REGULAMENTO GERAL DE PROTEÇÃO DE DADOS DO AGRUPAMENTO DE ESCOLAS ALFREDO DA SILVA

Rua Carlos Lopes - Bairro da Tabaqueira – Albarraque 2635-209 Rio de Mouro
Tel: 219 156 510
www.aeass.pt

ÍNDICE

PREÂMBULO---- 4

CAPÍTULO I - Disposições Gerais---- 5
- **Artigo 1.º - Objeto**---- 5
- **Artigo 2.º - Âmbito de aplicação** ---- 5
- **Artigo 3.º - Enquadramento jurídico**---- 5
- **Artigo 4.º - Princípios gerais**---- 6
- **Artigo 5.º - Definições**---- 6
- **Artigo 6.º - Objetivos do Regulamento** ---- 7

CAPÍTULO II - Responsável pelo Tratamento e Encarregado da Proteção de Dados---- 7
- **Artigo 7.º - Responsável pelo tratamento**---- 7
- **Artigo 8.º - Encarregado da Proteção de Dados**---- 8
- **Artigo 9.º - Dever de cooperação**---- 8
- **Artigo 10.º - Dever de confidencialidade**---- 8
- **Artigo 11.º - Formação e sensibilização**---- 9

CAPÍTULO III - Tratamento de Dados Pessoais---- 9
- **Artigo 12.º - Princípios gerais do tratamento**---- 9
- **Artigo 13.º - Finalidades do tratamento**---- 9
- **Artigo 14.º - Bases de licitude do tratamento**---- 10
- **Artigo 15.º - Categorias de dados pessoais tratados**---- 10
- **Artigo 16.º - Categorias especiais de dados pessoais**---- 11
- **Artigo 17.º - Tratamento de dados pessoais de menores**---- 11
- **Artigo 18.º - Minimização e exatidão dos dados**---- 11
- **Artigo 19.º - Comunicação e transmissão de dados pessoais**---- 11
- **Artigo 20.º - Utilização de plataformas digitais**---- 12
- **Artigo 21.º - Utilização de correio eletrónico institucional**---- 12
- **Artigo 22.º - Tratamento de imagens e gravações**---- 12
- **Artigo 23.º - Tratamento de dados no âmbito da Educação Inclusiva**---- 13
- **Artigo 24.º - Dados relativos à saúde**---- 13
- **Artigo 25.º - Privacidade desde a conceção e por defeito**---- 13

CAPÍTULO IV - Direitos dos Titulares dos Dados---- 14
- **Artigo 26.º - Direitos dos titulares dos dados**---- 14
- **Artigo 27.º - Exercício dos direitos**---- 14
- **Artigo 28.º - Direito à informação**---- 14
- **Artigo 29.º - Direito de acesso**---- 15
- **Artigo 30.º - Direito de retificação**---- 15
- **Artigo 31.º - Direito ao apagamento e à limitação do tratamento**---- 15
- **Artigo 32.º - Direito de oposição**---- 15
- **Artigo 33.º - Reclamações**---- 15
- **Artigo 34.º - Dever de colaboração dos titulares dos dados**---- 15

CAPÍTULO V - Segurança da Informação e Medidas de Proteção---- 16
- **Artigo 35.º- Princípios gerais de segurança da informação**---- 16
- **Artigo 36.º - Controlo de acessos**---- 16
- **Artigo 37.º - Credenciais de autenticação**---- 16
- **Artigo 38.º - Utilização de equipamentos informáticos**---- 17
- **Artigo 39.º - Utilização de dispositivos móveis**---- 17

Artigo 40.º - Conservação e destruição segura da informação---- 17
Artigo 41.º - Boas práticas de segurança---- 17
Artigo 42.º - Cópias de segurança---- 18
CAPÍTULO VI - Violação de Dados Pessoais e Gestão de Incidentes---- 18
Artigo 43.º - Conceito de violação de dados pessoais---- 18
Artigo 44.º - Comunicação interna de incidentes---- 18
Artigo 45.º - Avaliação do incidente---- 19
Artigo 46.º - Notificação à autoridade de controlo---- 19
Artigo 47.º - Comunicação aos titulares dos dados---- 19
Artigo 48.º - Registo dos incidentes---- 19
Artigo 49.º - Medidas corretivas e preventivas---- 20
CAPÍTULO VII - Governação da Proteção de Dados e Responsabilidades Institucionais---- 20
Artigo 50.º - Princípio da responsabilidade institucional---- 20
Artigo 51.º - Competências do Diretor---- 21
Artigo 52.º - Encarregado da Proteção de Dados---- 21
Artigo 53.º - Competências dos Coordenadores---- 21
Artigo 54.º - Competências dos docentes---- 21
Artigo 55.º - Competências dos assistentes técnicos---- 22
Artigo 56.º - Competências dos assistentes operacionais---- 22
Artigo 57.º - Competências dos Diretores de Turma, Professores Titulares de Turma e Educadores de Infância---- 22
Artigo 58.º - Competências dos Serviços de Psicologia e Orientação e da Equipa Multidisciplinar de Apoio à Educação Inclusiva---- 23
Artigo 59.º - Competências dos serviços administrativos---- 23
Artigo 60.º - Competências do Coordenador TIC e dos administradores dos sistemas de informação---- 23
Artigo 61.º - Prestadores de serviços e subcontratantes---- 23
Artigo 62.º - Dever permanente de confidencialidade---- 24
CAPÍTULO VIII - Tecnologias Digitais, Inteligência Artificial e Proteção de Dados---- 24
Artigo 63.º - Princípios gerais de utilização das tecnologias digitais---- 24
Artigo 64.º - Utilização de plataformas digitais---- 24
Artigo 65.º - Utilização de sistemas de Inteligência Artificial---- 25
Artigo 66.º - Utilização responsável pelos trabalhadores---- 25
Artigo 67.º - Literacia digital e sensibilização---- 25
Artigo 68.º - Melhoria contínua---- 25
CAPÍTULO IX - Conservação, Arquivo e Eliminação de Dados---- 26
Artigo 69.º - Prazos de conservação---- 26
Artigo 70.º - Critérios de conservação---- 26
Artigo 71.º - Arquivo e organização da informação---- 26
Artigo 72.º - Eliminação e destruição de dados---- 26
CAPÍTULO X – Disposições finais e transitórias---- 27
Artigo 73.º - Regulamentos complementares---- 27
Artigo 74.º - Interpretação e integração de lacunas---- 27
Artigo 75.º - Revisão do Regulamento---- 27
Artigo 76.º - Entrada em vigor---- 27

ANEXOS

ANEXO I – POLÍTICA DE SEGURANÇA DA INFORMAÇÃO ---------- 28
ANEXO II – PROCEDIMENTOS DE GESTÃO DE INCIDENTES ---------- 28
ANEXO III – MATRIZ DE RESPONSABILIDADES (RACI) ---------- 29
ANEXO IV – TABELA DE RETENÇÃO DE DADOS ---------- 29
ANEXO V – POLÍTICA DE COOKIES ---------- 30
ANEXO VI – PROTEÇÃO DE DADOS EM PLATAFORMAS DIGITAIS ---------- 31

PREÂMBULO

A proteção dos dados pessoais constitui um direito fundamental consagrado no artigo 35.º da Constituição da República Portuguesa e na Carta dos Direitos Fundamentais da União Europeia, assumindo particular relevância no contexto da Administração Pública e, em especial, no âmbito do sistema educativo, onde são tratados dados pessoais de crianças, alunos, encarregados de educação, trabalhadores e demais membros da comunidade educativa.

O Agrupamento de Escolas Alfredo da Silva, enquanto estabelecimento público de educação e ensino integrado na rede pública do Ministério da Educação, Ciência e Inovação, procede diariamente ao tratamento de dados pessoais indispensáveis ao exercício das suas atribuições legais, designadamente no âmbito da gestão administrativa, pedagógica, financeira, dos recursos humanos, da ação social escolar, da educação inclusiva, da segurança escolar e da comunicação institucional.

O tratamento desses dados deve observar, em permanência, os princípios da licitude, lealdade, transparência, limitação das finalidades, minimização dos dados, exatidão, limitação da conservação, integridade, confidencialidade e responsabilidade (*accountability*), previstos no Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que respeita ao tratamento de dados pessoais e à livre circulação desses dados (Regulamento Geral sobre a Proteção de Dados – RGPD), bem como na Lei n.º 58/2019, de 8 de agosto, que assegura a sua execução na ordem jurídica nacional.

O presente Regulamento estabelece as normas internas aplicáveis ao tratamento de dados pessoais efetuado pelo Agrupamento de Escolas Alfredo da Silva, definindo os princípios, deveres, procedimentos e medidas organizativas destinados a garantir a proteção dos direitos e liberdades fundamentais dos titulares dos dados, promovendo uma cultura institucional de responsabilidade, segurança da informação, transparência e respeito pela privacidade.

