AGRUPAMENTO DE ESCOLAS DO FORTE DA CASA

ANEXO 17 – POLÍTICAS DE SEGURANÇA DIGITAL

Índice

1. Objetivos e âmbito da Política de Segurança Digital

O Agrupamento de Escolas do Forte da Casa, adiante designado apenas por AEFC, reconhece que a Segurança Digital é um elemento fundamental na salvaguarda das crianças, jovens e adultos que, diariamente, utilizam tecnologias, como computadores, tablets, telemóveis e/ou outros dispositivos similares. Esta utilização, para além das oportunidades de aprendizagem que lhes proporciona, pode também colocá-los em perigo.

A segurança digital abrange questões relacionadas com todos os elementos da comunidade escolar e com a utilização que é feita da Internet e de todos os dispositivos eletrónicos que permitem a comunicação em ambiente escolar e fora dele. Assim, é necessário que todos os educadores e professores tenham consciência da importância das práticas de segurança digital, visando a educação, a proteção e a formação das crianças e jovens na utilização correta e adequada 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.

Em anexo encontra-se a "Política de Privacidade e Proteção de Dados Pessoais", onde são abordadas pormenorizadamente as questões relativas à disponibilização dos dados pessoais dos alunos.

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

- Garantir que o AEFC tem um ambiente seguro no que concerne à utilização de equipamentos eletrónicos, assim como da Internet, por parte de todos os membros da comunidade;
- Sensibilizar todos os membros do AEFC para os benefícios da utilização das tecnologias, bem como para os seus potenciais riscos;
- Identificar procedimentos claros a adotar, de forma a responder às preocupações de segurança online que são conhecidos por todos os membros da comunidade;
- Permitir que todos os funcionários trabalhem com segurança e responsabilidade, adotando um modelo comportamental online positivo, estando cientes da necessidade de gerir os seus próprios padrões e práticas na utilização das tecnologias.

A PSD aplica-se a todos os funcionários, incluindo o órgão de gestão, professores, pessoal não docente, prestadores de serviços, visitantes e outras pessoas que trabalham para ou prestam

serviços em nome do AEFC (coletivamente e adiante referidos como pessoal), bem como alunos e pais ou encarregados de educação.

Esta Política aplica-se a todos os dispositivos de acesso à Internet e utilização de dispositivos de comunicação e informação, incluindo dispositivos pessoais, ou outros que tenham sido fornecidos a alunos, funcionários ou outras pessoas.

Redação e revisão da PSD:

- A definição, coordenação e implementação da PSD são da responsabilidade do Diretor, o qual deve nomear um Coordenador de Segurança Digital;
- A PSD foi redigida pelo AEFC, tendo por base a Política do Selo de Segurança Digital e a legislação em vigor.

2. A importância da utilização da Internet

- Devendo fazer parte integrante do currículo como uma ferramenta essencial no apoio à aprendizagem, a utilização da Internet no AEFC 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 proporcionado aos alunos, sempre que possível, e estes deverão fazê-lo de forma responsável.
- 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.
- O acesso à Internet faz-se preferencialmente pela VLAN reservada para esse efeito na rede **minedu**, de modo a não pôr em causa a segurança dos dados dos alunos, professores, dos serviços administrativos e da Direção.
- 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 e devem ser adequadas, pelos professores, às diferentes faixas etárias.
- Todas as atividades escolares que impliquem o uso da Internet devem integrar a

apresentação de referências bibliográficas normalizadas.

3. Gestão de sistemas de informação

3.1. Manutenção da segurança dos sistemas de informação

- A segurança dos sistemas informáticos do AEFC e dos utilizadores será revista regularmente;
- Os dados pessoais enviados através da Internet ou transferidos para fora da escola estão protegidos pelos sistemas de segurança dos programas utilizados, sendo esta garantida pelo fornecedor do serviço/programa;
- A instalação de software para fins educativos nos computadores de secretária e portáteis propriedade do AEFC deve ser autorizada pelo Coordenador da Segurança Digital;
- Os utilizadores não devem colocar / deixar ficheiros de uso pessoal nos PC ou nos dispositivos móveis propriedade do AEFC. 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 e nos computadores partilhados é realizada uma manutenção que inclui a eliminação de todos os ficheiros, dados e contas dos utilizadores;
- É obrigatória a utilização de nomes de utilizador e palavras-passe para aceder aos servidores e respetivos serviços da escola;
- A página inicial de navegação de cada PC ao serviço dos utilizadores será definida, de acordo com as necessidades / interesses dos serviços. Os utilizadores não devem, em circunstância alguma, alterar as páginas de navegação pré-definidas;
- O abandono do computador sem terminar a respetiva sessão também implica que assumirá a responsabilidade por todas as ações realizadas por terceiros na sua conta.
- Os utilizadores devem manter os seus dados atualizados e com cópias de segurança, evitando a perda de informações valiosas.

