Política de Segurança Digital

DOCUMENTOS ESTRUTURANTES

AGRUPAMENTO DE ESCOLAS
LIMA - DE - FARIA
CANTANHEDE

Ficha Técnica:

Título: Política de Segurança Digital do Agrupamento de Escolas Lima-de-Faria, Cantanhede

Autoras

Cristina Silva, Isabel Bernardo, Leonor Melo e Maria Manuel Fael.

Equipa do Plano de Ação de Desenvolvimento Digital da Escola. Serviço das Bibliotecas Escolares.

Edição Agrupamento de Escolas Lima-de-Faria, Cantanhede

1.ª edição - setembro de 2014.
2.ª edição - atualização em janeiro de 2017.
3.ª edição - reformulada em julho e em setembro de 2025.

Documento aprovado no Conselho Pedagógico do AELdF, em 18.11.2014, como parte integrante do Regulamento Interno.

Atualizações aprovadas em Conselho Pedagógico do AELdF, em 12.09.2017, como parte integrante do Regulamento Interno.

Atualizações submetidas a apreciação em Conselho Pedagógico do AELdF, em 23.07.2025 e 05.09.2025, como parte integrante do Regulamento Interno.

A Política de Segurança Digital será revista quando oportuno, sob a orientação da equipa PADDE.

Este documento está licenciado com uma Licença Creative Commons BY-NC-SA (Atribuição, NãoComercial Compartilhalgual) 4.0.

Sumário

Introdução 4

1. O papel das tecnologias digitais em contexto escolar 4

2. Objetivos e âmbito de aplicação da Política de Segurança Digital 4

3. Coordenação e competências de aplicação e monitorização da Política de Segurança Digital 5

Coordenação 5

Competências do Diretor do AELdF e da Equipa PADDE 5

Competências da Coordenação de Segurança Digital 5

4. Responsabilidades gerais do pessoal docente e não docente, alunos e demais pessoas que trabalham ou prestam serviços no ou em nome do AELdF 5

5. Papel dos pais e encarregados de educação na implementação da Política de Segurança Digital 6

6. Tecnologias digitais no ensino e aprendizagem 6

Aprender com tecnologias digitais 6

Laboratório de Educação Digital 7

Equipamentos da Escola Digital 7

7. Comunicação 7

Correio eletrónico institucional 7

Gestão do correio eletrónico 7

Publicação de conteúdos e recolha de imagem e som 7

8. Organização e gestão 8

Gestão e manutenção de sistemas de informação 8

Manutenção dos sistemas de informação 9

Gestão de plataformas 9

Plataforma GIAE 9

Gestão dos sistemas de filtragem 9

Resolução de incidentes relativos à Segurança Digital 9

Gestão dos casos de *cyberbullying* 10

Gestão de telemóveis e outros equipamentos portáteis 10

9. Infração às regras definidas na Política de Segurança Digital 11

10. Divulgação da Política de Segurança Digital 12

Anexo 1 – Informação a constar nas autorizações a assinar pelos encarregados de educação 12

Anexo 2 – Política de privacidade 13

Introdução

Vivemos numa era em que crianças, jovens e adultos interagem diariamente com tecnologias digitais — computadores, telemóveis, consolas, *Internet*, sistemas de Inteligência Artificial, redes sociais, imagens e texto digital, entre outras. Estes recursos oferecem inúmeras oportunidades de aprendizagem, comunicação e interação social, mas também colocam desafios e riscos que exigem atenção, responsabilidade e acompanhamento.

No contexto escolar, o acesso à *Internet* tornou-se uma realidade incontornável. A maioria dos membros da comunidade escolar utiliza dispositivos com ligação à *Internet*, sejam eles fornecidos pela escola ou individuais, como portáteis, *tablets*, *smartphones* ou *smartwatches*, muitas vezes ligados através de dados pessoais. A presença constante da tecnologia digital no quotidiano escolar reforça a importância de promover uma cultura de uso seguro, crítico e ético da mesma.

A **Política de Segurança Digital** (doravante, *Política*) consiste num conjunto de orientações e regras definidas pela escola para promover o uso seguro, responsável e ético das tecnologias digitais por alunos, pessoal docente e não docente e demais membros da comunidade educativa, que interagem com o ambiente escolar. Inclui medidas de proteção de dados, prevenção de riscos *online* e promoção de comportamentos digitais adequados.