Constituem ainda objetivos do presente Regulamento assegurar a conformidade das atividades desenvolvidas pelo Agrupamento com a legislação aplicável, reforçar a confiança da comunidade educativa no tratamento dos seus dados pessoais, promover boas práticas de segurança da informação e contribuir para uma gestão eficiente, responsável e ética dos recursos digitais e documentais da organização.

O presente Regulamento aplica-se a todos os órgãos de administração e gestão, estruturas intermédias, serviços administrativos, docentes, trabalhadores não docentes, alunos, encarregados de educação, colaboradores, prestadores de serviços e demais pessoas singulares ou coletivas que, no âmbito da sua relação com o Agrupamento, intervenham em operações de tratamento de dados pessoais.

A interpretação e aplicação do presente Regulamento obedecem ao disposto no Regulamento (UE) 2016/679, na Lei n.º 58/2019, de 8 de agosto, e demais legislação nacional e europeia aplicável em matéria de proteção de dados pessoais, segurança da informação, arquivo administrativo e administração eletrónica.

REGULAMENTO GERAL DE PROTEÇÃO DE DADOS

Agrupamento de Escolas Alfredo da Silva

CAPÍTULO I

Disposições Gerais

Artigo 1.º

Objeto

1. O presente Regulamento estabelece as normas internas aplicáveis ao tratamento de dados pessoais efetuado pelo Agrupamento de Escolas Alfredo da Silva, doravante designado por **AEAS**, em conformidade com o disposto no Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016 (Regulamento Geral sobre a Proteção de Dados – RGPD), na Lei n.º 58/2019, de 8 de agosto, e demais legislação nacional e europeia aplicável.
2. O presente Regulamento define os princípios, regras, procedimentos e medidas técnicas e organizativas destinados a assegurar a proteção dos direitos, liberdades e garantias das pessoas singulares relativamente ao tratamento dos seus dados pessoais.
3. O Regulamento visa promover uma cultura institucional de proteção de dados, privacidade, segurança da informação, transparência e responsabilidade, garantindo o cumprimento das obrigações legais aplicáveis ao AEAS.

Artigo 2.º

Âmbito de aplicação

1. O presente Regulamento aplica-se a todas as operações de tratamento de dados pessoais efetuadas pelo AEAS, independentemente do suporte utilizado, automatizado ou não automatizado.
2. As disposições do presente Regulamento aplicam-se a:
   a) Crianças e alunos da educação pré-escolar, do ensino básico e do ensino secundário;
   b) Pais, encarregados de educação e representantes legais;
   c) Docentes;
   d) Trabalhadores não docentes;
   e) Técnicos especializados;
   f) Psicólogos;
   g) Trabalhadores em funções públicas;
   h) Candidatos a procedimentos concursais;
   i) Prestadores de serviços;
   j) Estagiários;
   k) Visitantes, colaboradores e demais pessoas singulares que mantenham qualquer relação com o AEAS.
3. O presente Regulamento aplica-se igualmente aos subcontratantes que tratem dados pessoais por conta do AEAS, sem prejuízo das obrigações legais e contratuais que sobre eles impendam.

Artigo 3.º

Enquadramento jurídico

1. O tratamento de dados pessoais realizado pelo AEAS rege-se, designadamente, pelos seguintes diplomas:

a) Constituição da República Portuguesa;
b) Carta dos Direitos Fundamentais da União Europeia;
c) Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016 (RGPD);
d) Lei n.º 58/2019, de 8 de agosto;
e) Lei n.º 51/2012, de 5 de setembro, na sua redação atual (Estatuto do Aluno e Ética Escolar);
f) Decreto-Lei n.º 54/2018, de 6 de julho, na sua redação atual (Educação Inclusiva);
g) Decreto-Lei n.º 55/2018, de 6 de julho, na sua redação atual (Currículo dos Ensinos Básico e Secundário);
h) Decreto-Lei n.º 75/2008, de 22 de abril, na sua redação atual (Regime de autonomia, administração e gestão dos estabelecimentos públicos de educação pré-escolar e dos ensinos básico e secundário);
i) Demais legislação nacional e europeia aplicável ao tratamento de dados pessoais e à segurança da informação.

2. O AEAS observa igualmente as orientações emitidas pela Comissão Nacional de Proteção de Dados, pela Direção-Geral dos Estabelecimentos Escolares e por outras entidades competentes em matéria de proteção de dados.

Artigo 4.º

Princípios gerais

1. O tratamento de dados pessoais efetuado pelo AEAS obedece aos princípios da:
   a) **Licitude, lealdade e transparência** – O tratamento de dados será realizado de forma justa e transparente, garantindo que os titulares dos dados estão devidamente informados sobre as operações efetuadas.
   b) **Limitação da finalidade** – Os dados pessoais serão recolhidos apenas para finalidades específicas, explícitas e legítimas, não podendo ser tratados para fins incompatíveis.
   c) **Minimização de dados** – Apenas serão recolhidos os dados estritamente necessários para a realização das finalidades determinadas.
   d) **Exatidão** – Os dados serão mantidos corretos e atualizados sempre que necessário.
   e) **Limitação da conservação** – Os dados serão conservados apenas pelo período necessário para a sua finalidade.
   f) **Integridade e confidencialidade** – Estão asseguradas medidas de segurança adequadas contra acessos não autorizados, perdas ou violações.
2. Todos os tratamentos de dados pessoais devem limitar-se ao estritamente necessário para a prossecução das atribuições legais e das atividades educativas, administrativas e organizacionais do Agrupamento.
3. O AEAS assegura que os dados pessoais são tratados de forma adequada, pertinente e limitada ao necessário para as finalidades que justificaram a sua recolha.

Artigo 5.º

Definições

Para efeitos do presente Regulamento, entende-se por:

a) **Dados pessoais** – qualquer informação relativa a uma pessoa singular identificada ou identificável;
b) **Tratamento** – qualquer operação ou conjunto de operações efetuadas sobre dados pessoais, por meios automatizados ou não automatizados;

c) **Titular dos dados** – a pessoa singular a quem os dados pessoais dizem respeito;
d) **Responsável pelo tratamento** – o Agrupamento de Escolas Alfredo da Silva, representado pela Diretor, que determina as finalidades e os meios do tratamento;
e) **Subcontratante** – a pessoa singular ou coletiva que trate dados pessoais por conta do responsável pelo tratamento;
f) **Destinatário** – a pessoa singular ou coletiva, autoridade pública, serviço ou organismo a quem sejam comunicados dados pessoais;
g) **Categorias especiais de dados** – os dados previstos no artigo 9.º do RGPD, designadamente os relativos à saúde, origem racial ou étnica, convicções religiosas, dados biométricos, entre outros legalmente previstos;
h) **Violação de dados pessoais** – a violação de segurança que provoque, de modo acidental ou ilícito, a destruição, perda, alteração, divulgação ou acesso não autorizado a dados pessoais;
i) **Consentimento** – manifestação de vontade livre, específica, informada e inequívoca pela qual o titular aceita, mediante declaração ou ato positivo inequívoco, o tratamento dos seus dados pessoais.

Artigo 6.º

Objetivos do Regulamento

Constituem objetivos do presente Regulamento:

a) Assegurar o cumprimento da legislação relativa à proteção de dados pessoais;
b) Garantir a proteção dos direitos e liberdades fundamentais dos titulares dos dados;
c) Promover a transparência no tratamento de dados pessoais;
d) Reforçar a confiança da comunidade educativa na atuação do AEAS;
e) Implementar medidas de segurança adequadas à proteção da informação;
f) Promover boas práticas na utilização de sistemas de informação, plataformas digitais e recursos tecnológicos;
g) Sensibilizar toda a comunidade educativa para a importância da proteção de dados pessoais e da segurança da informação;
h) Promover uma cultura organizacional baseada na responsabilidade, na ética e na proteção da privacidade.

CAPÍTULO II

Responsável pelo Tratamento e Encarregado da Proteção de Dados

Artigo 7.º

Responsável pelo tratamento

1. O Agrupamento de Escolas Alfredo da Silva, representado pelo Diretor, é o responsável pelo tratamento dos dados pessoais efetuado no âmbito das suas atribuições legais e das atividades educativas, administrativas, financeiras e organizacionais que desenvolve.
2. Enquanto responsável pelo tratamento, compete ao AEAS:
   a) Assegurar que o tratamento dos dados pessoais é efetuado em conformidade com a legislação aplicável;
   b) Determinar as finalidades e os meios de tratamento dos dados pessoais;
   c) Implementar medidas técnicas e organizativas adequadas à proteção dos dados pessoais;
   d) Garantir o exercício dos direitos dos titulares dos dados;

e) Assegurar que os tratamentos efetuados respeitam os princípios da licitude, lealdade, transparência, minimização dos dados, limitação das finalidades, exatidão, limitação da conservação, integridade, confidencialidade e responsabilidade.

