



AGRUPAMENTO DE ESCOLAS DE VALE D'ESTE, BARCELOS

Sede - Escola Básica e Secundária de Vale D'Este, Viatodos, Barcelos - 343687

Rua das Fontainhas, 175 4775-263 Viatodos Telef. 252 960 200 Fax 252 960 209 Contr. 600 077 926



Política de Segurança Digital

Setembro de 2025

Este documento foi elaborado a partir do modelo disponibilizado pela European Schoolnet (www.eun.org) e desenvolvido com recursos do Kent County Council. Está licenciado com a Licença Creative Commons – Atribuição – Partilha igual 3.0

Índice

Enquadramento.....	5
Objetivos da Política de Segurança	5
Principais responsabilidades	6
Pessoal Docente, Não Docente, Alunos, Prestadores de Serviços ou de Apoio	7
Principais responsabilidades de todos os membros:	7
Principais responsabilidades dos alunos:	7
Ao nível da adequação à idade, capacidades e vulnerabilidades:	7
Principais responsabilidades dos pais e encarregados de educação:	8
Ensino e Aprendizagem	8
A importância da utilização da internet no AEVE.....	8
Benefícios da utilização da internet no ensino	8
Avaliação dos conteúdos.....	9
Gestão de Sistemas de Informação	9
Gestão do correio eletrónico.....	9
Gestão dos conteúdos publicados.....	10
Publicação de fotografias e trabalhos de alunos	10
Gestão de comunidades sociais virtuais, redes sociais e publicações pessoais.....	10
Gestão dos Sistemas de Filtragem	10
Decisões quanto à Políticas	11
Autorização do Acesso à Internet	11
Resolução de incidentes relativos à Segurança Digital	11
Gestão de casos de Cyberbullying.....	11
Gestão de telemóveis ou equipamentos pessoais.....	12
Conhecimento da Política de Segurança Digital pela Comunidade Educativa.....	12

Conscientes que estamos da importância da Internet e das tecnologias digitais, bem como da proliferação da sua utilização, não podemos, face aos riscos inerentes e à situação de vulnerabilidade a que estamos sujeitos, adotar, enquanto comunidade educativa, uma atitude passiva e de total desinteresse. Urge, desta forma, a necessidade de adoção de uma atitude proativa, informada e preventiva face aos riscos inerentes. Daí, estarmos atentos ao tipo de utilização que a nossa comunidade faz das tecnologias e dos ambientes digitais, consciencializando-a para os problemas associados e dotando-a de conhecimentos, em suma “educando” os nossos alunos, professores, encarregados de educação e assistentes operacionais para que façam uma utilização segura, atenta e consciente da Internet e das novas tecnologias.

Assim, toda Comunidade Educativa deve estar consciente da importância das boas práticas no âmbito da segurança digital, tendo em conta a educação, a proteção e a formação dos aprendentes com vista ao correto uso das tecnologias.

A Política de Segurança Digital é, deste modo, essencial na definição dos princípios fundamentais de ação que devem ser aplicados por toda a Comunidade Educativa.

O Coordenador da Política de Segurança Digital é designado pelo Diretor e funciona como elemento de articulação com a Direção do Agrupamento de Escolas de Vale D'Este.

A Política de Segurança Digital, com base na legislação aplicável e no Código de Conduta, será revista periodicamente.

Este documento foi elaborado de acordo com o Regulamento Geral de Proteção de Dados (RGPD).

A esta Política de Segurança Digital aplica-se, ainda, o previsto no Código de Conduta deste Agrupamento.

O Coordenador da Política de Segurança Digital:

____/____/____

Enquadramento

A Política de Utilização Aceitável (PUA) das Tecnologias de Informação e Comunicação (TIC) e Política de Segurança Digital do Agrupamento de Escolas de Vale D'Este tem, como objetivo, estabelecer os princípios orientadores da utilização adequada dos sistemas informáticos e redes de telecomunicações da Escola acima referida.

O presente documento é aplicável a todos os seus docentes, não docentes, alunos/formandos, pais/encarregados de educação, colaboradores, parceiros e convidados.

Todos os intervenientes educativos devem estar conscientes da sua responsabilidade aquando do uso dos sistemas informáticos da escola, uso este que deve assumir-se inerentemente legal, ético e profissional. Todos devem adotar, dentro do possível, as medidas necessárias para proteger os sistemas de dados e de informação contra acesso não autorizado, danos, perdas, abusos e roubo.