A *Política* do Agrupamento de Escolas Lima-de-Faria, Cantanhede (AELdF) foi elaborada tendo em consideração a diversidade etária, pedagógica e de acesso a tecnologias digitais existentes nos diferentes níveis e ciclos de ensino. Assenta num compromisso coletivo de garantir a segurança, a cidadania digital e o bem-estar de todos os membros da comunidade escolar, e está alinhada com documentos estruturantes da educação nacional, nomeadamente:

- o *Perfil dos Alunos à Saída da Escolaridade Obrigatória* (PASEO)
- a *Estratégia Nacional de Educação para a Cidadania* (ENEC)
- o *Regulamento Geral de Proteção de Dados* (RGPD)
- o *Projeto Educativo* do AELdF
- o *Regulamento Interno* do AELdF
- o *Plano de Ação para o Desenvolvimento Digital da Escola* (PADDE).

1. O papel das tecnologias digitais em contexto escolar

Em contexto escolar, o uso das tecnologias digitais desempenha três funções essenciais: potenciar o ensino e a aprendizagem, promover a comunicação e facilitar a organização e a gestão.

No que respeita ao **processo de ensino, aprendizagem e avaliação**, as tecnologias digitais proporcionam o acesso a recursos educativos diversificados (texto, imagem, vídeo, recursos educativos abertos…), facilitadores da implementação de metodologias ativas e de processos de avaliação com dimensão formativa. Permite ainda a diversificação dos momentos de aprendizagem, tanto no que respeita à interação aluno-aluno e aluno-professor, como na interação com outros atores (por exemplo, especialistas numa determinada área, alunos e professores de outras escolas e países), cujo trabalho pode contribuir para enriquecer o currículo.

No que concerne à **comunicação**, através do correio eletrónico, das redes sociais, da página *Web* ou outros meios, as tecnologias digitais facilitam a circulação de informação e a criação de um sentido de comunidade interna e permitem a divulgação externa do trabalho desenvolvido no AELdF.

No âmbito da **organização e gestão**, as tecnologias digitais possibilitam a automatização de processos, tais como o registo de faltas, de sumários, matrículas, elaboração de horários, marcação de refeições, empréstimo de livros e equipamentos, entre muitos outros atos.

2. Objetivos e âmbito de aplicação da Política de Segurança Digital

São objetivos da *Política:*

- Proteger a comunidade educativa, garantindo a segurança dos dados pessoais e prevenindo riscos, como o *ciberbullying*, o acesso a conteúdos impróprios, ou a exposição a fraudes.

- Promover a cidadania digital, orientando os alunos para o uso das tecnologias digitais com responsabilidade, respeito pelos outros e consciência das suas ações no ambiente digital.
- Orientar o uso pedagógico das tecnologias, apoiando professores e alunos na integração segura das tecnologias digitais no ensino e na aprendizagem, fomentando boas práticas e prevenindo abusos ou dependências.

Esta *Política* aplica-se aos alunos, ao pessoal docente e não docente, no que respeita ao uso de tecnologias digitais dentro dos espaços do Agrupamento, ou no âmbito de atividades que, realizadas em seu nome, ocorram fora desses espaços.

Dada a importância dos pais ou encarregados de educação na constituição de uma comunidade educativa, esta *Política* define também o âmbito de articulação com os mesmos, com vista ao bom uso das tecnologias digitais pelas crianças e alunos.

Visitantes, voluntários e outros agentes que possam atuar no AELdF, ou em seu nome, devem ser informados, sempre que pertinente, da existência desta *Política* e da necessidade de a respeitar.

3. Coordenação e competências de aplicação e monitorização da Política de Segurança Digital

Coordenação

A pessoa responsável pela coordenação da *Política* é designada pelo Diretor do AELdF, de entre os membros da Equipa PADDE, e funciona como elemento de articulação com a Direção.