3. O AEAS promove uma cultura de proteção de dados pessoais, assegurando que todos os trabalhadores conhecem e cumprem as obrigações decorrentes do presente Regulamento.

Artigo 8.º

Encarregado da Proteção de Dados

1. O AEAS dispõe de Encarregado da Proteção de Dados (EPD), designado nos termos da legislação aplicável.
2. O EPD exerce as suas funções com independência, autonomia técnica e funcional, não podendo receber instruções relativamente ao exercício das competências que lhe são legalmente atribuídas.
3. Compete, designadamente, ao EPD:
   a) Informar e aconselhar o AEAS e os seus trabalhadores relativamente às obrigações decorrentes da legislação sobre proteção de dados;
   b) Controlar o cumprimento do presente Regulamento e da legislação aplicável;
   c) Sensibilizar e promover ações de formação em matéria de proteção de dados pessoais;
   d) Prestar aconselhamento sobre avaliações de impacto relativas à proteção de dados, sempre que aplicável;
   e) Cooperar com a Comissão Nacional de Proteção de Dados;
   f) Constituir o ponto de contacto entre o AEAS, os titulares dos dados e a autoridade de controlo.
4. Os contactos do Encarregado da Proteção de Dados são divulgados no sítio eletrónico do Agrupamento e nos restantes meios institucionais adequados.

Artigo 9.º

Dever de cooperação

1. Todos os trabalhadores, colaboradores e prestadores de serviços do AEAS devem cooperar com o Encarregado da Proteção de Dados no exercício das suas funções.
2. Sempre que solicitado, devem ser facultadas ao EPD todas as informações necessárias à verificação da conformidade dos tratamentos de dados pessoais.
3. Qualquer situação suscetível de constituir risco para a proteção dos dados pessoais deve ser comunicada, de imediato, ao superior hierárquico e ao Encarregado da Proteção de Dados.

Artigo 10.º

Dever de confidencialidade

1. Todas as pessoas que, no exercício das suas funções, tenham acesso a dados pessoais tratados pelo AEAS estão obrigadas ao dever de confidencialidade, mesmo após a cessação das respetivas funções.
2. O dever de confidencialidade abrange, designadamente:
   a) Dados relativos aos alunos e respetivos encarregados de educação;
   b) Dados dos trabalhadores;
   c) Dados de natureza disciplinar;
   d) Dados de saúde;
   e) Dados de ação social escolar;

f) Dados constantes de processos individuais;
g) Qualquer outra informação protegida por dever legal de sigilo.

3. A violação do dever de confidencialidade pode determinar responsabilidade disciplinar, civil, contraordenacional ou criminal, nos termos da legislação aplicável.

Artigo 11.º

Formação e sensibilização

1. O AEAS promove, de forma contínua, ações de informação, formação e sensibilização destinadas aos trabalhadores, colaboradores e demais intervenientes que tratem dados pessoais.
2. As ações de formação devem incidir, designadamente, sobre:
   a) Os princípios da proteção de dados pessoais;
   b) As boas práticas de segurança da informação;
   c) A utilização segura dos sistemas informáticos;
   d) A prevenção de incidentes de segurança;
   e) O tratamento adequado dos dados pessoais em contexto escolar;
   f) As responsabilidades individuais decorrentes da legislação aplicável.
3. A participação nas ações de formação promovidas pelo AEAS constitui um instrumento essencial para assegurar a conformidade legal e a melhoria contínua das práticas de proteção de dados.

CAPÍTULO III

Tratamento de Dados Pessoais

Artigo 12.º

Princípios gerais do tratamento

1. O tratamento de dados pessoais pelo Agrupamento de Escolas Alfredo da Silva observa, em todas as circunstâncias, os princípios previstos no Regulamento (UE) 2016/679, assegurando que os dados são:
   a) Tratados de forma lícita, leal e transparente;
   b) Recolhidos para finalidades determinadas, explícitas e legítimas;
   c) Adequados, pertinentes e limitados ao estritamente necessário para as finalidades que justificam o respetivo tratamento;
   d) Exatos e, sempre que necessário, atualizados;
   e) Conservados apenas durante o período necessário à prossecução das finalidades para que foram recolhidos ou pelo prazo legalmente estabelecido;
   f) Tratados de forma a garantir a sua segurança, integridade, disponibilidade e confidencialidade.
2. O AEAS adota medidas adequadas que permitam demonstrar o cumprimento dos princípios previstos no número anterior, em conformidade com o princípio da responsabilidade previsto no RGPD.

Artigo 13.º

Finalidades do tratamento

1. O tratamento de dados pessoais é efetuado exclusivamente para o exercício das competências legalmente atribuídas ao Agrupamento.
2. Constituem, designadamente, finalidades do tratamento:

a) Gestão do percurso escolar dos alunos;
b) Organização e funcionamento das atividades educativas;
c) Gestão pedagógica e avaliação;
d) Matrículas, transferências e certificação;
e) Educação inclusiva;
f) Apoio psicológico e serviços especializados;
g) Ação Social Escolar;
h) Gestão de recursos humanos;
i) Processamento remuneratório;
j) Gestão financeira e patrimonial;
k) Segurança de pessoas e bens;
l) Cumprimento de obrigações legais;
m) Comunicação institucional;
n) Organização de visitas de estudo, projetos e atividades complementares.

3. É proibido o tratamento de dados pessoais para finalidades incompatíveis com aquelas que determinaram a respetiva recolha, salvo quando exista fundamento legal bastante.

Artigo 14.º

Bases de licitude do tratamento

1. O tratamento de dados pessoais realizado pelo AEAS fundamenta-se nas bases de licitude previstas no artigo 6.º do RGPD.
2. O tratamento é efetuado, designadamente, quando:
   a) Seja necessário ao cumprimento de uma obrigação jurídica;
   b) Seja necessário ao exercício de funções de interesse público ou ao exercício da autoridade pública de que o Agrupamento está investido;
   c) Seja necessário para a execução de um contrato ou de diligências pré-contratuais;
   d) O titular tenha prestado consentimento, sempre que este constitua o fundamento legal adequado.
3. Sempre que o tratamento assente no consentimento, este deve ser livre, específico, informado, inequívoco e passível de retirada a todo o tempo, sem prejuízo da licitude do tratamento anteriormente efetuado.
4. O consentimento não será solicitado quando exista outra base jurídica que legitime o tratamento.

Artigo 15.º

Categorias de dados pessoais tratados

1. O AEAS trata apenas os dados pessoais estritamente necessários ao exercício das suas atribuições.
2. Podem ser tratados, designadamente:
   a) Dados de identificação;
   b) Dados de contacto;
   c) Dados académicos;
   d) Dados relativos à assiduidade;
   e) Dados de avaliação;
   f) Dados financeiros;
   g) Dados relativos à ação social escolar;

h) Dados de saúde, quando legalmente necessários;
i) Dados relativos à educação inclusiva;
j) Dados constantes dos processos individuais;
k) Imagens e gravações de vídeo, quando legalmente admissíveis.

Artigo 16.º

Categorias especiais de dados pessoais

1. O tratamento de categorias especiais de dados pessoais apenas é efetuado quando exista fundamento legal expresso e seja indispensável ao cumprimento das atribuições do Agrupamento.
2. São abrangidos pelo presente artigo, designadamente:
   a) Dados relativos à saúde;
   b) Dados necessários à implementação de medidas de suporte à aprendizagem e à inclusão;
   c) Dados relativos à segurança dos alunos;
   d) Outros dados previstos no artigo 9.º do RGPD.
3. O acesso a estas categorias de dados fica limitado aos trabalhadores que deles necessitem para o exercício das respetivas funções e está sujeito ao dever reforçado de confidencialidade.

Artigo 17.º

Tratamento de dados pessoais de menores

1. O tratamento de dados pessoais de crianças e alunos realiza-se no estrito respeito pelos princípios da proteção do superior interesse da criança, da proporcionalidade, da necessidade e da confidencialidade.
2. O AEAS assegura que os dados pessoais dos alunos são tratados exclusivamente para finalidades educativas, administrativas, legais ou de proteção social.
3. Sempre que a lei exija consentimento, este é prestado pelo titular das responsabilidades parentais ou por quem legalmente o represente.
4. Todos os trabalhadores devem adotar especiais deveres de diligência na proteção dos dados pessoais dos menores.

Artigo 18.º

Minimização e exatidão dos dados

1. O AEAS recolhe apenas os dados pessoais estritamente necessários para cada finalidade.
2. Sempre que possível, os dados são obtidos diretamente junto do respetivo titular ou do encarregado de educação.
3. Os titulares dos dados devem comunicar ao Agrupamento quaisquer alterações relevantes, de modo a garantir a permanente atualização da informação constante dos respetivos processos.

