



POLÍTICAS DE SEGURANÇA DÍGITAL DO AGRUPAMENTO E SAFETY

Índice

1. Política de Segurança Digital (eSafety)	2
2. Principais Responsabilidades.....	3
2.1 Pessoal Docente, Pessoal Não Docente, Alunos, Pais/Encarregados de educação.....	3
3. Ensino e aprendizagem	5
3.1 Importância da Internet	5
3.2 Benefícios da utilização da Internet no ensino	5
3.3 Formas da Internet melhorar a aprendizagem	6
3.4 Avaliação de conteúdos digitais	6
4. Comunicação online e Utilização Segura da Tecnologia	7
4.1 Gestão dos conteúdos publicados.....	7
4.2 Publicação de imagens, vídeos, atividades ou trabalhos dos alunos online.....	7
4.3 Gestão do correio eletrónico.....	8
4.4 Telemóveis e equipamentos pessoais	8
4.5 Utilização de equipamentos pessoais pelos professores.....	9
5. Os Media Sociais	9
5.1 Gestão redes sociais e publicações pessoais.....	9
6. Gestão de sistemas	10
6.1 Segurança dos sistemas de informação	10
6.2 Gestão dos sistemas de filtragem	10
7. Reduzindo os riscos online	11
7.1 Tecnologias emergentes	11
7.2 Autorização e utilização da Internet.....	11
7.3 Incidentes preocupantes	12
7.4 Denúncias relacionadas com a segurança digital	12
7.5 Cyberbullying.....	13
8. Conhecimento das políticas	14
8.1 Conhecimento das políticas pelo pessoal docente, não docente e pais e encarregados de educação.....	14

1. Política de Segurança Digital (eSafety)

Crianças, jovens e adultos interagem cada vez mais com tecnologias digitais, vivenciando uma grande variedade de oportunidades, atitudes e situações. A troca de ideias, a interação social e as oportunidades de aprendizagem daí decorrentes apresentam benefícios significativos para todos, mas podem por vezes colocar crianças, jovens e adultos em perigo.

Neste sentido, 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 e de todos os dispositivos que permitem a comunicação electrónica, em ambiente escolar e fora dele. Isto exige a 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 fundamentais de ação, que todos os elementos da comunidade escolar devem aplicar.

Os objetivos da **Política de Segurança Digital do Agrupamento de Escolas da Madalena (AEM)** são:

- estabelecer os princípios fundamentais, seguros e responsáveis em relação à utilização de equipamentos e da Internet como forma de garantir que o AEM seja um ambiente digital seguro.
- consciencializar todos os membros do AEM sobre os potenciais riscos, bem como dos benefícios da tecnologia.
- permitir que todos possam trabalhar com segurança e responsabilidade, com vista a um comportamento online digital seguro.
- identificar procedimentos claros a adotar de forma a responder aos incidentes de segurança digital online.

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 e a pessoal docente e não docente.

Este documento é complementado por outras políticas, relativas à conduta e segurança digital e proteção de dados.

O Coordenador da Política de Segurança Digital é um adjunto da direção.

A política de Segurança Digital, redigida com base na Política do Selo de Segurança Digital (eSafety) e na legislação aplicável, será revista anualmente. Política aprovada pelo diretor cinco de dezembro de 2022.

2. Principais Responsabilidades

2.1 Pessoal Docente, Pessoal Não Docente, Alunos, Pais/Encarregados de educação

As principais responsabilidades para todos os membros do AEM são:

- Tomar conhecimento das Políticas de Utilização Aceitável (PUAs), aceitando-as, cumprindo-as e fazendo-as cumprir.
- Contribuir para o desenvolvimento da Política de Segurança Digital.
- Assumir responsabilidade individual pela segurança dos dispositivos tecnológicos do agrupamento.
- Ter conhecimento das diferentes questões relacionadas com a segurança digital e como elas podem afetar os alunos.
- Apresentar boas práticas no uso das tecnologias.
- Incluir a educação para a segurança digital no currículo, sempre que possível.
- Identificar incidentes e tomar medidas apropriadas, seguindo as políticas e procedimentos de segurança do Agrupamento.
- Assegurar um comportamento profissional no uso pessoal de dispositivos tecnológicos, dentro e fora do local de trabalho.

