolução de incidentes relativos à Segurança Digital	7
4.3 – Gestão dos casos de <i>cyberbullying</i>	7
4.4 – Gestão de telemóveis e equipamentos pessoais	8
<b>5. Conhecimento das políticas</b>	
5.1– Conhecimento das políticas pelo pessoal docente, não docente e pais e encarregados de educação	9

## 1. Introdução e Enquadramento

A segurança digital visa proteger a confidencialidade, integridade e disponibilidade de autenticidade de documentos e dados pessoais. Atualmente, crianças, jovens e adultos interagem diariamente com as mais diversas tecnologias (os telemóveis, as consolas de jogos, a Internet, etc...) e contactam, experimentam e vivenciam uma infindável variedade de oportunidades, atitudes e situações. A troca de ideias, opiniões, experiências, a interação social online e as oportunidades de aprendizagem daí decorrentes apresentam enormes benefícios para todos, mas podem, por vezes, colocar crianças, jovens e adultos em perigo.

A segurança digital abrange questões relacionadas não só com crianças e jovens, mas também com adultos e com a utilização que todos fazem da Internet e de todos os dispositivos que permitem a comunicação eletrónica em ambiente escolar e fora dele. Isto exige a atenção e formação de todos os elementos da comunidade escolar sobre os riscos e responsabilidades envolvidas e faz parte do cuidado inerente à função de cada educador.

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

A política de segurança digital é, por isso mesmo, essencial na definição de princípios nucleares de ação, que todos os elementos da comunidade escolar devem aplicar.

O Coordenador da Política de Segurança Digital é um Adjunto da Direção e funciona como elemento de articulação com a Equipa de Desenvolvimento Digital (EDD).

A política de Segurança Digital, redigida com base na Política do Selo de Segurança Digital e na legislação aplicável, será revista anualmente.

Política Aprovada pelo Conselho Pedagógico de \_\_\_\_\_.

## **2. Ensino e Aprendizagem**

### **2.1 – A importância da utilização da Internet**

- Devendo fazer parte integrante do currículo como uma ferramenta essencial na aprendizagem, a utilização da Internet no Agrupamento deve elevar os padrões educativos, promover o sucesso dos alunos, apoiar o trabalho dos professores e reforçar a administração escolar.
- O acesso à Internet é um direito dos alunos que demonstrem responsabilidade e maturidade na sua utilização.
- Nas atividades de ensino e aprendizagem dever-se-á ensinar aos alunos o que é e o que não é uma utilização aceitável da Internet, e ser-lhes-ão indicados objetivos claros, quando utilizam a Internet, tendo em conta o currículo e a idade.
- A cópia, e a utilização subsequente de materiais obtidos na Internet, por alunos e professores, devem cumprir a legislação em matéria de direitos de autor, incluindo o conhecimento dos vários tipos de licenciamentos disponíveis na Web e as regras de utilização dos recursos educativos abertos.
- Os níveis de acesso à Internet serão estabelecidos de acordo com os requisitos do currículo e a idade e capacidades dos alunos.
- Todas as atividades escolares que impliquem o uso da Internet devem permitir aos alunos aprender a pesquisar e a avaliar / validar informação, de acordo com a sua autoria, pertinência e rigor.
- Todas as atividades escolares que impliquem o uso da Internet devem integrar a apresentação das referências bibliográficas.

## **3. Gestão de Sistemas de Informação**

### **3.1 – Manutenção da segurança dos sistemas de informação**

- A segurança dos sistemas informáticos do Agrupamento e dos utilizadores será revista anualmente.
- A proteção antivírus será atualizada frequentemente.
- Os dados pessoais enviados através da Internet ou transferidos para fora da escola estão protegidos pelos sistemas de segurança dos programas utilizados, tendo em conta as recomendações da Comissão Nacional de Proteção de Dados na Deliberação n.º 1495/2016 relativas as restrições de acesso a esses sistemas e à robustez das palavras-chave.
- Os dispositivos amovíveis serão utilizados de acordo com as autorizações específicas de cada serviço, estando os sistemas preparados para uma análise automática com antivírus.
- A instalação de software para fins educativos nos PC de mesa e portáteis deve ser autorizada pelo Coordenador da Segurança Digital e feita, preferencialmente, por um membro da equipa EDD, ou pelo membro da empresa de serviços de assistência técnica de informática. Os utilizadores não

devem colocar / deixar ficheiros de uso pessoal ou dos alunos nos PC ou nos dispositivos móveis. Após a utilização, nomeadamente para atividades letivas, todos os ficheiros devem ser removidos. Nos dispositivos móveis, os utilizadores também devem ter o cuidado de remover todas as contas pessoais associadas a aplicações.

- A capacidade e o funcionamento dos sistemas informáticos serão analisados, pelo menos, uma vez por ano letivo.
- É obrigatória a utilização de nomes de utilizador e palavras-passe para aceder à rede da escola.
- A página inicial de navegação de cada PC ao serviço dos utilizadores será definida pela direção, de acordo com as necessidades / interesses dos serviços. Os utilizadores não devem, em circunstância alguma, alterar as páginas de navegação pré-definidas.