Competências do Diretor do AELdF e da Equipa PADDE

São competências do Diretor e da Equipa PADDE:

- Promover uma cultura de segurança *online* para todas as partes envolvidas, em linha com as recomendações nacionais e internacionais, apoiando e consultando toda a comunidade escolar, sempre que necessário.
- Apoiar a Coordenação da Segurança Digital, garantindo que tenha recursos humanos e materiais suficientes para cumprir o seu papel de segurança digital e demais responsabilidades.
- Assegurar que todos os membros da Equipa PADDE têm acesso a formação necessária para o desempenho das suas funções.

Competências da Coordenação de Segurança Digital

São competências da Coordenação de Segurança Digital:

- Agir como ponto de contacto com a comunidade escolar, a Direção e demais organismos envolvidos, no que respeita a todos os aspetos de Segurança Digital do AELdF.
- Garantir que a segurança digital é promovida junto dos alunos, pessoal docente e não docente, os pais e encarregados de educação e demais intervenientes da atividade do AELdF.
- Implementar a proteção de dados, de acordo com a legislação vigente.
- Monitorizar os procedimentos de segurança digital, adequando as respostas às necessidades.
- Rever, quando necessário, a Política de Segurança Digital, propondo ao Diretor um documento atualizado e a subsequente integração no Regulamento Interno.

4. Responsabilidades gerais do pessoal docente e não docente, alunos e demais pessoas que trabalham ou prestam serviços no ou em nome do AELdF

São responsabilidades para todos os referidos:

- Conhecer a *Política*, nomeadamente através do exemplar disponível na página *Web* do AELdF.
- Contribuir para a execução da *Política*, cumprindo-a e fazendo-a cumprir, dentro e fora do AELdF, sempre que esteja em causa uma atividade em nome deste.
- Identificar, junto da Coordenação de Segurança Digital, situações que infrinjam a *Política,* ou que configurem situações de insegurança digital.

5. Papel dos pais e encarregados de educação na implementação da Política de Segurança Digital

- Assumir o compromisso informado, através de documento assinado no ato de matrícula, de tomar conhecimento e promover, por parte do seu educando, a implementação e o cumprimento da *Política*.
- Colaborar proactivamente com a escola, sempre que se verificar, na atuação do seu educando, risco na utilização de tecnologias digitais, ou um uso não conforme às regras definidas na *Política*.

6. Tecnologias digitais no ensino e aprendizagem

Para além dos equipamentos disponibilizados a alunos e professores pela Escola Digital, o AELdF disponibiliza recursos que possibilitam a integração de tecnologias digitais nos processos de ensino e aprendizagem e de avaliação. Estes recursos incluem acesso a equipamentos, ligação à *Internet*, mas também materiais educativos de suporte ao desenvolvimento de competências em literacia da informação, digital e mediática.

De entre os equipamentos disponíveis, destaca-se o Laboratório de Educação Digital, Tipo 3, mas também os disponíveis no "Aprendiz de Investigador" e no sítio *Web* do Serviço das Bibliotecas Escolares (*Ler é um risco!*), nomeadamente os desenvolvidos no âmbito do projeto "ProLiteracias".

Aprender com tecnologias digitais

O uso de tecnologias digitais para ensinar e aprender, incluindo as que implicam o acesso aos conteúdos *online*, é um direito dos alunos e dos professores, e dos que, em atividades autorizadas pelo AELdF, contribuem para o enriquecimento do currículo.

Nas atividades de ensino e aprendizagem deve ser claro, de acordo com a idade dos alunos, o que significa, em geral e em cada contexto específico, um uso das tecnologias digitais que obedeça aos princípios da procura da melhor informação para aprender, da honestidade intelectual e do respeito pelos direitos de autor.

Nas atividades de ensino e aprendizagem, deve ser explícito, sempre que aplicável e de acordo com a idade dos alunos, o papel da utilização de sistemas de Inteligência Artificial, nomeadamente sistemas generativos assentes em largos modelos de linguagem.