Objetivos da Política de Segurança

Os objetivos da Política de Segurança Digital (PSD) são:

- Identificar os princípios fundamentais, seguros e responsáveis esperados de todos os elementos da comunidade educativa em relação ao uso das tecnologias a fim de garantir um ambiente seguro na organização escolar no que respeita à utilização de equipamentos e Internet;
- Alertar a comunidade educativa para os potenciais riscos associados à utilização das tecnologias digitais sem, todavia, deixar de dar conhecimentos dos benefícios decorrentes das mesmas;
- Permitir que todos os utilizadores trabalhem com segurança e responsabilidade, com vista a um uso adequado, estando conscientes da necessidade de gerir as suas próprias práticas do uso da tecnologia;
- Identificar procedimentos claros a adotar de modo a responder às preocupações de segurança online que são conhecidos por todos os elementos da comunidade;

Esta política aplica-se a todos os elementos (órgão de gestão, professores, assistentes operacionais/técnicos, alunos, pais/encarregados de educação, prestadores de serviços, visitantes, entre outros que trabalhem direta ou indiretamente com o Agrupamento).

Esta PSD aplica-se a todos os equipamentos de acesso à internet, quer pessoais quer de pertença do Agrupamento, bem como à sua utilização e deve ser lida em conjunto com outras políticas escolares relevantes.

Principais responsabilidades

Competências do Órgão de Gestão e da Equipa de Segurança Digital:

- Promover uma cultura de segurança online, tendo em conta as recomendações nacionais e locais, apoiando a comunidade escolar;
- Garantir que a segurança online é considerada por todos como salvaguarda de todo o tipo de situações;
- Apoiar o Coordenador de Segurança Digital nas suas diversas responsabilidades;
- Assegurar que todos os elementos da equipa recebam formação regular e adequada no âmbito da segurança digital;
- 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 e dispositivos.

Competências do Coordenador de Segurança Digital:

- Ser o elemento de ligação em relação a todas as questões de segurança online;
- Manter-se atualizado em todos os aspetos relativos à segurança digital e online;
- Coordenar a participação em eventos locais ou nacionais promovendo um comportamento online positivo (ex.: Dia da Internet Segura);
- Garantir a promoção da segurança online a pais e encarregados de educação e comunidade educativa, em geral;
- Trabalhar com o Agrupamento na proteção e segurança de dados tendo em conta a legislação vigente;
- Monitorizar as definições de segurança online, identificando lacunas e atualizando a resposta dada às diferentes necessidades;
- Informar a equipa de gestão do Agrupamento e outras agências quanto às questões de segurança online;
- Facilitar a ligação com entidades locais e nacionais, conforme apropriado;
- Trabalhar, regularmente, com a Direção na revisão e atualização da Política de Segurança Digital, Políticas de Utilização Aceitável (PUAs), Política de Privacidade e outras relacionadas (pelo menos anualmente);
- Garantir que a segurança online é integrada noutras políticas e procedimentos da escola de forma apropriada.

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

Principais responsabilidades de todos os membros:

- Ler as Políticas, aceitá-las, cumpri-las e fazê-las cumprir;
- Contribuir para o desenvolvimento da Política de Segurança Digital;
- Assumir a responsabilidade pela segurança dos sistemas eletrónicos da escola;
- Estar consciente das diferentes situações no âmbito da segurança on-line e seu eventual efeito nos alunos;
- Dar a conhecer boas práticas no que se refere à utilização das tecnologias digitais;
- Enriquecer o currículo com a temática “Educação para a Segurança Online”, sempre que possível;
- Atendendo às políticas e procedimentos da escola adotar as medidas adequadas na identificação de situações preocupantes;
- Manter um nível de conduta profissional no uso pessoal da tecnologia, dentro e fora do local de trabalho.

Principais responsabilidades dos alunos:

- Dar o seu contributo no desenvolvimento das políticas de segurança online;
- Tomar conhecimento das Políticas e respeitá-las;
- Respeitar integralmente os outros, tanto online como offline;
- Procurar a ajuda de um adulto de confiança, se as coisas correrem mal, e apoiar aqueles que possam estar a ter problemas de segurança online.