Artigo 19.º

Comunicação e transmissão de dados pessoais

1. A comunicação ou transmissão de dados pessoais a entidades externas apenas pode ocorrer quando:
   a) Seja imposta por disposição legal;
   b) Seja necessária ao exercício de competências legalmente atribuídas ao Agrupamento ou à entidade destinatária;

c) Tenha sido autorizada pelo titular dos dados, quando o consentimento constitua fundamento de licitude;

d) Seja indispensável à proteção de interesses vitais do titular dos dados ou de outra pessoa singular;

e) Exista outra base de licitude prevista no Regulamento (UE) 2016/679.

2. A transmissão de dados deve limitar-se aos estritamente necessários para a prossecução da finalidade que a justifica.
3. O AEAS assegura que todas as comunicações de dados pessoais são efetuadas através de meios que garantam níveis adequados de segurança e confidencialidade.
4. Sempre que legalmente exigível, as comunicações de dados pessoais são objeto de registo.

Artigo 20.º

Utilização de plataformas digitais

1. O AEAS utiliza plataformas digitais exclusivamente para fins educativos, pedagógicos, administrativos ou de gestão escolar.
2. A seleção das plataformas deve atender, designadamente:

   a) À conformidade com o Regulamento Geral sobre a Proteção de Dados;

   b) À segurança da informação;

   c) À proteção dos direitos dos titulares dos dados;

   d) À existência de mecanismos adequados de autenticação e controlo de acessos.
3. Sempre que possível, devem ser privilegiadas plataformas disponibilizadas ou autorizadas pelo Ministério da Educação, Ciência e Inovação ou por outras entidades públicas competentes.
4. A utilização de novas plataformas digitais que impliquem tratamentos de dados pessoais deve ser previamente analisada quanto aos respetivos riscos para a proteção de dados.

Artigo 21.º

Utilização de correio eletrónico institucional

1. O correio eletrónico institucional constitui um instrumento de trabalho destinado ao exercício das funções profissionais dos trabalhadores do Agrupamento.
2. Os utilizadores devem assegurar uma utilização responsável do correio eletrónico institucional, observando as normas de segurança da informação e proteção de dados pessoais.
3. É proibido:

   a) Divulgar dados pessoais a destinatários não autorizados;

   b) Enviar informação confidencial sem as adequadas medidas de proteção;

   c) Utilizar contas pessoais para transmissão de informação institucional que contenha dados pessoais, salvo autorização expressa da Direção e mediante adoção das medidas de segurança adequadas.
4. Sempre que possível, os ficheiros contendo dados pessoais devem ser protegidos através de mecanismos de encriptação ou palavra-passe.

Artigo 22.º

Tratamento de imagens e gravações

1. A captação, utilização e divulgação de imagens, vídeos ou gravações de voz de alunos, trabalhadores ou demais membros da comunidade educativa devem respeitar a legislação

aplicável em matéria de proteção de dados pessoais, direitos de personalidade e direito à imagem.

2. A recolha de imagens para fins pedagógicos, educativos, científicos ou de divulgação institucional deve observar os princípios da necessidade, proporcionalidade e minimização.
3. Sempre que o tratamento dependa de consentimento, este deve ser previamente obtido, de forma livre, específica, informada e inequívoca.
4. A divulgação de imagens através do sítio institucional, redes sociais ou outros meios de comunicação apenas pode ocorrer quando exista fundamento jurídico que a legitime e sejam adotadas as medidas adequadas de proteção dos direitos dos titulares.
5. É proibida a utilização de imagens recolhidas no âmbito das atividades escolares para fins comerciais, publicitários ou quaisquer outros incompatíveis com as finalidades que justificaram a respetiva recolha.

Artigo 23.º

Tratamento de dados no âmbito da Educação Inclusiva

1. Os dados pessoais tratados no âmbito das medidas de suporte à aprendizagem e à inclusão revestem natureza especialmente sensível e beneficiam de proteção reforçada.
2. O acesso a estes dados é restrito aos profissionais que deles necessitem para o exercício das respetivas funções.
3. A consulta, partilha ou reprodução destes elementos deve limitar-se ao estritamente necessário para assegurar a adequada resposta educativa ao aluno.
4. O tratamento destes dados observa, para além do RGPD, a legislação específica aplicável à educação inclusiva e ao acompanhamento multidisciplinar dos alunos.

Artigo 24.º

Dados relativos à saúde

1. O tratamento de dados relativos à saúde é efetuado apenas quando indispensável ao cumprimento de obrigações legais ou à salvaguarda da saúde, segurança e bem-estar dos alunos e trabalhadores.
2. O acesso a estes dados é limitado aos profissionais que deles necessitem para o exercício das respetivas competências.
3. Os dados relativos à saúde são conservados com especiais medidas de segurança física e lógica, prevenindo qualquer acesso indevido ou divulgação não autorizada.

Artigo 25.º

Privacidade desde a conceção e por defeito

1. O AEAS integra os princípios da proteção de dados desde a conceção e por defeito na implementação de novos procedimentos administrativos, projetos, plataformas digitais, aplicações informáticas e demais tratamentos de dados pessoais.
2. Sempre que sejam introduzidos novos sistemas de informação ou novas tecnologias suscetíveis de implicar riscos elevados para os direitos e liberdades dos titulares dos dados, devem ser previamente avaliadas as respetivas implicações em matéria de proteção de dados.
3. Na definição dos tratamentos devem ser adotadas, desde o início, medidas que assegurem a recolha apenas dos dados necessários, a limitação dos acessos, a proteção da informação e a conservação pelo período estritamente indispensável.

CAPÍTULO IV

Direitos dos Titulares dos Dados

Nota Introdutória

O presente capítulo estabelece os direitos dos titulares dos dados pessoais e define os procedimentos internos a observar pelo Agrupamento de Escolas Alfredo da Silva (AEAS) para assegurar o respetivo exercício, em conformidade com o Regulamento (UE) 2016/679, a Lei n.º 58/2019 e demais legislação aplicável.

Artigo 26.º

Direitos dos titulares dos dados

1. O AEAS garante aos titulares dos dados pessoais o exercício dos direitos previstos na legislação aplicável.
2. Constituem direitos dos titulares dos dados, designadamente:
   a) Direito à informação;
   b) Direito de acesso;
   c) Direito de retificação;
   d) Direito ao apagamento, quando legalmente aplicável;
   e) Direito à limitação do tratamento;
   f) Direito de oposição;
   g) Direito à portabilidade dos dados, nos casos legalmente previstos;
   h) Direito de não ficar sujeito a decisões exclusivamente automatizadas, quando aplicável.
3. O exercício destes direitos é gratuito, salvo nos casos previstos na lei.

Artigo 27.º

Exercício dos direitos

1. Os pedidos de exercício de direitos podem ser apresentados pelo titular dos dados, pelo respetivo representante legal ou por quem demonstre legitimidade para o efeito.
2. Os pedidos são dirigidos ao responsável pelo tratamento, podendo ser apresentados por escrito, por via eletrónica ou através dos meios disponibilizados pelo AEAS.
3. Sempre que existam dúvidas razoáveis quanto à identidade do requerente, pode ser solicitada prova da respetiva identidade.
4. O AEAS responde aos pedidos no prazo legalmente previsto, sem demora injustificada.

Artigo 28.º

Direito à informação

1. O AEAS assegura que os titulares dos dados recebem informação clara, acessível, transparente e adequada sobre o tratamento dos seus dados pessoais.
2. A informação referida no número anterior deve incluir, designadamente:
   a) A identidade do responsável pelo tratamento;
   b) As finalidades do tratamento;
   c) A base de licitude;
   d) O prazo de conservação dos dados;
   e) Os destinatários dos dados, quando existam;
   f) Os direitos dos titulares;
   g) Os contactos do Encarregado da Proteção de Dados.

Artigo 29.º

Direito de acesso

1. O titular dos dados tem o direito de obter confirmação sobre se os seus dados pessoais são objeto de tratamento.
2. Sempre que solicitado, o AEAS disponibiliza ao titular acesso aos respetivos dados pessoais, nos termos da legislação aplicável.
3. O direito de acesso pode ser limitado quando tal resulte de disposição legal expressa ou da necessidade de salvaguardar direitos e liberdades de terceiros.

Artigo 30.º

Direito de retificação

1. O titular dos dados pode solicitar a retificação dos dados pessoais inexatos ou incompletos.
2. O AEAS procede à retificação sem demora injustificada, desde que o pedido seja fundamentado e confirmado.

Artigo 31.º

Direito ao apagamento e à limitação do tratamento

1. O direito ao apagamento é exercido nos casos previstos no Regulamento (UE) 2016/679.
2. O direito ao apagamento não prejudica a conservação de dados quando esta resulte de obrigação legal, do exercício de funções de interesse público ou da necessidade de defesa de direitos em processo judicial.
3. Sempre que o apagamento não seja legalmente possível, o titular pode requerer, nos casos previstos na lei, a limitação do tratamento.