Atividades que impliquem (ou possam implicar) pesquisa e utilização de informação acessível por via digital devem:

- ter explicitados os procedimentos de verificação da qualidade da informação, nomeadamente através da aplicação de competências de literacia da informação e literacia mediática, podendo haver articulação com os Serviços das Bibliotecas Escolares, se o professor o considerar oportuno;
- ter explicitados os procedimentos de penalização a aplicar em caso de plágio ou de fraude por utilização de sistemas com Inteligência Artificial, nomeadamente Inteligência Artificial generativa;
- ter indicações precisas para a realização de referências bibliográficas, como estilo APA, 7.ª edição, podendo haver remissão para os guias e tutoriais de apoio disponíveis no "Aprendiz de Investigador" (www.aprendizinvestigador.pt);
- ter indicação precisa da licença Creative Commons utilizada, caso o trabalho dos alunos venha a ser divulgado publicamente, podendo recorrer-se ao apoio dos guias e tutoriais do "Aprendiz de Investigador" (www.aprendizinvestigador.pt).

Atividades de avaliação, nomeadamente com intenção classificatória e suportadas em tecnologias digitais, devem ter explicitados os procedimentos de penalização a aplicar em caso de plágio ou de fraude por utilização indevida, nomeadamente por sistemas de Inteligência Artificial generativa.

A formação dos alunos em competências em literacia da informação e mediática pode ainda ser reforçada através da articulação com a disciplina de Oferta Complementar (1.º ciclo), Tecnologias da Informação e Comunicação (2.º e 3.º ciclos) e com o projeto "ProLiteracias / IA – Inteligência Atenta", a implementar, em articulação curricular, pelo Serviço das Bibliotecas Escolares, a partir do ano letivo 2025-2026.

Laboratório de Educação Digital

O Laboratório de Educação Digital (LED 3 – Área STEM (Science, Technology, Engineering, Mathematics + Área Artes e Multimédia) é coordenado por uma pessoa designada pelo Diretor do AELdF.

A utilização do LED 3 obedece a regulamento específico, que é parte integrante do Regulamento Interno e que obedece aos princípios desta *Política*.

Equipamentos da Escola Digital

As atividades de ensino e aprendizagem em sala de aula, com utilização ativa, pelos alunos, de equipamentos digitais, deve, preferencialmente, realizar-se com recurso aos equipamentos da Escola Digital (Kits digitais).

A gestão dos Kits digitais é efetuada pelos Serviços das Bibliotecas Escolares, sob supervisão do responsável, na Direção, pelos equipamentos e instalações.

7. Comunicação

Correio eletrónico institucional

A comunicação com alunos, pais e encarregados de educação, e com instituições para tratamento de assuntos oficiais do AELdF, 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*, evitando-se potenciais fugas de informação ou ataques à organização.

Gestão do correio eletrónico

É atribuída uma conta de correio eletrónico institucional a todos os funcionários do Agrupamento, para fins profissionais, que apenas está ativada durante a permanência do funcionário na instituição, sendo eliminada no momento da sua saída, salvaguardando, a pedido do mesmo, um tempo limite para a realização de cópia de segurança da informação existente na conta e na Google Drive associada.

No primeiro ano de matrícula no AELdF, é atribuída a cada aluno uma conta de correio eletrónico institucional, que terá a duração igual à da permanência do aluno na instituição. Esta conta será utilizada para fins pedagógicos e administrativos.

O envio de informação ou de documentos, por parte da Direção e dos Serviços Administrativos, para os professores, técnicos superiores, assistentes técnicos e assistentes operacionais deverá ser feito através dos endereços eletrónicos institucionais.

Quando uma mesma mensagem é enviada para vários recetores, deverá, preferencialmente, ser enviada em Bcc, de modo a preservar a privacidade.

Publicação de conteúdos e recolha de imagem e som

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.

Não serão publicadas listas de turmas e de pautas *online* e as listas e 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 deve assegurar que os conteúdos publicados são corretos e adequados e que estão em consonância com os valores preconizados no Projeto Educativo do Agrupamento.

Nenhum elemento da comunidade escolar deverá criar qualquer *site*, canal ou página *online* sem comunicação e autorização prévia do Diretor.

Publicações relativas a eventos promovidos pelo AELdF não deverão ser feitas, originariamente, em páginas pessoais, a não ser que sejam salvaguardadas todas as questões relativas ao direito de privacidade e imagem dos intervenientes.

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.

No âmbito das atividades promovidas pelo AELdF, antes da publicação de imagens, voz ou de gravações vídeo que incluam alunos, assim como de trabalhos realizados pelos mesmos, deve ser garantido que existe a autorização expressa e informada, de acordo com a legislação aplicável, que foi dada a assinar aos encarregados de educação no ato da matrícula no AELdF, e que consta no processo individual de cada aluno.

