Política de Segurança Digital do ***AET***

Documento

Política de Segurança Digital do AET

Diretor

Conselho Pedagógico

Julho 2022

Contacto

TELEFONE:
253 470 670

MORADA
Rua do Pinheiral - Apartado 4025
4806-909 Caldas das Taipas

SITE:
http://www.aetaipas.pt
https://www2.nonio.uminho.pt/aetaipas

EMAIL:
secretaria@aetaipas.pt
direcao@aetaipas.pt

Índice

Elaboração	Diretor	João Montes	
Parecer	Conselho Pedagógico	João Montes	Positivo 1/06/2022
Aprovação	Conselho Geral	Cláudia Vieira	26/07/2022
Divulgação	Diretor	João Montes	
Próxima revisão	Diretor I Coordenador da PSD	João Montes Carlos Silva	Junho 2023

Introdução

O acesso à Internet nas escolas é cada vez mais fácil, pois as tecnologias digitais fazem parte do nosso dia-a-dia. O número de dispositivos com ligação à Internet no espaço escolar tem aumentado de forma exponencial. Grande parte dos colaboradores (alunos, docentes e não docentes) são portadores do seu equipamento tecnológico para as diferentes unidades do Agrupamento de Escolas das Taipas e usa-o para fins profissionais (tablets, computadores portáteis, telemóveis). Estes equipamentos permitem que os docentes, por exemplo, possam introduzir e alterar dados sensíveis do sistema como as notas, sumários, faltas ou ocorrências diversas e tenham acesso aos dados pessoais de alunos e das suas famílias. Por outro lado, é também cada vez maior o número de alunos que trazem dispositivos que permitem ligação à Internet e a diferentes plataformas de trabalho, nomeadamente do AETaipas.

Para tirar o máximo partido das oportunidades que as tecnologias digitais oferecem é necessário conhecê-las e saber utilizá-las corretamente. Ao adotar políticas para a segurança digital podemos garantir um ambiente mais seguro para a comunidade escolar e para os colaboradores protegendo e preparando-os para os perigos que uma utilização incorreta pode implicar.

Ciente de que, atualmente, parte do nosso dia é passado *online*, o Agrupamento de Escolas das Taipas alerta para a importância dos cuidados a ter na utilização de ferramentas e serviços de Internet, sugerindo um conjunto de iniciativas e recursos de sensibilização de Educação para a Cidadania Digital. Disponibiliza recomendações e orientações, a ter em conta na utilização das tecnologias de suporte ao ensino e destaca os serviços de apoio essenciais na prevenção de situações de risco *online*, que crianças e jovens podem enfrentar.

Por seu turno, os serviços administrativos constituem-se como centro nevrálgico de um acerbo de informação significativo que implica práticas de sigilo e de proteção acentuada e prescritiva.

Importa, pois, definir uma Política de Segurança Digital que ofereça duas condições basilares – um aproveitamento máximo dos meios digitais no e para o trabalho e, paralelamente, níveis de segurança elevados que garantam uma utilização dos suportes informáticos disponibilizados pelo AETaipas.

Política de Segurança Digital

A segurança digital visa proteger a confidencialidade, integridade e disponibilidade de autenticidade de documentos e dados pessoais. Atualmente, crianças, jovens e adultos interagem diariamente com as mais diversas tecnologias e contactam, experimentam e vivenciam uma infindável variedade de oportunidades, atitudes e situações. A troca de ideias, opiniões, experiências, a interação social *online* e as oportunidades de aprendizagem daí decorrentes apresentam enormes benefícios para todos, mas podem, por vezes, colocar crianças, jovens e adultos em perigo.

A segurança digital abrange questões relacionadas não só com crianças e jovens, mas também com adultos e com a utilização que todos fazem da Internet e de todos os dispositivos que permitem a comunicação eletrónica em ambiente escolar ou fora dele. Tal exige a atenção e a formação de todos os elementos da comunidade escolar sobre os riscos e as responsabilidades envolvidas e faz parte do cuidado inerente à função de cada educador.