As principais responsabilidades dos alunos, adequadas à sua idade, capacidades e fragilidades, são:

- Colaborar de forma positiva para o desenvolvimento das políticas de segurança digital.
- Tomar conhecimento das Políticas de Utilização Aceitável (PUAs) e respeitá-las.
- Respeitar os outros, tanto online como offline.
- Procurar a ajuda de um adulto de confiança, caso seja vítima de cyberbullying (ou tenha conhecimento que algum colega é vítima) e apoiar outros que podem estar na mesma situação.
- Assumir a responsabilidade por manter-se a si e aos outros, em segurança digital.
- Avaliar os riscos pessoais do uso de qualquer tecnologia e adotar um comportamento seguro e responsável para limitar esses riscos, através da sua própria consciência e aprendizagem.

As principais responsabilidades dos pais e encarregados de educação são:

- Tomar conhecimento das Políticas de Utilização Aceitável (PUAs) do Agrupamento, incentivando os seus educandos, a cumpri-las.
- Analisar as questões de segurança digital com os educandos, colaborando com a escola nas suas iniciativas sobre o tema, intensificando comportamentos digitalmente seguros e adequados em casa.
- Ser um exemplo positivo no uso ponderado da tecnologia e na adoção de comportamentos seguros digitalmente.
- Identificar alterações no comportamento dos seus educandos, que possam indicar que estão em risco.
- Procurar ajuda e apoio do Agrupamento, ou de outras instituições competentes, se os seus educandos detetarem situações problemáticas e potencialmente perigosas.
- Ter conhecimento das diferentes questões relacionadas com a segurança digital e como elas podem afetar os educandos.

3. Ensino e aprendizagem

3.1 Importância da Internet

A utilização da Internet fará parte integrante do currículo 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 podem proteger.

A finalidade da utilização da Internet nas escolas 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 museus e galerias de arte.
- Intercâmbio cultural e educativo entre alunos de vários países.
- 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 software.
- Possibilidade de aprendizagem quando e onde for mais conveniente.

3.3 Formas da Internet melhorar a aprendizagem

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

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

O Agrupamento 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 professores atribuirão aos alunos atividades com recurso à Internet que estejam de acordo com os objetivos de aprendizagem e com a sua idade e perfil.

Os alunos aprenderão a utilizar eficazmente a Internet para fins de pesquisa, designadamente desenvolver competências de procura, obtenção e avaliação de informação.

Os alunos devem aprender como indicar as fontes da informação 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 e perfil.

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

4. Comunicação online e Utilização Segura da Tecnologia

4.1 Gestão dos conteúdos publicados

As informações de contacto na Página do Agrupamento devem ser a morada, o número de telefone e o e-mail da escola. Não deve ser publicada qualquer informação pessoal de alunos, pessoal docente e não docente.

O Diretor é o responsável editorial geral pelos conteúdos digitais publicados pela comunidade escolar e deve assegurar que os conteúdos publicados são corretos e adequados.

O Portal do Agrupamento deve cumprir as diretrizes vigentes em matéria de publicações, designadamente, respeitar os direitos de propriedade intelectual, as políticas de privacidade e os direitos de autor.

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

No início de cada ano letivo, será obtida autorização por escrito dos pais ou encarregados de educação para publicação de qualquer imagem/vídeo de alunos.

As imagens ou gravações vídeo que incluem alunos serão selecionadas cuidadosamente e não serão inseridas em materiais reutilizados.

Os nomes completos dos alunos não serão utilizados em parte alguma do site do Agrupamento, em especial junto a fotografias.

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 as leis sobre segurança e proteção de dados, Políticas de Utilização Aceitável e códigos de conduta.

4.3 Gestão do correio eletrónico

Os alunos apenas podem utilizar contas de e-mail institucional para assuntos relacionados com a escola.