Nas publicações que impliquem alunos, deve evitar-se informação que permita a relação direta entre o nome do aluno e a sua imagem ou voz. Excetuam-se as situações devidamente identificadas nas quais o aluno, isoladamente, participa numa atividade ou ganha um prémio, havendo autorização expressa por parte do encarregado de educação para a publicação nestas circunstâncias.

A publicação de trabalhos dos alunos deve estar acompanhada de uma ficha técnica e de uma licença de publicação. De acordo com a idade, o aluno que dá autorização para a publicação do seu trabalho deve conhecer os termos da licença de publicação.

Também os docentes e não docentes devem dar o seu consentimento expresso e informado para a recolha e disseminação de imagem e som que respeite às suas pessoas e que seja realizada no âmbito das atividades do AELdF.

A publicação de trabalhos realizados no âmbito da atividade profissional de pessoal docente e não docente apenas pode ser realizada com o seu consentimento e protegida com uma licença de publicação.

8. Organização e gestão

Gestão e manutenção de sistemas de informação

A segurança dos sistemas informáticos do AELdF e dos utilizadores será revista anualmente.

A proteção antivírus será atualizada mensalmente.

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 às restrições de acesso a esses sistemas e à robustez das palavras-chave.

O uso dos dispositivos móveis do Projeto “Literacias na escola: formar os parceiros da biblioteca” deve ser efetuado de acordo com o estipulado no respetivo regulamento.

A instalação de *software* para fins educativos nos computadores de mesa e portáteis deve ser autorizada pelo Coordenador da Segurança Digital e feita, preferencialmente, por um membro da Equipa de Apoio TIC. No caso dos dispositivos móveis à guarda dos Serviços das Bibliotecas Escolares, a instalação de *software* deve ser articulada com estes serviços.

Os utilizadores não devem deixar ficheiros de uso pessoal, ou dos alunos, nos computadores de mesa 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. As credenciais de cada utilizador são fornecidas pela Equipa de Apoio TIC.

A página inicial de navegação de cada computador ou dispositivo ao serviço dos utilizadores será definida pela Equipa PADDE, de acordo com as necessidades dos serviços. Os utilizadores não devem, em circunstância alguma, alterar as páginas de navegação pré-definidas.

Manutenção dos sistemas de informação

Gestão de plataformas

O AELdF possui:

- uma licença do Office 365, o que permite a todos os utilizadores o acesso às ferramentas constantes dessa licença, a saber: Microsoft Teams, Outlook, Word, Excel, PowerPoint, OneDrive, OneNote, Forms, Sway, Stream, Whiteboard;
- licenciamento Office 2016, Windows 10, Photoshop, Biblionet e LabelJoy;
- a solução Workspace da Google, com acesso de todos utilizadores ao universo Google, ainda que com regras e graus de segurança específicos a cada estrutura; uma das aplicações é o Google Classroom, de que cada utilizador faz a criação e gestão;
- a plataforma Moodle, que permite o registo autónomo de cada utilizador e de cada docente, que faz a sua gestão de disciplinas.

No âmbito do projeto "ProLiteracias", o AELdF terá ainda acesso a licenças de *software*, potenciado por Inteligência Artificial, como o Padlet, o DeepL, o Gamma e outras aplicações, cujo uso será regulamentado e divulgado junto da comunidade escolar pelo Serviço das Bibliotecas Escolares.

No caso de alunos com uma incapacitação temporária ou doença prolongada, as plataformas Teams, Meet ou Zoom poderão ser utilizadas para ensino a distância, de acordo com os procedimentos estabelecidos entre os alunos e os professores, sob orientação do diretor de turma e do responsável direto da Direção ou da Coordenação de Estabelecimento.

Plataforma GIAE

Todos os professores, diretores de turma, alunos, pais, encarregados de educação e funcionários administrativos têm acessos diferenciados a esta plataforma. As credenciais de acesso ou palavras-passe não deverão ser partilhadas.