3.2. A gestão do correio eletrónico

- O AEFC disponibiliza contas de correio eletrónicas institucionais (@aefc.edu.pt) aos professores e funcionários e a comunicação institucional é feita por esta via;
- A comunicação com instituições para tratamento de assuntos oficiais do AEFC deve ser realizada a partir de endereços eletrónicos institucionais;
- Os grupos de contactos de correio eletrónico são geridos centralmente com o objetivo de facilitar o trabalho dos utilizadores;
- A troca de mensagens com os alunos deve ser feita preferencialmente através das contas de endereços eletrónicos institucionais;
- A troca de mensagens com encarregados de educação é feita pelo Diretor de Turma, para as contas pessoais dos Encarregados de Educação, que foram inseridas no programa Inovar ou transmitidas diretamente ao Diretor de Turma;
- 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 AEFC devem constar a morada, os números de telefone e o email oficial do AEFC. Não deve ser publicada qualquer informação pessoal de alunos ou professores;
- Não serão publicadas pautas e listagens de turma online e as pautas e listas afixadas em papel nos locais destinados para o efeito e 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 AEFC na Internet e deve assegurar que os conteúdos publicados são corretos e adequados;
- Todas as publicações em formato digital da responsabilidade do AEFC devem respeitar os direitos de propriedade intelectual, as políticas de privacidade e os direitos de autor.

3.4. Publicação de fotografias, de gravações de voz e de trabalhos de alunos

- 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 só são admissíveis se não houver uma relação direta entre a imagem e o som e o nome dos alunos, reduzindo, assim, significativamente, a possibilidade de identificação dos mesmos;
- A captação de imagens dos alunos deve, preferencialmente, ser executada de longe ou de ângulos que reduzam significativamente a possibilidade de identificação;
- Os professores não devem recolher imagens ou voz dos alunos com os seus dispositivos pessoais e não podem publicar diretamente imagens ou outros registos dos alunos nas suas redes sociais pessoais;
- O consentimento por escrito será mantido pelo agrupamento, 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 online com a autorização dos mesmos e dos pais / encarregados de educação das crianças e devem ter em conta as referências bibliográficas e os direitos de autor.

3.5. Gestão de comunicações virtuais, redes sociais e publicações pessoais

- Através de atividades dinamizadas pelos professores em sala de aula, nomeadamente nas aulas de TIC, e pelo Serviço das Bibliotecas Escolares, os alunos serão instruídos 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;
- Através da página Web do AEFC, serão feitas algumas campanhas de sensibilização de pais / encarregados de educação sobre a utilização segura de redes sociais e outros sítios de publicação de dados pessoais (dentro ou fora da escola), especialmente para os alunos mais novos. Estas ações de sensibilização para o uso seguro da Internet podem

vir a ser organizadas em colaboração com as Bibliotecas Escolares do Agrupamento e as Associações de Pais e Encarregados de Educação do AEFC.

3.6. Gestão dos sistemas de filtragem

- O acesso à Internet fornecido pelo AEFC inclui sistemas de filtragem de conteúdos impróprios, implementados centralmente pela Direção-Geral de Estatísticas da Educação e Ciência, que fornece o acesso à Internet e garante a manutenção regular destes sistemas de filtragem;
- 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;
- Os professores que encontrarem sites bloqueados com interesse pedagógico ou sites impróprios que se encontrem desbloqueados devem fazer chegar essa informação à Direção de modo a poder fazer-se o pedido de atualização à Direção-Geral de Estatísticas da Educação e Ciência.