Ao nível da adequação à idade, capacidades e vulnerabilidades:

- Responsabilizar-se por manter-se a si e aos outros seguros online;
- Responsabilizar-se pela sua própria consciência e aprendizagem em relação a oportunidades e riscos inerentes às tecnologias digitais;
- Avaliar os riscos pessoais associados à utilização das tecnologias e demonstrar atitudes responsáveis compatíveis para limitar esses riscos.

Principais responsabilidades dos pais e encarregados de educação:

- Adotar comportamentos seguros no uso da internet e nos dispositivos e plataformas digitais assumindo responsabilidade pela sua própria consciência e aprendizagem face ao tema;
- Ler as políticas da escola, incentivando os seus educandos ao seu cumprimento;
- Em colaboração com a escola reforçar junto dos seus educandos comportamentos online seguros;
- Estar atento a possíveis alterações comportamentais dos seus educandos;
- Em situações de risco procurar apoio/ajuda junto das instituições competentes (escola ou outros);

Ensino e Aprendizagem

A importância da utilização da internet no AEVE

Devendo fazer parte integrante do currículo como uma ferramenta essencial na aprendizagem, a utilização da internet no Agrupamento De Escolas de Vale D'Este, deve promover o desenvolvimento das competências digitais dos alunos e consequentemente o sucesso das suas aprendizagens, apoiar o trabalho dos professores em todas as suas vertentes reforçar a administração escolar.

O acesso à internet é um direito de quaisquer elementos da comunidade educativa que demonstre responsabilidade e maturidade na sua utilização.

Benefícios da utilização da internet no ensino

- Acesso a recursos pedagógicos educativos;
- Intercâmbio cultural e educativo entre alunos de vários países;
- Atualização de programas, gestão de redes ou qualquer outro apoio de natureza técnica;
- Potenciar diferentes abordagens pedagógicas;
- Potenciar o desenvolvimento de competências de pesquisa, avaliação e validação de informação atendendo ao cumprimento da legislação em matérias de direitos de autor;

Avaliação dos conteúdos

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

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.

Gestão de Sistemas de Informação

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. São exemplos os telemóveis, os PDA, as câmaras digitais, o correio eletrónico e os sites de redes sociais.

A proteção antivírus é atualizada frequentemente.

Os equipamentos e programas informáticos disponibilizados pela escola só podem ser utilizados para fins relacionados com a escola e para uso educacional.

Não se deve tentar instalar qualquer software adquirido ou descarregado, sem permissão do responsável pelo sistema ou da direção da escola.

O acesso aos servidores e bastidores do AEEV são restritos ao pessoal autorizado pelo Diretor.

Deve-se respeitar os direitos de autor e propriedade intelectual.

A cada início/reinício de sessão o sistema repõe a sua imagem original.

É obrigatória a autenticação para aceder à rede da escola.

Gestão do correio eletrónico

É atribuída uma conta de email institucional a todos os intervenientes da comunidade educativa (professores/educadoras, assistentes operacionais/ técnicos, alunos, pais/encarregados de educação) para fins profissionais que apenas está ativada durante a permanência dos mesmos na instituição. Após a sua saída a conta fica suspensa por determinado período findo o qual é eliminada.

A comunicação com alunos, pais/encarregados de Educação e com instituições para tratamento de assuntos oficiais do Agrupamento, deve ser preferencialmente realizada a partir de endereços eletrónicos institucionais.

Os endereços eletrónicos encontram-se organizados em unidades organizacionais com diferentes permissões.

A unidade organizacional alunos, não permite o envio e/ou receção de emails externos à organização.

São criados grupos de email para diferentes estruturas, a saber: alunos por turma, encarregados de educação por turma, Conselhos de Turma, Grupos Disciplinares, etc.

É vedada a utilização de grupos de email, criados pela unidade educativa, a todos os encarregados de educação bem como é vedada a utilização de grupos de email, criados pela unidade educativa, a todos os alunos com a exceção do grupo de email associado à turma onde o mesmo se encontra inserido.

Gestão dos conteúdos publicados

As informações de contacto no sítio do Agrupamento de Escolas de Vale D'Este devem ser a morada, os números de telefone, fax e email do Agrupamento/Serviços Administrativos.

Os conteúdos das publicações em formato digital são da responsabilidade dos seus autores e devem respeitar os direitos de propriedade intelectual, as políticas de privacidade e os direitos de autor.