A palavra-passe inicial deve ser substituída por uma outra que siga as normas de segurança para a criação de palavras-passe fortes, a saber: comprimento, complexidade, evitar informações pessoais, usar frases em vez de palavras, não reutilizar palavras-passe, usar um gestor de palavras-passe ou ativar e substituir a palavra-passe com frequência.

A disseminação de informação ou dados pessoais dos alunos é proibida.

Gestão dos sistemas de filtragem

O acesso à *Internet* fornecido pelo AELdF incluirá sistemas de filtragem adequados à idade, à maturidade dos alunos e às necessidades do currículo.

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 Regulamento Interno.

Serão feitas verificações regulares, para comprovar a eficácia dos métodos de filtragem adotados. Sempre que é detetada alguma anomalia, a escola é contactada pelo Centro Nacional de Cibersegurança, para dar conta da situação e da respetiva resolução.

Se sítios indesejáveis chegarem ao conhecimento de alunos, professores ou outros elementos da comunidade educativa, 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 o AELdF considere ser ilegal será denunciado através dos mecanismos oficiais, segundo as normas em vigor.

Resolução de incidentes relativos à Segurança Digital

Todos os elementos do AELdF devem informar o Coordenador da Segurança 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, entre outras.

As queixas relativas à utilização indevida da *Internet* serão tratadas no quadro dos procedimentos de apresentação de queixas ou denúncias adotadas pela escola e poderão ser encaminhadas para a Linha Internet Segura ou o Centro Nacional de Cibersegurança.

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 da Comissão de Proteção de Crianças e Jovens (CPCJ), através da Direção, do Coordenador da Segurança Digital e encaminhará a situação para as Autoridades Competentes.

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.

O Coordenador da Segurança Digital registará todos os incidentes, no livro de registo de incidentes comunicados, bem como todas as medidas aplicadas, e tomará as providências necessárias nos casos de *cyberbullying*.

Gestão dos casos de *cyberbullying*

Os incidentes de *cyberbullying* devem ser comunicados ao Coordenador da Segurança Digital, que articulará com a Direção e as autoridades competentes, quando necessário.

Em situação de *cyberbullying*, alunos, professores e pais e encarregados de educação serão aconselhados a manter os registos como prova.

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

Todos os elementos da escola serão sensibilizados para a importância de manterem uma conduta adequada na utilização da *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.

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 suspenso o seu direito de acesso à *Internet* na escola durante um período a determinar pela Direção, em articulação com o Coordenador da Segurança Digital;
- os pais / encarregados de educação serão informados da sanção aplicada; a Polícia e as Autoridades Judiciais serão contactadas / informadas, caso se suspeite de ação ilícita.

Gestão de telemóveis e outros equipamentos portáteis

Educação Pré-Escolar ao 3.º Ciclo

Crianças da Educação Pré-Escolar e alunos do 1.º ao 3.º Ciclo não podem ser portadores de qualquer dispositivo móvel pessoal (*smartphone, tablet* e *smartwatch*), com acesso à *Internet,* para as instalações do estabelecimento de ensino que frequentam. Os alunos do 2.º e 3.º ciclos podem ser portadores de telemóveis de teclas, sem acesso à Internet.

São exceções à restrição de uso, pelos alunos do 2.º e 3.º ciclos, de dispositivos móveis com acesso à Internet: A) alunos com proficiência de Português Língua Não Materna até ao nível A2, inclusive; B) alunos com sistemas de alerta digital em caso de doença crónica. Para serem aplicadas estas exceções, os diretores de turma devem providenciar o pedido de autorização junto do Diretor do AELdF e efetuar o arquivo do documento no dossier da turma, uma vez assinado.

O uso dos Kits digitais pelos alunos do 1.º ao 3.º Ciclo, em espaço escolar, é definido pelos professores que solicitem a presença do equipamento na aula, consoante as atividades programadas.

Para além do uso em sala de aula, os alunos dos 2.º e 3.º ciclos apenas podem usar os computadores dos Kits digitais na Biblioteca Escolar, se exclusivamente para a realização de trabalhos escolares.

Ensino Secundário

Os alunos do Ensino Secundário devem, durante o período de aulas, deixar os telemóveis, *tablets* e *smartwatch,* de que são portadores, na secretária do professor (numa gaveta da secretária), ou em local designado para o efeito pelo professor. Sob pena de procedimento disciplinar, a utilização destes dispositivos durante o tempo das atividades letivas só pode ocorrer mediante a orientação expressa do professor.