3.7. Regras de acesso aos programas informáticos

O acesso aos Programas Informáticos rege-se, genericamente, pelas seguintes normas:

1. A gestão da rede e software é da responsabilidade do membro da Direção nomeado para o efeito que, para tal, pode criar uma equipa constituída por professores e funcionários;
2. Alterações à rede ou configurações passam por pedido aos gestores da rede e autorização do Diretor da Escola;
3. As atualizações dos programas administrativos são realizadas pelos gestores da rede e software ou pela empresa fornecedora do software/serviço;
4. Os equipamentos ativos de rede e os servidores encontram-se alojados em locais com acesso restrito e fechado. Os servidores estão colocados num bastidor e ligados a uma UPS para evitar quebras em caso de falha de energia. Os servidores estão configurados em RAID;
5. No servidor foi instalado o domínio Active Directory (AD) no qual estão criados os utilizadores e os computadores, seguindo as orientações emanadas pela DGEEC;
6. A escola possui um servidor RADIUS (instalado no âmbito do PTE e localizado no

bastidor) para controlo de acesso à rede (Wired e Wireless) e utiliza várias VLAN de acordo com o estipulado pela matriz de coletividade do plano PTE;

7. Existe um utilizador Administrador do Domínio que o controla;
8. Cada Assistente Técnico tem um nome de utilizador e uma palavra-passe para acesso ao computador, entrando como utilizador autenticado no AD;
9. Os computadores estão protegidos com programas antivírus;
10. As bases de dados dos programas administrativos e de gestão pedagógica estão alojadas nos servidores próprios da empresa que fornece o serviço, tendo estes sido contratualizados pela autarquia;
11. Existe uma base de dados que contém as palavras-passe de administrador dos diferentes programas. No cofre encontra-se, à responsabilidade do Diretor, a chave de acesso à mesma;
12. Anualmente (ou sempre que se revelar necessário) os acessos dos professores e diretores de turma são atualizados de acordo com a distribuição de serviço;
13. O acesso pelos Assistentes Técnicos aos programas, bem como os privilégios de que dispõem, depende do serviço que lhes é atribuído pelo Diretor e é-lhes concedido a qualquer momento, mediante informação fornecida pelo mesmo;
14. Os acessos criados anualmente nos programas para os Diretores de turma e professores, assim como nos dos Serviços Administrativos, são entregues pessoalmente;
15. As cópias de segurança dos programas alojados no servidor AD do Agrupamento são feitas automaticamente pelos programas e alojadas no servidor. Simultaneamente são realizadas cópias de segurança dos servidores para um NAS;
16. As cópias de segurança dos programas contratualizados pela autarquia não são da responsabilidade do Agrupamento;
17. Não existe permissão para alojar nem instalar programas nos computadores da Escola. Tal acesso passa por pedido aos gestores da rede;
18. Para acesso aos programas do Inovar são definidos login e uma password. É comunicado ao utilizador de uma forma segura quais são os acessos iniciais, dispondo o utilizador, na área reservada, de instruções para alterar a sua senha, sendo que esta deverá ser alterada, pelo menos com a periodicidade pedida pelo programa.

4. Decisões quanto às políticas

4.1. Autorização do acesso à Internet

- Pessoal docente, não docente e alunos estão autorizados a aceder à Internet, desde o que o façam de forma responsável e no âmbito das suas funções;
- No ato da matrícula, os pais / encarregados de educação terão conhecimento da Política de Segurança Digital e da Política de Privacidade e Proteção de Dados Pessoais, disponíveis na página da internet do AEFC e serão incentivados a analisá-los com os seus educandos.

4.2. Resolução de incidente relativos à Segurança Digital

- Todos os elementos do AEFC deverão informar o Diretor ou 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.);
- O Diretor, em articulação com o Coordenador da Segurança Digital, tomará as providências necessárias para resolver os incidentes de segurança digital, nomeadamente nos casos de cyberbullying;
- 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, pessoal docente 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 AEFC contactará a Comissão Nacional de Promoção dos Direitos e Proteção das Crianças e Jovens, através da Direção, e encaminhará a situação para as autoridades competentes.

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;

- Aos alunos serão disponibilizadas atividades e sessões de sensibilização para as questões do cyberbullying, dinamizadas por diferentes entidades do AEFC;
- Todos os incidentes de cyberbullying comunicados serão investigados, aplicando-se, quando necessário, os procedimentos de inquirição usados nos processos disciplinares, de acordo com o estabelecido no Regulamento Interno;
- As sanções para os envolvidos em cyberbullying podem incluir:
  - A 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;
  - Os pais / encarregados de educação serão informados da sanção aplicada;
  - As autoridades competentes serão contactadas, caso se suspeite de ação ilícita.