Artigo 32.º

Direito de oposição

1. O titular dos dados pode opor-se ao tratamento dos seus dados pessoais quando tal direito seja reconhecido pela legislação aplicável.
2. O AEAS aprecia cada pedido de oposição, ponderando os interesses públicos e as obrigações legais que fundamentam o tratamento.

Artigo 33.º

Reclamações

1. Sem prejuízo de qualquer outro meio administrativo ou judicial, os titulares dos dados têm o direito de apresentar reclamação junto da Comissão Nacional de Proteção de Dados.
2. O exercício do direito de reclamação não prejudica o recurso aos tribunais competentes nem aos demais meios de tutela previstos na lei.
3. O AEAS promove a resolução célere das questões suscitadas pelos titulares dos dados, privilegiando, sempre que possível, a resolução administrativa das situações comunicadas.

Artigo 34.º

Dever de colaboração dos titulares dos dados

1. Os titulares dos dados devem fornecer ao AEAS informações verdadeiras, completas e atualizadas.
2. Sempre que ocorram alterações relevantes, designadamente relativas à identificação, contactos, responsabilidades parentais ou outras informações necessárias ao

desenvolvimento da atividade educativa, devem as mesmas ser comunicadas ao Agrupamento com a maior brevidade possível.

3. O incumprimento do dever previsto no número anterior pode comprometer o adequado funcionamento dos serviços e a prossecução das atribuições legalmente cometidas ao AEAS.

CAPÍTULO V

Segurança da Informação e Medidas de Proteção

Nota Introdutória

A proteção dos dados pessoais depende da adoção de medidas técnicas e organizativas adequadas, destinadas a prevenir o acesso não autorizado, a perda, a destruição, a alteração ou a divulgação indevida da informação. O presente capítulo estabelece as regras de segurança da informação aplicáveis ao Agrupamento de Escolas Alfredo da Silva.

Artigo 35.º

Princípios gerais de segurança da informação

1. O AEAS adota medidas técnicas e organizativas adequadas para assegurar um nível de segurança apropriado ao risco associado ao tratamento de dados pessoais.
2. As medidas de segurança devem garantir, designadamente:
   a) A confidencialidade da informação;
   b) A integridade dos dados;
   c) A disponibilidade dos sistemas e serviços;
   d) A resiliência dos sistemas de informação;
   e) A capacidade de restaurar a disponibilidade dos dados em caso de incidente.
3. As medidas adotadas são revistas periodicamente, tendo em consideração a evolução tecnológica, os riscos identificados e as orientações das entidades competentes.

Artigo 36.º

Controlo de acessos

1. O acesso aos sistemas de informação do AEAS é concedido exclusivamente aos utilizadores que dele necessitem para o exercício das respetivas funções.
2. Os perfis de acesso são definidos de acordo com o princípio do menor privilégio, garantindo que cada utilizador apenas acede à informação indispensável ao desempenho das suas funções.
3. Os acessos atribuídos devem ser revistos periodicamente e sempre que ocorram alterações de funções, mobilidade ou cessação de vínculo.

Artigo 37.º

Credenciais de autenticação

1. Cada utilizador é responsável pela utilização das credenciais de autenticação que lhe sejam atribuídas.
2. As palavras-passe devem:
   a) Ser de utilização exclusivamente pessoal;
   b) Manter-se confidenciais;
   c) Possuir um nível adequado de complexidade;
   d) Ser alteradas sempre que exista suspeita de comprometimento.

3. É proibida a partilha de credenciais de acesso entre utilizadores.
4. Sempre que tecnicamente possível, devem ser utilizados mecanismos de autenticação multifator para o acesso aos sistemas que tratem dados pessoais.

Artigo 38.º

Utilização de equipamentos informáticos

1. Os equipamentos informáticos disponibilizados pelo AEAS destinam-se prioritariamente ao exercício de funções profissionais e educativas.
2. Os utilizadores devem assegurar uma utilização diligente dos equipamentos, prevenindo acessos indevidos, instalação de software não autorizado e outras situações suscetíveis de comprometer a segurança da informação.
3. Sempre que um equipamento contenha dados pessoais, devem ser adotadas medidas de proteção adequadas, designadamente bloqueio automático do ecrã, encriptação dos dispositivos e atualização regular dos sistemas.

Artigo 39.º

Utilização de dispositivos móveis

1. A utilização de computadores portáteis, tablets e telemóveis para tratamento de dados pessoais deve observar as regras de segurança definidas pelo AEAS.
2. Sempre que sejam utilizados dispositivos móveis fora das instalações do Agrupamento, devem ser adotadas medidas acrescidas de proteção contra perda, furto ou acesso não autorizado.
3. A transferência de dados pessoais para dispositivos externos deve limitar-se às situações estritamente necessárias e observar as medidas de segurança adequadas.

Artigo 40.º

Conservação e destruição segura da informação

1. Os documentos que contenham dados pessoais são conservados durante os prazos legalmente estabelecidos.
2. Findos os prazos de conservação, os documentos são eliminados de forma segura, garantindo a impossibilidade da sua recuperação.
3. A destruição de documentos em suporte de papel deve ser efetuada através de meios que impeçam a reconstituição da informação.
4. Os suportes informáticos devem ser sujeitos a procedimentos seguros de eliminação ou destruição antes da respetiva reutilização ou abate.

Artigo 41.º

Boas práticas de segurança

1. Todos os trabalhadores devem observar boas práticas de segurança da informação, designadamente:
   a) Não deixar documentos contendo dados pessoais em locais acessíveis ao público;
   b) Bloquear o computador sempre que se ausentem do posto de trabalho;
   c) Recolher imediatamente os documentos impressos;
   d) Evitar a utilização de dispositivos de armazenamento não autorizados;
   e) Confirmar os destinatários antes do envio de mensagens de correio eletrónico;
   f) Comunicar imediatamente qualquer incidente suscetível de comprometer a segurança dos dados.

2. O incumprimento das boas práticas previstas no presente artigo pode determinar a adoção das medidas legalmente adequadas.

Artigo 42.º

Cópias de segurança

1. O AEAS assegura a realização de cópias de segurança dos sistemas de informação considerados essenciais ao funcionamento dos serviços.
2. As cópias de segurança devem garantir a recuperação da informação em caso de falha técnica, incidente de segurança ou desastre.
3. O acesso às cópias de segurança fica limitado às pessoas devidamente autorizadas.

CAPÍTULO VI

Violação de Dados Pessoais e Gestão de Incidentes

Nota Introdutória

A proteção dos dados pessoais exige que qualquer incidente suscetível de comprometer a confidencialidade, integridade ou disponibilidade da informação seja comunicado, avaliado e tratado de forma célere e eficaz.

O presente capítulo estabelece os procedimentos internos aplicáveis à deteção, comunicação, gestão e mitigação de incidentes de segurança e de violações de dados pessoais, em conformidade com o Regulamento (UE) 2016/679.

Artigo 43.º

Conceito de violação de dados pessoais

1. Para efeitos do presente Regulamento, entende-se por violação de dados pessoais qualquer incidente de segurança que provoque, de modo acidental ou ilícito:
   a) A destruição de dados pessoais;
   b) A perda de dados pessoais;
   c) A alteração de dados pessoais;
   d) A divulgação não autorizada de dados pessoais;
   e) O acesso não autorizado a dados pessoais transmitidos, conservados ou sujeitos a qualquer outro tipo de tratamento.
2. Constituem exemplos de violação de dados pessoais, designadamente:
   a) O envio de informação para destinatário incorreto;
   b) A perda ou furto de computador portátil, telemóvel, pen USB ou outro dispositivo contendo dados pessoais;
   c) O acesso indevido a processos individuais de alunos ou trabalhadores;
   d) A divulgação não autorizada de classificações, avaliações ou informações disciplinares;
   e) O ataque informático suscetível de comprometer dados pessoais;
   f) A destruição acidental de documentação contendo dados pessoais.

Artigo 44.º

Comunicação interna de incidentes

1. Qualquer trabalhador ou colaborador que tenha conhecimento de um incidente suscetível de constituir uma violação de dados pessoais deve comunicá-lo imediatamente ao respetivo superior hierárquico e ao serviço designado pela Direção para a gestão destas ocorrências.

2. A comunicação deve conter, sempre que possível:
   a) A descrição do incidente;
   b) A data e hora da ocorrência ou da sua deteção;
   c) As categorias de dados afetadas;
   d) O número aproximado de titulares envolvidos, quando conhecido;
   e) As medidas já adotadas para limitar os efeitos do incidente.
3. A omissão injustificada da comunicação de um incidente pode constituir incumprimento dos deveres funcionais.

Artigo 45.º

Avaliação do incidente

1. Após a receção da comunicação, o AEAS procede à avaliação do incidente, com o apoio do Encarregado da Proteção de Dados sempre que necessário.
2. A avaliação deve considerar, designadamente:
   a) A natureza dos dados pessoais envolvidos;
   b) O número de titulares afetados;
   c) As consequências previsíveis para os titulares;
   d) A probabilidade de ocorrência de riscos para os direitos e liberdades das pessoas singulares;
   e) As medidas necessárias para reduzir ou eliminar os riscos identificados.