Nas aulas de Educação Física, a guarda destes equipamentos deve obedecer às regras específicas estabelecidas nos balneários.

A utilização de dispositivos móveis com acesso à *Internet* (*smartphone, tablet* e *smartwatch*), incluindo computadores pessoais e dos Kits digitais, não pode ser realizada em espaços comuns cobertos, tais como, corredores, bar, cantina e zonas de circulação entre blocos de aula.

Os alunos poderão usar, na Biblioteca Escolar, dispositivos móveis com acesso à *Internet* (apenas *tablets* e computadores portáteis), se exclusivamente para a realização de trabalhos escolares.

Os utilizadores são responsáveis por qualquer tipo de dispositivos eletrónicos que tragam para as instalações do AELdF. Este não assume qualquer responsabilidade pela perda, roubo ou dano de tais objetos, mesmo no caso do equipamento constante dos Kits digitais.

Equipamentos portáteis, incluindo os Kits digitais, devem manter-se desligados durante os tempos das atividades curriculares e de complemento curricular, a não ser para efeitos pedagógicos devidamente autorizados, orientados e supervisionados pelo professor.

A funcionalidade de *Bluetooth* dos equipamentos deve estar sempre desligada e não pode ser utilizada para enviar ficheiros ou para interferir com o funcionamento de outros dispositivos.

Outros

Os professores, ou outros responsáveis, podem confiscar um telemóvel ou equipamento, conforme o estabelecido no Código de Conduta do AELdF. O Coordenador de Segurança Digital pode fazer uma pesquisa ao telemóvel ou equipamento, com o consentimento do aluno ou dos pais e 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 portáteis serão entregues aos encarregados de educação.

Se um aluno 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 através dos telemóveis, durante o horário letivo. Em caso de necessidade de contacto urgente, devem usar o número de telefone do estabelecimento de ensino do AELdF frequentado pelo seu educando.

Os professores e educadores não devem 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 emergências e quando outros meios de contacto não estejam operacionais.

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

A captura de imagem, vídeo ou som deverá ser feita, preferencialmente, com equipamentos disponíveis no AELdF.

9. Infração às regras definidas na Política de Segurança Digital

As infrações identificadas são tratadas como infrações disciplinares, devendo ser comunicadas ao Coordenador da Política de Segurança Digital que articula com o Diretor, no âmbito das suas competências.

São também consideradas infrações a esta *Política* o uso indevido de recursos digitais, nomeadamente os potenciados por Inteligência Artificial, para plagiar ou realizar, pelo aluno, qualquer tipo de tarefa escolar. Estas situações, assim como o uso indevido de dispositivos portáteis pessoais ou dos Kits digitais, devem ser comunicadas aos Diretores de Turma e aos Pais e Encarregados de Educação através da plataforma GIAE.

De acordo com a gravidade da situação, compete aos Diretores de Turma articular com o Coordenador de Segurança Digital.

Nas situações de *cyberbullying*, aplicam-se os procedimentos acima definidos, devendo a comunicação ser efetuada diretamente com o coordenador de segurança digital.

Nas situações de uso não autorizado de dispositivos portáteis pessoais de acesso à Internet nos espaços comuns, incluindo os Kits digitais, os alunos devem ser identificados e a comunicação efetua-se através do preenchimento de um formulário, cujo acesso é enviado pela Direção a todos os docentes e não docentes.

10. Divulgação da Política de Segurança Digital

No ato da matrícula, e nas primeiras reuniões com o diretor de turma, os pais e encarregados de educação terão conhecimento da Política de Segurança Digital e serão incentivados a analisá-la com os seus educandos.

A *Política de Segurança Digital* está disponível no sítio *Web* do Agrupamento e no sítio *Web* do Serviço das Bibliotecas Escolares do Agrupamento.

Uma leitura e uma discussão da *Política de Segurança Digital,* adequadas à faixa etária dos alunos, serão efetuadas pelos professores titulares de turma e pelos diretores de turma dos anos iniciais nas escolas Carlos de Oliveira, Febres, e Lima-de-Faria, Cantanhede.