Publicação de fotografias e trabalhos de alunos

Na publicação de imagens e/ou gravações de vídeo que incluem alunos, deve ser garantida a proteção da imagem dos mesmos de acordo com a legislação aplicável e após autorização por escrito dos pais/encarregados de educação.

Gestão de comunidades sociais virtuais, redes sociais e publicações pessoais

Através de atividades dinamizadas em sala de aula, participação em projetos e iniciativas e Bibliotecas Escolares, os alunos serão ensinados a usar a Internet, aplicações digitais e redes sociais, de modo a protegerem a sua privacidade, a não divulgar os dados pessoais, negarem o acesso a desconhecidos e bloquear e denunciar comunicações não desejadas.

Gestão dos Sistemas de Filtragem

O acesso à Internet fornecido pelo Agrupamento inclui sistemas de filtragem adequados.

Qualquer material/situação que a escola considere ser ilegal será denunciado através dos mecanismos oficiais segundo as normas em vigor.

A utilização da Internet é objeto de monitorização periódica por parte do responsável da rede.

Decisões quanto à Políticas

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 têm conhecimento da Política de Segurança Digital no início do ano letivo bem como dos recursos para a utilização da Internet disponíveis na página do Agrupamento que são analisados na mesma altura.

Resolução de incidentes relativos à Segurança Digital

Perante o conhecimento de situações preocupantes, do ponto de vista de segurança digital, os elementos da Comunidade Escolar deverão informar o Coordenador de 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. No caso dos docentes, assistentes operacionais, devem estes expor a situação à Direção, e no caso dos discentes, deve ser dado conhecimento ao diretor de turma que, conforme a gravidade da situação, a encaminhará para as instâncias superiores. Estes procedimentos aplicam-se também a situações de cyberbullying.

Relativamente a esta última situação, serão adotados procedimentos claros na investigação dos mesmos. Aluno, professores e pais/encarregados de educação serão aconselhados a manter um registo como prova.

Sempre que houver razões que apontem para a suspeita/confirmação de atividade ilegal, dentro deste âmbito, encaminhar-se-á a situação para as atividades competentes.

Gestão de casos de Cyberbullying

A situações de cyberbullying identificadas serão dadas a conhecer à Direção e/ou Coordenador de Segurança Digital e, quando necessário, às autoridades competentes. Serão seguidas diligências claras na investigação dos incidentes ou alegados casos de Cyberbullying. Aos envolvidos (alunos, professores e pais/encarregados de educação) será aconselhado que mantenham o registo de prova das ocorrências.

O Agrupamento de Escolas de Vale D'Este promoverá junto da Comunidade Educativa uma cultura de sensibilização e responsabilização da importância de manterem uma conduta adequada na utilização da Internet e dos recursos digitais.

As sanções, para os envolvidos em cyberbullying, poderão incluir:

- a eliminação de todo o material considerado inadequado;
- a suspensão do direito de acesso à Internet na escola durante um período de tempo a determinar pela Direção;
- a comunicação às autoridades competentes, caso se suspeite de ação ilícita.

Os pais/encarregados de educação serão informados da sanção aplicada.

Gestão de telemóveis ou equipamentos pessoais

Aos alunos da Educação Pré-escolar, do 1.º e 2.º Ciclos não é permitida a utilização de smartphones, smartwatches, telemóveis e dispositivos de comunicação móveis em todos os espaços escolares, interiores e exteriores.

Aos alunos do 3.º ciclo, apenas é permitida a utilização de smartphones, smartwatches, telemóveis e dispositivos de comunicação móveis para a realização de atividades quando previamente solicitada por professores.

As exceções às limitações supracitadas encontram-se definidas no Regulamento do Uso dos Telemóveis (RUT) deste Agrupamento.

O Agrupamento AEVE não assume qualquer responsabilidade pela perda, roubo ou dano de dispositivos eletrónicos. Estes são da exclusiva responsabilidade dos seus utilizadores, conforme previsto no artigo 13º do RUT.

A captura de imagens e/ou vídeo e respetiva divulgação obedece ao estipulado nos artigos 8º e 9º do RUT.

Ao incumprimento das situações descritas aplica-se as medidas previstas no artigo 10º do RUT.

Conhecimento da Política de Segurança Digital pela Comunidade Educativa

A Política de Segurança Digital está disponível, para conhecimento e consulta, na página web do Agrupamento.