4.4. Gestão de telemóveis e equipamentos pessoais

- Em sessões de sensibilização e atividades dirigidas a alunos, dinamizadas, quando possível, em articulação com as atividades curriculares, os alunos serão instruídos quanto à utilização segura e adequada de telemóveis e outros equipamentos pessoais e serão sensibilizados para os limites e consequências dos seus atos;
- Os telemóveis ou equipamentos pessoais não podem ser utilizados durante as aulas ou tempos letivos formais (devendo, por isso, estar desligados), 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, equipamentos pessoais, captação de imagens/sons que ponham em causa a privacidade de terceiros, (como por exemplo, vestiários ou casas de banho);
- 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, corredores 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 utilizar os seus telemóveis ou equipamentos pessoais para contactar crianças, jovens ou os 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;
- Sempre que for necessário contactar alunos ou pais/encarregados de educação, deverão usar o telefone da escola;
- Os telemóveis e outros equipamentos estarão desligados ou em modo de "silêncio", a comunicação Bluetooth estará “oculta” ou desligada e os telemóveis e outros equipamentos não serão utilizados em períodos letivos, exceto em situações de emergência, ou em atividades pedagógicas, desde que haja consentimento para tal de todas as partes envolvidas na atividade.

5. Conhecimento das políticas por parte da Comunidade Escolar

- A PSD está disponível, para conhecimento e consulta, na página de internet do AEFC.
- O AEFC incentiva os docentes da escola a frequentar formação atualizada e adequada sobre a utilização segura e responsável da Internet, disponibilizada pelo Centro de Formação, e a promover atividades de esclarecimento junto do pessoal não docente, alunos e pais / encarregados de educação;
- O AEFC sensibilizará os pais e alunos para a sua PSD, através de boletins informativos, de um boletim a ser entregue no momento da matrícula, das reuniões regulares com os diretores de turma e da disponibilização da informação na sua plataforma oficial na Internet.

ANEXO

Política de Privacidade e de Proteção de Dados Pessoais do Agrupamento de Escolas do Forte da Casa

Introdução

O Regulamento Geral sobre Proteção de Dados Pessoais da União Europeia (RGPD) – Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho de 27 de abril de 2016, estabelece as regras relativas à proteção de dados pessoais de pessoas singulares, sendo aplicável diretamente na ordem jurídica de todos os Estados-Membros, e impondo uma série de deveres que se destinam, designadamente, a pessoas coletivas públicas. Em Portugal, encontra-se ainda em vigor a Lei n.º 58/2019, de 8 de agosto, que assegura a execução do RGPD.

A Lei nº 67/98, de 26 de outubro, sobre a proteção de dados, aplica-se, nomeadamente, à videovigilância e outras formas de captação, tratamento e difusão de sons e imagens que permitam identificar pessoas, sempre que o responsável pelo tratamento esteja domiciliado ou sediado em Portugal ou utilize um fornecedor de acesso a redes informáticas e telemáticas.

A Lei n.º 103/2015, de 24 de agosto, cria o sistema de registo de identificação criminal de condenados pela prática de crimes contra a autodeterminação sexual e a liberdade sexual de menores. Adicionalmente, a Lei n.º 51/2012, de 5 de setembro (Estatuto do Aluno e Ética Escolar), e o regulamento (UE) N.º 2016/679, de 27 de abril de 2016 estabelecem disposições especificas sobre o tratamento de dados pessoais e à livre circulação desses dados.

A deliberação n.º 1495/2016, de 6 de setembro, define orientações precisas sobre os limites legais para a recolha e tratamento de dados pessoais dos alunos e demais elementos da comunidade educativa.

O AEFC é um serviço integrante da Administração Direta do Estado, comprometido com a proteção dos dados pessoais dos cidadãos – muito em particular, daqueles que com ele se relacionam. Por isso, foi definida a presente Política de Privacidade e tratamento de dados.

Âmbito

A Política de Privacidade aplica-se aos dados recolhidos e tratados pelo AEFC no exercício das suas atribuições, designadamente através do Portal «Certifica», na representação e participação formal em órgãos institucionais, fóruns decisórios, plataformas online, grupos de trabalho e redes de cooperação, tanto a nível nacional e internacional, ou ainda no âmbito de comunicações ou requerimentos dirigidos ao agrupamento.

Dados Pessoais

Consideram-se «dados pessoais» quaisquer informações relativas a uma pessoa singular identificada ou identificável. É considerada identificável a pessoa singular que possa ser identificada, direta ou indiretamente, especialmente através de um referenciador, como o nome, dados de localização ou elementos específicos da integridade física, fisiológica, entre outros.