Educadores e professores devem, pois, ter consciência da importância das boas práticas de segurança digital, visando a educação, a proteção e a formação das crianças e dos jovens sob o seu cuidado para o correto e adequado uso das tecnologias.

A política de segurança digital é, por isso mesmo, essencial na definição de princípios nucleares de ação, que todos os elementos da comunidade escolar devem observar e aplicar.

O Coordenador da Política de Segurança Digital é designado pelo Diretor e funciona como elemento de articulação com o Diretor do Agrupamento de Escolas das Taipas.

A Política de Segurança Digital, redigida com base na Política do Selo de Segurança Digital e na legislação aplicável, será revista anualmente.

Este documento foi elaborado de acordo com o Regulamento Geral de Proteção de Dados (RGPD) que entrou em vigor em 25 de maio de 2018.

1 de junho de 2022

O Coordenador da Política de Segurança Digital

_____

(Carlos Manuel Ferreira da Silva)

Política aprovada pelo Diretor

_____

(João Barroso Cunha Montes)

Objetivos da Política de Segurança Digital

Os objetivos da Política de Segurança Digital (PSD) do AET são os seguintes:

- Identificar claramente os princípios fundamentais, seguros e responsáveis, esperados de todos os membros da comunidade educativa em relação à tecnologia como forma de garantir que a instituição seja um ambiente seguro no que concerne à utilização de equipamentos e da Internet;
- Sensibilizar todos os membros da comunidade educativa sobre os potenciais riscos, bem como dos benefícios da tecnologia;
- Permitir que todos possam trabalhar com segurança e responsabilidade, com vista a um modelo comportamental positivo *online*, estando cientes da necessidade de gerir os seus próprios padrões e práticas ao usar a tecnologia;
- Identificar procedimentos claros a adotar de forma a responder às preocupações de segurança.

Esta PSD aplica-se a todos os funcionários/trabalhadores, incluindo o órgão de gestão, professores, pessoal de apoio, prestadores de serviços, visitantes, voluntários e outras pessoas que trabalham ou prestam serviços em nome do Agrupamento (coletivamente e adiante referidos como «pessoal» nesta Política), 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. Esta Política deve ser lida em conjunto com outras políticas escolares relevantes.

Principais responsabilidades

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

- Desenvolver e promover uma visão e cultura de segurança *online*, em linha com as recomendações nacionais, apoiando e consultando adequadamente toda a comunidade escolar;
- Garantir que a segurança *online* é vista proativamente por toda a comunidade educativa como uma questão de salvaguarda;
- Apoiar o Coordenador de Segurança Digital, garantindo que tenha tempo e recursos suficientes para cumprir o seu papel de segurança *online* e demais responsabilidades;
- Assegurar uma política de formação regular e adequada quanto à segurança e responsabilidades *online* e as orientações relativas a comunicações seguras e adequadas;
- Tomar conhecimento e decidir acerca de quaisquer incidentes de segurança *online*;
- Assegurar que são realizadas avaliações de risco adequadas sobre a utilização segura da tecnologia, incluindo a garantia de uma utilização responsável dos dispositivos;
- Intervir disciplinarmente sobre quem, de forma dolosa, coloque em causa a segurança de pessoas e de instituições.

Competências do Coordenador de Segurança Digital:

- Agir como ponto de contacto e de ligação com outros membros do pessoal e outras agências, conforme apropriado, em relação a todas as questões de segurança *online*.
- Manter-se atualizado ao nível da legislação e tendências em matéria de segurança digital e *online*;
- Coordenar a participação em eventos locais para promover o comportamento *online* positivo, por exemplo, no Dia da Internet Segura, em articulação com o Clube de Proteção Civil;
- Garantir que a segurança *online* é promovida junto dos pais e encarregados de educação e da comunidade em geral, através de uma variedade de canais e de abordagens;
- Trabalhar com a escola para a proteção e segurança de dados, de forma a garantir que a prática está de acordo com a legislação vigente;
- Monitorizar as definições de segurança *online* para identificar as lacunas e usar esses dados para atualizar a resposta da escola a essas necessidades;
- Informar e apoiar o diretor, conforme apropriado, em questões de segurança *online*;
- Facilitar a ligação com organismos locais e nacionais, conforme apropriado;
- Trabalhar com o Diretor na revisão e atualização da Política de Segurança Digital, Política de Utilização Aceitável (PUAs), Política de Privacidade e outras políticas relacionadas, numa base regular (pelo menos anualmente);
- Garantir que a segurança *online* é integrada noutras políticas e procedimentos da escola de forma apropriada.