O pessoal docente e não docente recebe, no momento de entrada em funções no AELdF, um formulário, no qual se compromete a cumprir e fazer cumprir o que está definido na *Política*.

Na fase de implementação desta *Política*, docentes e não docentes em exercício de funções no AELdF irão receber um formulário, no qual se comprometem a cumprir e fazer cumprir o que está definido na *Política*.

ANEXOS

Anexo 1 – Informação a constar nas autorizações a assinar pelos encarregados de educação

POLÍTICA DE SEGURANÇA DIGITAL

A segurança digital abrange questões relacionadas com a utilização que todos fazem da *Internet* e dos dispositivos que permitem a comunicação eletrónica em ambiente escolar e fora dele. Uma 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 Agrupamento de Escolas Lima-de-Faria, Cantanhede, adotou, e incluiu no seu Regulamento Interno, uma **Política de Segurança Digital**, a qual está disponível para consulta na página *Web* do Agrupamento e na página *Web* do Serviço das Bibliotecas Escolares.

Sugerimos ao/à senhor/a encarregado/a de educação a leitura do documento **Política de Segurança Digital** e sua análise com o/a seu/sua educando/a. Ao longo do ano letivo, o Agrupamento proporcionará formação aos alunos e a outros membros da comunidade escolar, pelo que apelamos para que sensibilize o seu/sua educando/a a participar ativamente nessa formação.

Declaro que tomei conhecimento de que o Agrupamento de Escolas Lima-de-Faria, Cantanhede, tem uma **Política de Segurança Digital**, acessível a consulta na página *Web* do Agrupamento e na do Serviço das Bibliotecas Escolares, e aceito o cumprimento das regras nela estabelecidas.

Anexo 2 – Política de privacidade

Ao aceitar a Política de Privacidade, está a autorizar ao Agrupamento de Escolas Lima-de-Faria a proceder ao tratamento dos seus dados pessoais e dos dados pessoais do seu educando. Declara, ainda:

Estar ciente e plenamente informado/a de que o tratamento dos seus dados pessoais e os dados pessoais do seu educando inclui todas as operações efetuadas sobre os dados por si transmitidos, por meios automatizados ou não, necessários à frequência ao AE Lima-de-Faria e ao desenvolvimento de todo o processo educativo, de acordo com a legislação em vigor.

Aceitar e consentir que os seus dados e os dados pessoais do seu educando sejam transmitidos a outras entidades públicas, ou privadas na condição de subcontratantes, exclusivamente para fins legais e no exercício das atribuições e competências do Agrupamento de Escolas Lima-de-Faria.

Tomar conhecimento de que os seus dados e os dados pessoais do seu educando serão guardados pelo período fixado em lei, regulamento ou o estritamente necessário às finalidades para que foram recolhidos.

Tomar conhecimento que, nos termos da legislação aplicável, é garantido, a todo o tempo, o exercício (i) dos direitos de acesso, retificação, atualização e eliminação (apagamento) dos seus dados pessoais e dos dados pessoais do seu educando, podendo ainda opor-se ao tratamento dos mesmos, mediante pedido escrito dirigido ao AE Lima-de-Faria, bem como (ii) do direito de apresentar queixa junto Comissão Nacional de Proteção de Dados através do Website www.cnpd.pt. Prestar o presente consentimento de forma livre e voluntária;

Assim,

Assumo que o meu educando mantenha a câmara ligada em caso de necessidade de sessões de ensino não presencial. Garanto que o meu educando cumpre o dever de assiduidade e as tarefas escolares em situação de ensino não presencial.

Autorizo a abertura de email institucional (do qual me será dado conhecimento quando o meu educando tiver menos de 13 anos de idade). Autorizo a inscrição do meu educando em plataformas digitais necessárias às atividades planificadas pelos professores.

Autorizo / Não autorizo a recolha de imagem (fotografia ou vídeo) e voz para efeitos de divulgação da participação do meu educando em atividades (divulgação em jornais, páginas Web ou redes socias, incluindo a possibilidade de divulgação de nome e imagem/voz, no caso de participações individuais) e a publicação, na página Web do “Ler é um risco/Arriscas-te?!” de trabalhos que o meu educando produza nas atividades escolares.