Os alunos têm de informar imediatamente os professores caso recebam mensagens de e-mail ofensivas.

Os alunos não podem revelar dados pessoais sobre eles próprios ou outros, nem estabelecer contactos não autorizados e monitorizados.

No caso do 1.º ciclo do Ensino Básico, devem ser principalmente utilizados endereços eletrónicos de grupo (um endereço por turma, por exemplo) para fins de comunicação com o exterior.

Os elementos do Agrupamento devem utilizar os endereços fornecidos pelo Agrupamento apenas para comunicar com alunos e pais/encarregados de educação.

As mensagens de e-mail enviadas para organizações externas devem ser escritas cuidadosamente antes de serem enviadas.

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

4.4 Telemóveis e equipamentos pessoais

A utilização de equipamentos pessoais (computadores portáteis, telemóveis, tablets...) pelos elementos da Comunidade Educativa dentro do agrupamento enquadra-se no disposto no Regulamento Interno.

O envio de mensagens ou conteúdos abusivos ou inadequados através de telemóveis ou equipamentos pessoais por parte de qualquer elemento do Agrupamento é proibido e quaisquer violações deste princípio serão tratadas em conformidade com a política de disciplina e de conduta do Agrupamento.

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*. O Coordenador de Segurança Digital ou Orgão de Gestão podem fazer uma pesquisa ao telemóvel ou equipamento com o consentimento do aluno (se maior de idade) ou dos pais/encarregados de educação. Caso se suspeite que o equipamento pessoal contém materiais que podem constituir prova de uma ação ilícita, será entregue à polícia para averiguações.

Os professores e restante pessoal são responsáveis pelos dispositivos eletrónicos de todos os tipos que tragam para do Agrupamento. A escola não assume qualquer responsabilidade pela perda, roubo ou dano de tais objetos.

4.5 Utilização de equipamentos pessoais pelos professores

Sempre que for necessário contactar alunos ou pais/encarregados de educação, deverão usar um telefone da escola.

Os telemóveis e outros equipamentos deverão estar desligados ou em modo de "silêncio".

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 a política de Segurança Digital.

5. Os Media Sociais

5.1 Gestão redes sociais e publicações pessoais

O uso oficial das redes sociais pela escola só acontecerá com objetivos do trabalho educacional, divulgação ou comunicação destinada, por exemplo, a aumentar o envolvimento dos pais e encarregados de educação.

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.

Os alunos serão aconselhados a nunca fornecerem quaisquer dados de carácter pessoal que permitam identificá-los e/ou ao local onde se encontram, por exemplo, o seu nome verdadeiro, a morada, o número de telefone ou telemóvel, a escola que frequentam, endereços de e-mail ou de sistemas de mensagens instantâneas, nomes completos de amigos/familiares, interesses específicos, clubes, etc.

Os conteúdos digitais que representem o AEM, tais como blogues, páginas web e redes sociais geridos pelos professores devem ser aprovados pelo Diretor do Agrupamento. Recomendar-se-á que os professores não criem espaços em redes sociais que destinem a ser usados pelos alunos numa base pessoal.

Os alunos serão aconselhados quanto a questões de segurança e privacidade na Internet e incentivados a definir palavras-passe, negar o acesso a desconhecidos e bloquear comunicações não desejadas. Os alunos serão incentivados a aceitar e convidar apenas amigos conhecidos em sítios de redes sociais e a negar o acesso a outros, tornando para tal, o seu perfil privado.

Todos os elementos da comunidade escolar são aconselhados a não publicar opiniões pessoais específicas e pormenorizadas, especialmente se estes puderem ser considerados ameaçadores, ofensivos ou difamatórios.

Sempre que solicitado, serão abordadas com os pais/encarregados de educação questões e preocupações relacionadas com a utilização de redes sociais, especialmente quando se trata de alunos mais novos.

6. Gestão de sistemas

6.1 Segurança dos sistemas de informação

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 cybersegurança.

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

O gestor da rede analisará a capacidade e o funcionamento do sistema com regularidade.