Artigo 46.º

Notificação à autoridade de controlo

1. Sempre que a violação de dados pessoais seja suscetível de implicar risco para os direitos e liberdades dos titulares dos dados, o AEAS promove a respetiva notificação à Comissão Nacional de Proteção de Dados, nos termos e prazos previstos na legislação aplicável.
2. A decisão de proceder à notificação deve ser devidamente fundamentada e documentada.
3. Sempre que legalmente exigível, a notificação é efetuada com a colaboração do Encarregado da Proteção de Dados.

Artigo 47.º

Comunicação aos titulares dos dados

1. Quando a violação de dados pessoais seja suscetível de implicar elevado risco para os direitos e liberdades dos titulares, estes são informados sem demora injustificada, nos termos da legislação aplicável.
2. A comunicação deve ser redigida em linguagem clara e acessível e conter, sempre que possível:
   a) A descrição da natureza da violação;
   b) As consequências prováveis;
   c) As medidas adotadas pelo AEAS;
   d) As recomendações destinadas a minimizar os eventuais efeitos negativos;
   e) Os contactos do Encarregado da Proteção de Dados.

Artigo 48.º

Registo dos incidentes

1. O AEAS mantém um registo atualizado de todas as violações de dados pessoais, independentemente da obrigatoriedade da respetiva notificação.
2. O registo deve conter, designadamente:
   a) A descrição do incidente;
   b) A data da ocorrência;
   c) As categorias de dados envolvidas;
   d) As medidas corretivas adotadas;
   e) As decisões tomadas;
   f) A fundamentação relativa à eventual notificação ou não notificação à autoridade de controlo.
3. O registo referido no presente artigo é conservado pelo período legalmente aplicável e encontra-se acessível apenas às pessoas autorizadas.

Artigo 49.º

Medidas corretivas e preventivas

1. Após cada incidente, o AEAS procede à análise das respetivas causas e adota as medidas corretivas necessárias para evitar a repetição de situações idênticas.
2. Sempre que se revele necessário, podem ser determinadas:
   a) A revisão de procedimentos;
   b) A atualização das medidas de segurança;
   c) A realização de ações de formação;
   d) A revisão dos perfis de acesso aos sistemas de informação;
   e) A implementação de novas soluções tecnológicas de proteção da informação.
3. As medidas adotadas devem ser proporcionais aos riscos identificados e adequadas às características do incidente.

CAPÍTULO VII

Governação da Proteção de Dados e Responsabilidades Institucionais

Nota Introdutória

A proteção dos dados pessoais constitui uma responsabilidade transversal a toda a comunidade educativa.

O presente capítulo define as competências e responsabilidades dos diversos intervenientes no âmbito do tratamento de dados pessoais, promovendo uma cultura institucional de responsabilidade, segurança, cooperação e melhoria contínua.

Artigo 50.º

Princípio da responsabilidade institucional

1. A proteção dos dados pessoais constitui uma responsabilidade de todos os trabalhadores, colaboradores e utilizadores dos sistemas de informação do AEAS.
2. Cada interveniente responde pelo tratamento dos dados pessoais que realize no exercício das respetivas funções, nos termos da legislação aplicável e do presente Regulamento.
3. O cumprimento das normas de proteção de dados integra os deveres gerais de prossecução do interesse público, legalidade, imparcialidade, sigilo profissional e boa administração.

Artigo 51.º

Competências do Diretor

1. Compete ao Diretor, enquanto órgão de direção, administração e gestão do AEAS:
   a) Assegurar o cumprimento do presente Regulamento;
   b) Promover a implementação de medidas técnicas e organizativas adequadas à proteção dos dados pessoais;
   c) Garantir a disponibilização dos recursos necessários ao cumprimento das obrigações legais;
   d) Promover uma cultura organizacional de proteção de dados e segurança da informação;
   e) Determinar a adoção de medidas corretivas sempre que sejam identificadas situações de incumprimento;
   f) Assegurar a articulação institucional com o Encarregado da Proteção de Dados.
2. O Diretor promove, sempre que necessário, ações de sensibilização e formação dirigidas aos trabalhadores e colaboradores do Agrupamento.

Artigo 52.º

Encarregado da Proteção de Dados

1. O AEAS assegura o exercício das funções de Encarregado da Proteção de Dados, nos termos do artigo 37.º do Regulamento (UE) 2016/679 e da legislação nacional aplicável.
2. O Encarregado da Proteção de Dados exerce as suas funções com independência e autonomia técnica, não podendo receber instruções quanto ao exercício das competências que lhe são legalmente atribuídas.
3. Compete, designadamente, ao Encarregado da Proteção de Dados:
   a) Informar e aconselhar o AEAS relativamente às obrigações decorrentes da legislação sobre proteção de dados;
   b) Acompanhar o cumprimento do presente Regulamento;
   c) Sensibilizar e promover ações de formação;
   d) Cooperar com a Comissão Nacional de Proteção de Dados;
   e) Constituir ponto de contacto entre o AEAS, os titulares dos dados e a autoridade de controlo.

Artigo 53.º

Competências dos Coordenadores

1. Os Coordenadores de Departamento, Coordenadores de Estabelecimento, Coordenadores Técnicos e demais responsáveis por unidades orgânicas colaboram na implementação das medidas de proteção de dados no âmbito das respetivas áreas de responsabilidade.
2. Compete-lhes, designadamente:
   a) Promover o cumprimento das normas constantes do presente Regulamento;
   b) Sensibilizar os trabalhadores sob a sua coordenação;
   c) Comunicar situações de risco ou incumprimento;
   d) Colaborar na implementação de medidas corretivas.

Artigo 54.º

Competências dos docentes

1. Os docentes tratam os dados pessoais dos alunos e respetivos encarregados de educação exclusivamente para o exercício das funções educativas e pedagógicas legalmente atribuídas.
2. Os docentes devem, designadamente:

a) Assegurar a confidencialidade das informações de que tomem conhecimento;
b) Utilizar exclusivamente os sistemas e plataformas autorizados pelo Agrupamento;
c) Garantir a segurança dos documentos e equipamentos utilizados;
d) Comunicar qualquer incidente de segurança de que tenham conhecimento;
e) Respeitar as orientações emitidas pelo AEAS em matéria de proteção de dados.

Artigo 55.º

Competências dos assistentes técnicos

1. Os assistentes técnicos asseguram o tratamento dos dados pessoais necessários ao funcionamento administrativo do AEAS, observando rigorosamente os princípios da proteção de dados.
2. Devem, designadamente:
   a) Garantir a confidencialidade dos processos administrativos;
   b) Confirmar a identidade dos requerentes antes da prestação de informação;
   c) Assegurar a correta conservação dos documentos;
   d) Comunicar qualquer situação suscetível de comprometer a segurança da informação.

Artigo 56.º

Competências dos assistentes operacionais

1. Os assistentes operacionais devem respeitar o dever de confidencialidade relativamente às informações pessoais de que tomem conhecimento no exercício das respetivas funções.
2. É-lhes vedada a divulgação de informações relativas a alunos, trabalhadores ou demais membros da comunidade educativa, salvo quando legalmente autorizados.
3. Sempre que detetem situações suscetíveis de constituir violação de dados pessoais, devem comunicá-las de imediato ao respetivo superior hierárquico.

Artigo 57.º

Competências dos Diretores de Turma, Professores Titulares de Turma e Educadores de Infância

1. Os Diretores de Turma, Professores Titulares de Turma e Educadores de Infância asseguram o tratamento dos dados pessoais indispensáveis ao acompanhamento educativo das crianças e dos alunos, em conformidade com os princípios da licitude, necessidade, confidencialidade e minimização dos dados.
2. Compete-lhes, designadamente:
   a) Garantir a confidencialidade da informação constante dos processos individuais dos alunos;
   b) Utilizar os dados pessoais exclusivamente para finalidades educativas e administrativas legalmente previstas;
   c) Assegurar que as comunicações com pais e encarregados de educação respeitam a confidencialidade dos restantes alunos;
   d) Evitar a divulgação pública de informações suscetíveis de identificar alunos ou respetivos agregados familiares;
   e) Zelar pela correta conservação da documentação que lhes seja confiada.
3. Sempre que utilizem plataformas digitais de comunicação ou gestão pedagógica, devem observar as orientações emitidas pelo AEAS relativamente à proteção dos dados pessoais.