As tipologias concretas de dados pessoais objeto de tratamento pelo AEFC encontram-se diretamente relacionados com as suas atribuições e incluem entre outros: nome, idade ou data de nascimento, número de identificação civil, NIF, NISS, morada, correio eletrónico, número de telefone ou telemóvel, categoria profissional ou cargo desempenhado, serviço onde se desempenham funções.

Outras definições relevantes

No contexto desta Política, há outros conceitos cuja definição se torna essencial para garantir uma compreensão clara. Assim, destacam-se:

a) **Tratamento** – designa qualquer operação ou um conjunto de operações realizadas sobre dados pessoais, por meios automatizados ou não, tais como a recolha, registo, organização, apagamento ou alteração;

b) **Responsável pelo Tratamento** – refere-se à entidade, seja pessoa singular ou coletiva, autoridade pública, agência ou outro organismo que, individualmente ou em conjunto com outros, determina as finalidades e os meios de tratamento dos dados pessoais;

c) **Consentimento** – corresponde a uma manifestação de vontade, livre, específica, informada e inequívoca, através do qual o titular dos dados concorda, mediante declaração ou ato positivo claro, com o tratamento dos seus dados.

Fundamento e Finalidade do tratamento de dados pessoais

O AEFC procede à recolha e tratamento de dados pessoais com o objetivo de executar as suas atribuições e funções, incluindo:

- Cumprimento de obrigações legais ou regulamentares;
- Processamento de pedidos e requerimentos submetidos por cidadãos ou entidades;
- Resposta consultas e comunicações recebidas;
- Gestão de processos de candidatura ou recrutamento;
- Aplicação de formulários ou questionários, como instrumentos de avaliação de satisfação de serviços;
- Inscrição de participantes em eventos promovidos pela organização, como oficinas, seminários, congressos, plataformas online ou ações semelhantes.
- Recolha de indicadores e informações relevantes para a análise de atividade.

O tratamento de dados pessoais será realizado com base em fundamentos legais ou contratuais, ou ainda o consentimento do titular, que deverá ser sempre livre, específico, informado e inequívoco. Adicionalmente, todas as operações de tratamento serão executadas em rigorosa conformidade com os princípios jurídicos aplicáveis, assegurando transparência, lealdade, limitação das finalidades, minimização de dados, entre outros.

Partilha e divulgação dos dados

O Agrupamento apenas partilha dados pessoais com terceiros se houver fundamento legal que o justifique, como o consentimento explícito do titular, o cumprimento de obrigações legais ou o exercício de funções de interesse púbico.

Em qualquer outra circunstância, os dados pessoais não são transmitidos, vendidos ou trocados com terceiros, sendo exclusivamente armazenados e tratados dentro da infraestrutura tecnológica do Agrupamento.

Conservação dos dados

Os dados pessoais recolhidos e tratados são conservados apenas pelo período estipulado na legislação aplicável ou, na ausência de regulamentação especifica, pelo tempo estritamente

necessário para a execução das finalidades que motivaram a sua recolha.

Segurança dos dados pessoais

O AEFC compromete-se a assegurar a proteção e segurança dos dados pessoais, implementando medidas técnicas e organizativas adequadas para prevenir acessos não autorizados, alterações, divulgações ou destruições indevidas de dados.

Política de cookies

O AEFC utiliza cookies nos seus websites para otimizar a experiência dos visitantes e melhorar o desempenho das plataformas digitais.

Cookies são pequenos ficheiros de texto que, ao visitar um website, são armazenados no computador ou dispositivo móvel do utilizador por meio de navegador de internet (browser). Esses ficheiros permitem que o website reconheça o dispositivo em visitas futuras, proporcionando uma navegação mais personalizada e eficiente.

Os cookies utilizados não recolhem informações que identifiquem diretamente os visitantes. Eles recolhem dados genéricos, como o modo de acesso ao site, a localização aproximada (país ou região) e as páginas visualizadas, sendo utilizados exclusivamente para fins estatísticos e de melhoria do desempenho do website.

A qualquer momento o utilizador pode, através do seu navegador de internet (browser), decidir ser notificado sobre a receção de cookies, bem como bloquear a respetiva entrada no seu sistema.