A utilização de nomes de utilizador e palavras-passe para aceder à rede da escola deverá ser obrigatória.

A integração de extensões de programas nos navegadores de Internet, permitirá a utilização de uma navegação mais privada e com menor índice de publicidade não desejada, durante o uso da web.

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

A escola irá monitorizar o uso da tecnologia para determinar se a Política de Segurança Digital é adequada e que a sua implementação é apropriada.

6.2 Gestão dos 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 do Agrupamento, que, por sua vez documentará o incidente e fá-lo-á chegar à pessoa responsável, conforme adequado.

O Agrupamento deverá garantir que os sistemas adequados de filtragem e controlo estão implementados de forma a evitar que pessoal docente, não docente e alunos possam aceder a conteúdo inadequado ou ilegal.

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

Devido às características dos conteúdos disponíveis na Internet, nem sempre é possível garantir que o acesso a material inadequado nunca ocorrerá através de uma configuração ou dispositivo escolar, no entanto, a escola irá tomar todas as precauções razoáveis para garantir que os utilizadores acedam apenas a material apropriado.

O Agrupamento efetuará verificações regulares para comprovar a eficácia dos métodos de filtragem adotados

7. Reduzindo os riscos online

7.1 Tecnologias emergentes

Cada professor deve 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.

Os alunos deverão ser instruídos quer por professores, quer por Encarregados de Educação, sobre a utilização adequada e segura de equipamentos pessoais dentro e fora da escola em conformidade com as Políticas de Utilização Aceitável do AEM.

7.2 Autorização e utilização da 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 escola devem tomar conhecimento da "Política de Utilização Aceitável das Tecnologias de Informação e Comunicação" do Agrupamento antes de utilizar quaisquer recursos informáticos da escola.

Os pais e encarregados de educação tomam conhecimento da Política de Utilização Aceitável das TIC dos seus educandos, no ato da matrícula. Ser-lhes-á solicitado que leiam e debatam a mesma com os seus filhos ou educandos.

Ao considerar o acesso de elementos vulneráveis da comunidade escolar (como é o caso de crianças com necessidades educativas especiais), a escola tomará as suas decisões com base nas necessidades específicas e no conhecimento que se tem do(s) aluno(s) em questão.

7.3 Incidentes preocupantes

Todos os elementos do Agrupamento 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 registará todos os incidentes comunicados e todas as medidas tomadas, em meios próprios.

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 Diretor do Agrupamento que agirá em conformidade.

O Agrupamento gerirá os incidentes relacionados com a segurança digital em conformidade com as políticas da escola em matéria de disciplina/conduita.

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

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 alunos será encaminhada para o Diretor.

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

Toda a comunidade escolar será informada dos procedimentos necessários para apresentação de queixas.

Todos os elementos da comunidade escolar 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

Todos os incidentes de *cyberbullying* (assim como todas as outras formas de *bullying*) de qualquer elemento do Agrupamento não serão tolerados e devem ser reportados diretamente ao Diretor do Agrupamento.

O Agrupamento 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.

Todos os incidentes de *cyberbullying* comunicados ao Agrupamento serão registados.

O Diretor do Agrupamento decidirá sobre os incidentes comunicados e tomará as medidas necessárias à sua resolução.

Será solicitado a alunos, professores e pais/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, deverá 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 de Utilização Aceitável.
- Os pais/encarregados de educação serão informados.
- A Polícia de Segurança Pública será contactada caso se suspeite de ação ilícita.

8. Conhecimento das políticas

8.1 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 portal do Agrupamento.

No ato da matrícula, os pais e Encarregados de Educação terão conhecimento das Políticas de Segurança Digital e dos recursos para a utilização segura da Internet, disponíveis no portal do Agrupamento e serão incentivados a analisá-los com os seus educados.

O Agrupamento ministrará, a todos os elementos do mesmo, formação atualizada e adequada sobre a utilização segura e responsável da Internet, tanto ao nível profissional como pessoal.

No portal do Agrupamento são disponibilizados recursos de apoio para uma utilização segura e responsável da Internet e de equipamentos informáticos.