Artigo 58.º

Competências dos Serviços de Psicologia e Orientação e da Equipa Multidisciplinar de Apoio à Educação Inclusiva

1. Os profissionais afetos aos Serviços de Psicologia e Orientação (SPO) e à Equipa Multidisciplinar de Apoio à Educação Inclusiva (EMAEI) tratam categorias especiais de dados pessoais, observando especiais deveres de reserva, confidencialidade e segurança.
2. O acesso à informação de natureza psicológica, clínica, social ou educativa fica limitado aos profissionais cuja intervenção o justifique.
3. A partilha de informação entre os membros das equipas multidisciplinares deve obedecer ao princípio da necessidade de conhecer e limitar-se ao estritamente indispensável para assegurar a adequada resposta educativa aos alunos.
4. Os relatórios técnicos devem ser conservados e transmitidos através de procedimentos que garantam a respetiva confidencialidade.

Artigo 59.º

Competências dos serviços administrativos

1. Os serviços administrativos asseguram o tratamento dos dados pessoais necessários à gestão académica, administrativa, financeira e de recursos humanos do Agrupamento.
2. Compete-lhes, designadamente:
   a) Confirmar a legitimidade dos pedidos de acesso à informação;
   b) Garantir a atualização e exatidão dos dados tratados;
   c) Assegurar a correta aplicação das regras de conservação documental;
   d) Adotar medidas que impeçam o acesso indevido a processos administrativos;
   e) Colaborar com a Direção e com o Encarregado da Proteção de Dados na implementação das medidas previstas no presente Regulamento.

Artigo 60.º

Competências do Coordenador TIC e dos administradores dos sistemas de informação

1. O Coordenador TIC e os administradores dos sistemas de informação colaboram na implementação das medidas técnicas destinadas à proteção dos dados pessoais tratados pelo AEAS.
2. Compete-lhes, designadamente:
   a) Garantir a segurança técnica dos sistemas de informação;
   b) Gerir os perfis de acesso dos utilizadores;
   c) Assegurar a instalação das atualizações de segurança;
   d) Monitorizar os sistemas relativamente a incidentes de segurança;
   e) Colaborar na recuperação dos sistemas em caso de falha ou incidente.
3. Os administradores dos sistemas estão sujeitos a especiais deveres de confidencialidade relativamente à informação a que possam aceder no exercício das respetivas funções.

Artigo 61.º

Prestadores de serviços e subcontratantes

1. Sempre que o AEAS recorra a entidades externas para o tratamento de dados pessoais, deve assegurar que estas apresentam garantias suficientes de cumprimento da legislação aplicável em matéria de proteção de dados.

2. O tratamento realizado por subcontratantes depende da celebração de contrato ou outro ato jurídico que regule o tratamento dos dados pessoais, nos termos do artigo 28.º do Regulamento (UE) 2016/679.
3. Os prestadores de serviços apenas podem tratar os dados pessoais de acordo com as instruções documentadas do AEAS e para as finalidades contratualmente estabelecidas.

Artigo 62.º

Dever permanente de confidencialidade

1. Todas as pessoas que, no exercício das respetivas funções, tenham acesso a dados pessoais ficam obrigadas ao dever de confidencialidade.
2. O dever de confidencialidade mantém-se mesmo após a cessação das funções ou da relação jurídica com o AEAS.
3. A violação do dever de confidencialidade determina a aplicação das consequências previstas na lei, sem prejuízo da eventual responsabilidade disciplinar, civil, contraordenacional ou criminal.

CAPÍTULO VIII

Tecnologias Digitais, Inteligência Artificial e Proteção de Dados

Nota Introdutória

A transformação digital constitui uma oportunidade para melhorar os processos pedagógicos, administrativos e organizacionais do Agrupamento.

A utilização de tecnologias digitais deve, contudo, assegurar o respeito pelos direitos fundamentais, pela proteção dos dados pessoais, pela segurança da informação e pelos princípios da transparência, da responsabilidade e da supervisão humana.

Artigo 63.º

Princípios gerais de utilização das tecnologias digitais

1. A utilização de tecnologias digitais no AEAS deve respeitar os princípios da legalidade, necessidade, proporcionalidade, segurança, acessibilidade e proteção dos dados pessoais.
2. As tecnologias utilizadas devem contribuir para a melhoria das atividades educativas e administrativas, salvaguardando sempre os direitos e liberdades dos titulares dos dados.
3. Sempre que sejam adotadas novas soluções tecnológicas suscetíveis de implicar tratamento de dados pessoais, deve ser previamente analisada a respetiva conformidade com a legislação aplicável.

Artigo 64.º

Utilização de plataformas digitais

1. O tratamento de dados pessoais através de plataformas digitais deve realizar-se, preferencialmente, mediante a utilização de soluções disponibilizadas ou autorizadas pela tutela ou pelo AEAS, após verificação da respetiva conformidade jurídica e técnica.
2. A adoção de novas plataformas digitais deve atender, designadamente:
   a) À proteção dos dados pessoais;
   b) À segurança da informação;
   c) À localização e condições de tratamento dos dados;
   d) À existência de garantias adequadas relativamente aos subcontratantes;

e) À necessidade e proporcionalidade da utilização da plataforma.

3. Sempre que se revele necessário, podem ser solicitados pareceres técnicos ou jurídicos antes da adoção de novas soluções tecnológicas.

Artigo 65.º

Utilização de sistemas de Inteligência Artificial

1. A utilização de sistemas de Inteligência Artificial no AEAS deve respeitar a legislação aplicável, os princípios da ética pública, da proteção de dados pessoais, da transparência e da supervisão humana.
2. A utilização destas tecnologias não dispensa a intervenção, análise e decisão humana sempre que estejam em causa decisões de natureza pedagógica, disciplinar ou administrativa.
3. Não devem ser introduzidos em sistemas públicos de Inteligência Artificial dados pessoais identificáveis, categorias especiais de dados ou informação confidencial, salvo quando exista fundamento jurídico adequado e estejam garantidas as medidas técnicas e organizativas exigidas por lei.
4. A utilização de ferramentas de Inteligência Artificial pelos trabalhadores do AEAS deve respeitar as orientações internas aprovadas pela Direção.

Artigo 66.º

Utilização responsável pelos trabalhadores

1. Os trabalhadores do AEAS devem utilizar as tecnologias digitais de forma responsável, diligente e conforme às respetivas funções.
2. É vedada a utilização de tecnologias digitais para finalidades incompatíveis com as atribuições do Agrupamento ou suscetíveis de comprometer a segurança da informação.
3. Os trabalhadores devem assegurar a verificação da exatidão dos conteúdos produzidos com recurso a ferramentas digitais ou de Inteligência Artificial antes da respetiva utilização em contexto profissional.

Artigo 67.º

Literacia digital e sensibilização

1. O AEAS promove ações de sensibilização e formação destinadas a fomentar uma utilização segura, ética e responsável das tecnologias digitais.
2. As ações de formação podem abranger, designadamente:
   a) Proteção de dados pessoais;
   b) Segurança da informação;
   c) Inteligência Artificial;
   d) Cibersegurança;
   e) Boas práticas na utilização das tecnologias digitais;
   f) Prevenção da desinformação e utilização crítica das fontes digitais.

Artigo 68.º

Melhoria contínua

1. O AEAS acompanha a evolução tecnológica e promove a atualização periódica das orientações internas relativas à utilização das tecnologias digitais.
2. Sempre que a evolução tecnológica ou legislativa o justifique, podem ser emitidas instruções internas complementares ao presente Regulamento.

3. A aplicação do presente capítulo deve contribuir para a promoção de uma cultura de inovação responsável, proteção dos direitos fundamentais e utilização ética das tecnologias digitais.

CAPÍTULO IX

Conservação, Arquivo e Eliminação de Dados

Artigo 69.º

Prazos de conservação

1. Os dados pessoais tratados pelo AEAS são conservados apenas pelo período estritamente necessário à prossecução das finalidades que motivaram a sua recolha.
2. Os prazos de conservação respeitam a legislação aplicável em matéria de arquivo administrativo, educação, recursos humanos, ação social escolar e demais regimes legais específicos.
3. Sempre que não exista prazo legalmente definido, os dados são conservados de acordo com critérios de necessidade administrativa, pedagógica e de responsabilidade legal.

Artigo 70.º

Critérios de conservação

1. Na definição dos prazos de conservação são considerados, designadamente:
   a) Obrigações legais e fiscais;
   b) Necessidades pedagógicas e administrativas;
   c) Defesa de direitos em sede judicial ou administrativa;
   d) Orientações da tutela e da CNPD.
2. Os prazos de conservação são objeto de revisão periódica.

Artigo 71.º

Arquivo e organização da informação

1. O AEAS assegura a organização adequada dos seus sistemas de arquivo físico e digital.
2. O acesso aos arquivos é restringido aos trabalhadores devidamente autorizados.
3. Devem ser adotadas medidas que garantam a integridade, rastreabilidade e segurança da informação arquivada.

Artigo 72.º

Eliminação e destruição de dados

1. Findo o prazo de conservação, os dados pessoais são eliminados de forma segura e irreversível.
2. A eliminação de dados em suporte físico deve ser efetuada por meios que impeçam a sua reconstituição.
3. A eliminação de dados em suporte digital deve garantir a impossibilidade de recuperação através de meios técnicos adequados.
4. Sempre que aplicável, deve ser elaborado registo da eliminação efetuada.