A recusa de uso de cookies no site, pode resultar na impossibilidade de ter acesso a algumas das suas áreas ou de receber informação personalizada.

Os cookies são usados para ajudar a determinar a autenticidade, utilidade, interesse e o número de utilizações dos websites, permitindo uma navegação mais rápida e eficiente e eliminando a necessidade de introduzir repetidamente as mesmas informações.

Os nossos cookies têm diferentes funções:

- Cookies essenciais necessários para aceder a áreas específicas do website. Permitindo funcionalidades como login em áreas reservadas. Sem estes cookies, certos serviços não podem ser disponibilizados.
- Cookies analíticos – Permitem analisar o comportamento dos utilizadores e monitorizar a

performance do website, ajudando a melhorar a qualidade da navegação e a corrigir eventuais problemas. Estes cookies são utilizados apenas para estatísticas e não recolhem informações pessoais.

- Cookies de funcionalidade – Facilitam a personalização da experiência do utilizador, permitindo, por exemplo, o armazenamento de preferências de navegação ou a eliminação da necessidade de introduzir informações repetidas vezes. Os utilizadores podem, a qualquer momento, configurar o navegador para ser notificado sobre a receção de cookies ou bloqueá-los. Contudo a recusa de cookies pode limitar o acesso a algumas funcionalidades do website ou a conteúdos personalizados. Os cookies ajudam a garantir uma experiência de navegação mais eficiente e adaptada às necessidades dos utilizadores, contribuindo para a autenticação funcionalidade e desempenho do website.

Tipos de cookies utilizados:

- **Cookies permanentes** - Armazenados no navegador de internet (browser) nos dispositivos de acesso do utilizador (PC, mobile e tablet). São ativados sempre que o utilizador retorna ao site e utilizados para direcionar a navegação de acordo com os interesses do visitante, oferecendo uma experiência personalizada.
- **Cookies de sessão** – Temporários, permanecem ativos apenas durante a sessão de navegação, sendo removidos assim que o utilizador fecha o navegador. Estes cookies ajudam a identificar problemas e a melhorar a experiência de navegação.
- Mesmo após autorizar o uso de cookies, o utilizador pode desativar total ou parcialmente os cookies a qualquer momento, configurando as definições do navegador. Contudo, a desativação pode comprometer o funcionamento de algumas áreas do website.

Mais informações sobre cookies podem ser encontradas em: www.allaboutcookies.org

Direitos dos utilizadores em relação aos dados

O titular dos dados tem o direito de solicitar ao AEFC o acesso aos dados pessoais que lhe digam respeito, à sua retificação ou ao seu apagamento, à observância da limitação do tratamento dos seus dados e à portabilidade dos dados quando tecnicamente viável. O titular dos dados pode opor-se ao tratamento ou retirar, em qualquer momento, o consentimento previamente dado.

Como pode exercer os direitos:

Para exercer esses direitos, os titulares dos dados devem contactar o Encarregado da Proteção de Dados através do e-mail: oficial@aefc.edu.pt.

Responsável pela recolha e tratamento dos dados

O AEFC, pessoa coletiva n.º 600080226 com sede na Rua da República, 2626-503 Forte da Casa, é, para efeitos da legislação aplicável, o responsável pela recolha e tratamento dos dados.

Cabe ao responsável pelo tratamento dos dados aplicar as medidas técnicas e organizativas que forem adequadas para assegurar e estar em condições de comprovar que a recolha e o tratamento de dados pessoais são feitos em cumprimento das regras que resultam do RGPD e da respetiva Lei de Execução.

Alterações à Política de Privacidade

A Política de Privacidade e de Proteção de Dados Pessoais ora definida, pode ser alterada periodicamente sem necessidade de prévio consentimento do titular dos dados. Quaisquer alterações significativas serão comunicadas com o mesmo grau de publicidade que presidiu à divulgação da sua versão inicial.

Política interna de privacidade e de disponibilização de dados pessoais de alunos

O presente documento visa definir uma política interna sobre as condições exigíveis para a disponibilização de dados pessoais nas plataformas *online* do Agrupamento, com particular destaque para as áreas reservadas, bem como para a segregação da informação em função da finalidade, no que respeita às escolas do 1.º, 2.º e 3.º ciclos do ensino básico e no ensino secundário, nas matérias que lhes sejam aplicáveis.