### **3.2 – A gestão do correio eletrónico**

- A comunicação com alunos, pais / encarregados de educação e com instituições para tratamento de assuntos oficiais do Agrupamento deve ser realizada a partir de endereços eletrónicos institucionais.
- As mensagens de correio eletrónico enviadas para organizações externas devem obedecer a procedimentos de escrita e de protocolo similares aos do envio de ofícios por correio físico.
- O reencaminhamento de mensagens em cadeia deve ser evitado e a difusão de informação em grupo deve ser cuidadosa, de modo a evitar ser objeto de spam.

### **3.3 – Gestão dos conteúdos publicados**

- As informações de contacto na página Web do agrupamento devem ser a morada, os números de telefone e o email do agrupamento. Não deve ser publicada qualquer informação pessoal de alunos ou professores.
- A publicitação online de horários das turmas e a listagem dos alunos das turmas só será efetuada se os sistemas garantirem um acesso restrito a alunos e a pais e encarregados de educação, com palavras-passe robustas. Não serão publicadas pautas online e as pautas afixadas em papel nos locais de estilo seguirão as recomendações da Comissão Nacional sobre Proteção de Dados relativas a faltas e outros dados de natureza pessoal.
- O Diretor é o responsável editorial geral pelos conteúdos digitais publicados pelo Agrupamento na Internet e deve assegurar que os conteúdos publicados são corretos e adequados.
- Todas as publicações em formato digital da responsabilidade de membros do Agrupamento devem respeitar os direitos de propriedade intelectual, as políticas de privacidade e os direitos de autor.

### **3.4 – Gestão dos conteúdos publicados**

- Antes da publicação de imagens ou de gravações vídeo que incluam alunos, deve ser garantida a autorização expressa e informada, de acordo com a legislação aplicável.

- A publicação em linha, em rede aberta ou circuito fechado, de imagens dos alunos ou de gravações contendo a sua voz devem garantir não haver uma relação direta entre a imagem e o som e o nome dos alunos, reduzindo, assim, significativamente, a possibilidade de identificação dos alunos.
- A captação de imagens dos alunos deve, preferencialmente, ser executada de longe ou de ângulos que reduzam significativamente a possibilidade de identificação.
- Os professores e pessoal não docente não podem publicar diretamente imagens ou outros registos dos alunos nas suas redes sociais pessoais.
- O consentimento por escrito será mantido pela escola, sempre que as imagens de alunos forem utilizadas para fins de publicidade, até as imagens em causa deixarem de ser usadas.
- Os trabalhos de alunos só serão publicados com a autorização dos mesmos ou dos pais / encarregados de educação das crianças.

### **3.5 – Gestão de comunidades sociais virtuais, redes sociais e publicações pessoais**

- Através de atividades dinamizadas pelos professores em sala de aula e pelo Serviço das Bibliotecas Escolares, os alunos serão ensinados a usar a Internet e as redes sociais, de modo a protegerem a sua privacidade, a evitarem a divulgação de dados pessoais, a negarem o acesso a desconhecidos e a bloquearem comunicações não desejadas
- Os professores que pretendam utilizar ferramentas das redes sociais com os alunos em atividades curriculares devem avaliar o risco dos sítios na Internet, antes de os utilizarem e verificar os termos e condições dos mesmos, de modo a garantir que são adequados às idades dos alunos.
- Os blogues ou wikis oficiais geridos pelos professores devem estar protegidos por palavra-passe.
- Através da página Web do Agrupamento, são disponibilizados aos pais / encarregados de educação materiais relacionadas com a utilização de redes sociais, meios sociais e sítios de publicação pessoal (dentro ou fora da escola), especialmente para os alunos mais novos. Ações de sensibilização para o uso seguro da Internet podem vir a ser organizadas em colaboração com as Associações de Pais e Encarregados de Educação do Agrupamento.

### **3.6 – Gestão dos sistemas de filtragem**

- O acesso à Internet fornecido pelo Agrupamento incluirá sistemas de filtragem adequados à idade e à maturidade dos alunos.
- Todos os membros da comunidade escolar que violarem os sistemas de filtragem ou acederem a sítios com conteúdos inadequados ao espaço escolar serão alvo de procedimento disciplinar, de acordo com o RI.
- Serão feitas verificações regulares, para comprovar a eficácia dos métodos de filtragem adotados.

## **4. Decisões quanto às políticas**

### **4.1 – Autorização do acesso à Internet**

- O Agrupamento manterá um registo atualizado de todos os alunos e professores que são autorizados a aceder às comunicações eletrónicas da escola.
- Todos os elementos da comunidade educativa terão conhecimento da *Política de Segurança Digital* e dos recursos para a utilização segura da *Internet*, disponíveis no sítio *Web* do Agrupamento e serão incentivados a analisá-los com os seus educados.