CAPÍTULO X

Disposições Finais e Transitórias

Artigo 73.º

Regulamentos complementares

1. O presente Regulamento pode ser complementado por orientações internas, despachos, circulares ou normas técnicas aprovadas pela Direção.
2. Esses instrumentos não podem contrariar o disposto no presente Regulamento nem na legislação aplicável.

Artigo 74.º

Interpretação e integração de lacunas

1. As dúvidas de interpretação do presente Regulamento são resolvidas pela Direção do AEAS, em articulação com o Encarregado da Proteção de Dados.
2. As lacunas são integradas com recurso à legislação aplicável, em especial o RGPD e a Lei n.º 58/2019.

Artigo 75.º

Revisão do Regulamento

1. O presente Regulamento é objeto de revisão sempre que se verifiquem alterações legislativas ou organizacionais relevantes.
2. A revisão pode ser total ou parcial, devendo garantir a atualização permanente das práticas de proteção de dados do AEAS.

Artigo 76.º

Entrada em vigor

1. O presente Regulamento entra em vigor no dia seguinte ao da sua aprovação pelo órgão competente do Agrupamento.
2. A sua divulgação é assegurada por meios internos e institucionais adequados, garantindo o conhecimento por toda a comunidade educativa.

Agrupamento de Escolas Alfredo da Silva, 2 de setembro 2026

Diretor do AEAS: Joana Sofia Baptista

Responsável pela proteção de dados no Agrupamento de Escolas Alfredo da Silva
Profª Paula Telles da Silva
E-mail: rgpd@aeass.pt

ANEXOS

ANEXO I – POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

1. Princípios gerais

O Agrupamento de Escolas Alfredo da Silva adota uma política de segurança da informação baseada nos princípios da confidencialidade, integridade e disponibilidade da informação, assegurando a proteção dos dados pessoais contra destruição, perda, alteração, divulgação ou acesso não autorizado.

2. Controlo de acessos

2.1. O acesso a sistemas de informação é concedido com base no princípio da necessidade de conhecimento (need-to-know).

2.2. Cada utilizador dispõe de credenciais individuais e intransmissíveis.

2.3. São aplicados perfis de acesso diferenciados por função.

3. Segurança dos sistemas informáticos

3.1. Os sistemas são protegidos por mecanismos de autenticação e, quando aplicável, autenticação multifator.

3.2. São implementadas atualizações regulares de segurança (patch management).

3.3. É proibida a instalação de software não autorizado.

4. Segurança física

4.1. O acesso a áreas com sistemas críticos (secretaria, servidores) é restrito a pessoal autorizado.

4.2. Documentos em suporte físico contendo dados pessoais devem ser armazenados em local seguro e fechado.

5. Comunicações e redes

5.1. As comunicações institucionais devem ser realizadas através de canais seguros e oficiais.

5.2. O acesso remoto a sistemas internos deve ser protegido por encriptação.

6. Cópias de segurança

6.1. São realizadas cópias de segurança regulares dos sistemas críticos.

6.2. As cópias são armazenadas de forma segura e testadas periodicamente.

ANEXO II – PROCEDIMENTOS DE GESTÃO DE INCIDENTES

1. Definição de incidente

Considera-se incidente de segurança qualquer evento que comprometa ou possa comprometer a confidencialidade, integridade ou disponibilidade de dados pessoais.

2. Comunicação interna

2.1. Qualquer trabalhador deve comunicar imediatamente um incidente ao Encarregado de Proteção de Dados (EPD).

2.2. A comunicação deve ser feita por via segura e documentada.

3. Avaliação do incidente

O EPD procede à análise do risco, determinando:

- natureza dos dados afetados
- número de titulares envolvidos
- impacto potencial

4. Notificação à autoridade de controlo

Quando aplicável, o incidente é notificado à Comissão Nacional de Proteção de Dados (CNPD) no prazo de 72 horas.

5. Comunicação aos titulares

Quando o incidente implicar elevado risco para os direitos e liberdades dos titulares, estes devem ser informados sem demora injustificada.

6. Registo de incidentes

Todos os incidentes são registados e arquivados para efeitos de auditoria e melhoria contínua.

ANEXO III – MATRIZ DE RESPONSABILIDADES (RACI)

Legenda:

- **R = Responsável pela execução**
- **A = Responsável final (Accountable)**
- **C = Consultado**
- **I = Informado**

Atividade	Diretor	EPD	Docentes	Secretaria	Técnico Informático
Definição de políticas de proteção de dados	**A**	**C**	**I**	**I**	**C**
Cumprimento do RGPD	**A**	**R**	**R**	**R**	**R**
Gestão de acessos a sistemas	**A**	**C**	**I**	**R**	**R**
Registo de atividades de tratamento	**A**	**R**	**I**	**R**	**C**
Gestão de consentimentos	**A**	**C**	**R**	**R**	**I**
Formação em proteção de dados	**A**	**R**	**C**	**C**	**I**
Gestão de incidentes de segurança	**A**	**R**	**I**	**I**	**R**
Comunicação com a CNPD	**A**	**R**	**I**	**I**	**C**
Conservação e eliminação de dados	**A**	**C**	**I**	**R**	**C**

ANEXO IV – TABELA DE RETENÇÃO DE DADOS

1. Princípio geral

Os dados pessoais são conservados apenas pelo período estritamente necessário ao cumprimento das finalidades legais, administrativas e educativas, sendo eliminados ou anonimizados após o termo dos prazos legais.

2. Registos escolares

Tipo de dado	Prazo de conservação
Processos individuais de alunos	5 anos após saída do aluno
Registos de avaliação	5 anos
Pautas finais	Permanente (arquivo histórico)
Exames internos	5 anos
Registos disciplinares	5 anos após conclusão de ciclo

3. Recursos humanos

Tipo de dado	Prazo de conservação
Processos de docentes	5 anos após cessação de funções
Processos de não docentes	5 anos após cessação de funções
Registos de assiduidade	5 anos
Processos disciplinares	10 anos

4. Dados administrativos e financeiros

Tipo de dado	Prazo de conservação
Faturas e pagamentos	10 anos
Contratos	10 anos após cessação
Registos contabilísticos	10 anos

5. Dados digitais e sistemas

Tipo de dado	Prazo de conservação
Logs de sistema	1 ano
Registos de acessos	1 ano
Backups	Ciclo rotativo (30–90 dias)

6. Dados de encarregados de educação

Tipo de dado	Prazo de conservação
Contactos e autorizações	Durante a frequência do aluno + 1 ano
Consentimentos	Até revogação + 2 anos (prova de conformidade)

ANEXO V – POLÍTICA DE COOKIES

1. Princípio geral

O Agrupamento de Escolas Alfredo da Silva utiliza cookies estritamente necessários ao funcionamento técnico das suas plataformas digitais e serviços educativos.

2. Tipologia de cookies

São utilizados apenas cookies essenciais, nomeadamente:

- cookies de autenticação e sessão
- cookies de segurança
- cookies técnicos de funcionamento das plataformas

Não são utilizados cookies de marketing, publicidade ou rastreamento comportamental.

3. Finalidade

Os cookies têm como finalidade:

- garantir o funcionamento correto das plataformas digitais
- assegurar a autenticação dos utilizadores

- melhorar a segurança da informação

4. Consentimento

Sempre que aplicável, o utilizador é informado da utilização de cookies e, quando legalmente exigido, o consentimento é recolhido de forma explícita.

5. Gestão de cookies

Os utilizadores podem configurar o seu navegador para bloquear ou eliminar cookies, podendo tal afetar o funcionamento de algumas funcionalidades.

ANEXO VI – PROTEÇÃO DE DADOS EM PLATAFORMAS DIGITAIS

1. Âmbito

O presente regulamento aplica-se a todas as plataformas digitais utilizadas pelo AEAS, incluindo sistemas de gestão escolar, plataformas de aprendizagem (LMS), correio eletrónico institucional e ferramentas colaborativas.

2. Acesso e autenticação

O acesso às plataformas digitais é restrito a utilizadores autenticados, mediante credenciais individuais e intransmissíveis.

3. Finalidade do tratamento

Os dados tratados nas plataformas digitais destinam-se exclusivamente a fins pedagógicos, administrativos e organizacionais.

4. Segurança

São implementadas medidas técnicas e organizativas adequadas, incluindo:

- autenticação individual
- perfis de acesso diferenciados
- registo de atividades (logs)
- encriptação quando aplicável

5. Proibições

É expressamente proibido:

- partilhar credenciais de acesso
- aceder a dados sem autorização
- exportar ou divulgar dados fora dos canais institucionais

6. Plataformas externas

Sempre que sejam utilizadas plataformas de terceiros, o AEAS assegura a existência de garantias adequadas de proteção de dados, nos termos do RGPD.