Ressalva-se que apenas se aprecia aqui a operação sobre dados pessoais em que se traduz a disponibilização dos mesmos na Internet, para efeito do acesso aos mesmos pelo próprio ou por terceiros, **não sendo aqui objeto de análise o acesso aos dados pessoais dos alunos conservados pelas escolas.**

Condições de legitimidade para a disponibilização de dados pessoais na internet

A escola reconhece a importância da Internet para a circulação de informações e para a divulgação de atividades que enriquecem o currículo dos alunos e promovem boas práticas. Contudo, essas ações devem observar o disposto na Lei n.º 67/98, de 26 de outubro, e na sua versão atualizada pela Lei n.º 103/2015, de 24 de agosto (Lei de Proteção de Dados Pessoais - LPDP). De acordo com o artigo 7.º, n.º 1 da LPDP, os dados pessoais dos alunos são considerados informações sensíveis, devendo ser tratados com especial cuidado.

Consentimento para Tratamento de Dados

No caso de alunos menores de idade, o consentimento para o tratamento dos seus dados deve ser obtido junto dos respetivos encarregados de educação, nos termos do artigo 43.º, n.º 4 da Lei n.º 51/2012, de 5 de setembro (Estatuto do Aluno e Ética Escolar). A consulta aos próprios alunos também é recomendada, em função da sua idade e grau de maturidade.

Situações que decorrem do dever de publicidade e a sua concretização: Afixação das pautas de classificações; afixação de listagem dos alunos matriculados ou que requereram matrícula (artigo 24.º, n.º 5, do Despacho normativo n.º 1-F/2016, de 5 de abril, Artigo 14.º do Despacho normativo n.º 7-B/2015, de 7 de maio);

Pautas de avaliação

As pautas devem ser afixadas em local apropriado no interior da escola, contendo apenas a identificação do aluno, ano, turma, e classificações por disciplina. Não devem incluir informações sobre faltas, apoio social escolar ou qualquer outro dado excessivo. A sua disponibilização na Internet em página de acesso livre é proibida. Contudo, é permitida em área reservada e autenticada, como na plataforma **INOVAR – CONSULTA ALUNOS**, com acesso seguro (SSL). A conservação desses dados na área reservada deve limitar-se ao final do ano letivo correspondente, garantindo o apagamento eficaz após esse período.

Listagens de alunos

No caso da divulgação das listas de crianças e alunos que requereram ou a quem foi renovada a

matrícula, determina-se o seguinte: A afixação tem lugar no local destinado para o efeito, no interior da escola. Nas listas de matrícula é apenas permitido para identificar as crianças/alunos matriculados, o nome completo, o estado da matrícula, nível de escolaridade e turma de colocação. Não é permitida a sua divulgação na página da Internet do Agrupamento, de acesso livre, sendo, no entanto, permitida a sua publicação através da plataforma digital do Agrupamento, desde que respeitados os requisitos de segurança atrás enunciados (controlo rigoroso de utilizadores registados e mecanismos de autenticação).

Outros dados pessoais do processo individual do aluno

Considerando-se a sensibilidade da informação pessoal relativa a crianças e jovens e o impacto que a sua publicação *online* pode ter no seu desenvolvimento pessoal e na sua segurança deve ter-se em atenção o seguinte: Não há qualquer legitimidade para disponibilizar na Internet, em regime de livre acesso, os dados pessoais relacionados com a constituição das turmas, com a identificação do ano de escolaridade e da turma, o nome completo dos alunos, a sua idade, a opção pela disciplina de religião, horários das turmas e organização das atividades curriculares; incluem-se, também, neste tópico quaisquer dados relativos ao domicílio, ao percurso escolar, à situação socioeconómica, a existência de apoio social escolar, ao tipo e número de faltas dadas por disciplina, informação de saúde associada à justificação de faltas, a situação de deficiência, a medidas disciplinares, a referenciação pela Comissão de Proteção de Crianças e Jovens e a necessidades educativas especiais; os dados anteriormente referidos também não devem ser divulgados nos conselhos de turma onde estão presentes os representantes dos Encarregados de Educação e os delegado e subdelegado representantes dos alunos da turma; admite-se, no entanto, a disponibilização dos dados pessoais relativos às turmas, horários, atividades extracurriculares na Internet, em área reservada de acesso credenciado para a comunidade escolar, como é o caso do *INOVAR – CONSULTA ALUNOS*, delimitado no tempo, no máximo, até final do ano letivo correspondente.