### **4.2 – Resolução de incidentes relativos à Segurança Digital**

- Todos os elementos do Agrupamento deverão informar o Coordenador da Segurança Digital se tiverem conhecimento de situações preocupantes, do ponto de vista da segurança digital (tais como violações do sistema de filtragem, *cyberbullying*, conteúdos ilícitos, utilização inadequada de equipamento, etc).
- As queixas relativas à utilização indevida da Internet serão tratadas no quadro dos procedimentos de apresentação de queixas ou denúncias adotadas pela escola.
- A aplicação de medidas para superação de problemas relativos à Segurança Digital, incluindo os que possam implicar a aplicação de medidas disciplinares, deve ser articulada com os responsáveis pelos serviços onde ocorreram os problemas.
- Alterações no acesso e nos Serviços, decorrentes da aplicação de medidas no âmbito da Segurança Digital, devem ser comunicadas a alunos, docentes e pessoal não docente, ainda que com a devida proteção de confidencialidade das pessoas envolvidas.
- Sempre que houver razões para crer ou recear que ocorreu ou está a ocorrer alguma atividade ilegal, o Agrupamento contactará a Equipa de Proteção de Menores, através da Direção, e encaminhará a situação para a Polícia.

### **4.3 – Gestão dos casos de *cyberbullying***

- O *cyberbullying* não será tolerado e todos os incidentes detetados serão comunicados à Direção, ao Coordenador da Segurança Digital e às autoridades competentes, quando necessário.
- Alunos, professores e pais/encarregados de educação serão aconselhados a manter um registo do bullying como prova.
- Todos os incidentes de *cyberbullying* comunicados serão registados e serão investigados, aplicando-se, quando necessário, os procedimentos de inquirição usados nos processos disciplinares, tal como estabelecido no Regulamento Interno.
- As sanções para os envolvidos em *cyberbullying* podem incluir:

- eliminação de todo o material considerado inapropriado pelo(a) autor(a) dos atos ou, caso se recuse ou não seja capaz de o fazer, eliminação realizada pelo fornecedor do serviço para que apague os conteúdos em questão;
  - o(a) autor(a) poderá ver o seu direito de acesso à *Internet* na escola suspenso durante um período de tempo a determinar pela direção
  - os pais / encarregados de educação serão informados da sanção aplicada; o a Polícia será contactada, caso se suspeite de ação ilícita.
- 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.

#### **4.4– Gestão de telemóveis e equipamentos pessoais**

- Os telemóveis ou equipamentos pessoais não podem ser utilizados durante as aulas ou tempos letivos formais, a não ser para efeitos pedagógicos devidamente autorizados, orientados e supervisionados pelo professor.
- Os utilizadores são responsáveis por qualquer tipo de dispositivos eletrónicos que tragam para a escola. A escola não assume qualquer responsabilidade pela perda, roubo ou dano de tais objetos, nem por quaisquer efeitos prejudiciais para a saúde causados por estes dispositivos, sejam eles reais ou potenciais.
- Não é autorizado o uso de telemóveis e equipamentos pessoais em determinadas áreas dentro da escola, como vestiários ou casas de banho.
- Os professores podem confiscar um telemóvel ou equipamento. O Coordenador de Segurança Digital pode fazer uma pesquisa ao telemóvel ou equipamento, com o consentimento do aluno ou dos pais / encarregados de educação. Caso se suspeite que o equipamento pessoal contém materiais que podem constituir prova de uma ação ilícita, o telemóvel será entregue à Polícia para averiguações.
- No caso de apreensão, os telemóveis e outros equipamentos pessoais serão entregues aos pais / encarregados de educação.
- Não é permitido levar telemóveis e outros equipamentos para os exames. Os alunos que tenham um telemóvel na sua posse durante um exame estarão sujeitos às normas estabelecidas pelo Júri Nacional de Exames.
- Se um(a) aluno(a) necessitar de contactar os pais ou encarregado de educação, deve usar, preferencialmente, o telefone da escola ou contactar os pais ou encarregado de educação através do



seu telemóvel, em período não letivo e fora de espaços como salas de aula, biblioteca, zonas comuns dos blocos e outros espaços onde possa perturbar o funcionamento dos serviços.

- Os pais e encarregados de educação não devem contactar os filhos para os telemóveis durante o horário letivo. Em caso de necessidade de contacto urgente devem usar o número de telefone da Escola.
- Os professores e educadores não devem preferencialmente utilizar os seus telemóveis ou equipamentos pessoais para contactar crianças, jovens ou seus familiares dentro ou fora da escola na sua qualidade de profissionais, a não ser em situações de emergência e quando outros meios de contacto não estejam operacionais.
- Se um docente ou não docente violar as políticas da escola, podem ser tomadas medidas disciplinares.

## **5. Conhecimento das políticas**

### **5.1– Conhecimento das políticas pelo pessoal docente, não docente e pais e encarregados de educação**

- A *Política de Segurança Digital* está disponível, para conhecimento e consulta, no sítio *Web* do Agrupamento.
- O Agrupamento ministrará, a todos os elementos da escola, formação atualizada e adequada sobre a utilização segura e responsável da *Internet*, tanto ao nível profissional como pessoal.
- No sítio *Web* do Agrupamento são disponibilizados recursos de apoio para uma utilização segura e responsável da *Internet* e de equipamentos informáticos.