Acresce que todos os dados anteriormente referidos se integram no processo individual do aluno, sobre o qual recai um dever de confidencialidade, conforme disposto no artigo 11.º, n.º 7, do Estatuto do Aluno, e estabelecendo o n.º 4 do mesmo artigo quem a ele tem acesso.

Publicação de imagens dos alunos

A maioria das atividades das escolas é dinamizada ou dirigida aos seus alunos, pelo que a divulgação de imagem, vídeo e som na Internet surge como forma de divulgar o trabalho realizado. Contudo, a imagem e voz dos alunos constituem dados pessoais que contribuem para a identificação de crianças e jovens, pelo que o Agrupamento deverá, no que respeita à publicação nos seus *sites* oficiais e nas plataformas *online* de trabalho curricular, extracurricular e/ou de projetos, tanto em sistema aberto como em área reservada mediante autenticação, observar o seguinte: A publicação de imagem e som dos alunos deve ser reduzida ao mínimo indispensável; no âmbito das atividades da escola é admissível a divulgação de imagens que não permitam a identificação das crianças e jovens; deve-se privilegiar a captação de imagens de longe e de ângulos em que as crianças não sejam facilmente identificáveis e suprimindo legendas que permitam a sua identificação.

Mesmo obedecendo ao anteriormente preceituado, é sempre necessário o consentimento prévio e informado dos encarregados de educação. Mesmo que as imagens não se destinem à divulgação na Internet, mas tenham uma utilização em circuito mais fechado ou fiquem apenas para arquivo ou exposição no espaço escolar, será sempre imprescindível obter o consentimento escrito do encarregado de educação, o qual deve ser previamente informado, de forma clara e transparente, sobre o contexto da captação, os fins e a utilização a ser dada às imagens.

No caso dos alunos de maior idade devem ser estes a assinar o referido consentimento informado. Os eventuais consentimentos que sejam obtidos dos encarregados de educação ou dos próprios jovens para a recolha de imagens devem passar a constar do processo individual do aluno.

A página da Internet das escolas como Portal de acesso

Acesso remoto dos docentes

Os docentes podem aceder ao sistema de informação interno do agrupamento (aplicações como **INOVAR** e Gestão Documental) através da Internet, desde que:

- Sejam utilizados mecanismos que garantam a confidencialidade das comunicações, como o protocolo **SSL (Secure Sockets Layer)**;
- Seja adotada uma política rigorosa de gestão de utilizadores, que inclua a atribuição de perfis de acesso. Essa política deve assegurar que o acesso a dados pessoais respeita o princípio da **necessidade de conhecer**, em função das funções desempenhadas e competências

atribuídas.

Os responsáveis pela gestão dessas plataformas devem implementar as seguintes medidas:

- **Prevenção de palavras-passe fracas**: Os utilizadores não devem ter a possibilidade de criar senhas com poucas letras, sem algarismos ou caracteres especiais.
- **Gestão eficiente de contas**: Deve haver procedimentos para desativar contas de utilizadores que não estejam mais ligados à instituição ou que tenham mudado de funções.

Plataformas de e-Learning

As plataformas eletrónicas de apoio ao ensino são ferramentas cada vez mais comuns na comunicação entre docentes e alunos. Elas permitem:

- A divulgação de informações e conteúdos programáticos;
- O acompanhamento das classificações dos alunos;
- O fomento de discussões entre alunos e professores em fóruns.

Dado que estas plataformas são projetadas para serem acessíveis remotamente, é essencial configurá-las de modo a garantir que apenas utilizadores autorizados, devidamente associados aos conteúdos, tenham acesso às informações disponibilizadas.

Disposições finais

O Agrupamento, através dos diferentes responsáveis, está obrigado, caso o titular dos dados o requeira, a permitir o acesso, retificação ou a eliminação dos dados facultados. Neste âmbito assumimos para com os utilizadores os seguintes compromissos: respeitar o sigilo profissional em relação aos dados tratados; assegurar o consentimento expresso do titular dos dados sempre que tal for exigido; proceder ao tratamento de dados de forma lícita e transparente, recolhendo apenas a informação necessária e pertinente à finalidade a que se destinam; permitir ao titular dos dados o acesso, atualização e correção das informações sobre si registadas; garantir o direito de eliminação dos dados utilizados quando requerida pelo titular; adotar medidas de segurança que impeçam a consulta, modificação, destruição ou adição dos dados por pessoa não autorizada a fazê-lo.