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

As principais responsabilidades para todos os membros (pessoal) são:

- Contribuir para o desenvolvimento da Política de Segurança Digital;
- Ler as Políticas, aceitando-as, cumprindo-as e fazendo-as cumprir;
- Assumir a sua responsabilidade individual pela segurança e utilização dos sistemas eletrónicos do Agrupamento;
- Ter consciência de uma variedade de questões relacionadas com a segurança *online* e como elas podem afetar ou interferir com os alunos sob os seus cuidados;
- Apresentar boas práticas na utilização das novas tecnologias;
- Incorporar a educação para a segurança *online* no currículo, sempre que possível;
- Identificar e sinalizar situações individuais de preocupação e tomar medidas apropriadas, seguindo as políticas e procedimentos de salvaguarda do AET;
- Saber quando e como escalar questões de segurança *online*, interna e externamente;
- Manter um nível de conduta profissional, ao nível da segurança, no uso pessoal da tecnologia, dentro e fora do local de trabalho.

As principais responsabilidades dos alunos são:

- Contribuir positivamente para o desenvolvimento e concretização das políticas de segurança *online*;

- Ler ou pedir que lhes sejam explicadas pelo Diretor de Turma as Políticas de Segurança do AETaipas e respeitá-las;
- Respeitar os sentimentos e os direitos dos demais, tanto *online* como *offline*;
- Procurar a ajuda de um adulto de confiança, numa situação crítica, e apoiar outros que podem estar a enfrentar problemas de segurança *online*.

A um nível que é adequado à idade do aluno, capacidades e vulnerabilidades:

- Assumir a responsabilidade por manter-se a si e aos outros seguros *online*;
- Assumir a responsabilidade pela sua própria consciência e aprendizagem em relação às oportunidades e riscos decorrentes das tecnologias novas e emergentes;
- Avaliar os riscos pessoais do uso de qualquer tecnologia específica, e comportar-se de forma segura e responsável, para limitar esses riscos;
- Participar das sessões ou ações promovidas no âmbito da cidadania e da segurança digital.

As principais responsabilidades dos pais e encarregados de educação são:

- Ler as Políticas da escola, incentivando os seus educandos ao cumprimento;
- Discutir questões de segurança *online* com os seus filhos, apoiando a escola nas suas abordagens sobre o tema, reforçando comportamentos *online* seguros e adequados em casa;
- Ser um modelo apropriado na utilização racional da tecnologia e na adoção de comportamentos seguros *online*;
- Identificar mudanças no comportamento que possam indicar que o seu filho ou educando está em risco de dano *online*;
- Procurar ajuda e apoio da escola, ou de outros órgãos competentes, se os seus filhos ou educandos encontrarem problemas ou preocupações *online*;
- Assumir a responsabilidade pela sua própria consciência e aprendizagem em relação às oportunidades e riscos decorrentes das tecnologias novas e emergentes;
- Garantir, junto do seu educando, o cumprimento das regras definidas relativamente ao uso do telemóvel nas diferentes escolas do AETaipas;
- Assumir as responsabilidades que lhe são inerentes e auxiliar na resolução de situações de má utilização das tecnologias em ambiente escolar ou relacionadas com o trabalho escolar, nomeadamente o uso indevido do telemóvel, quando colocam em risco a idoneidade, a dignidade, a identidade e a segurança de terceiros.

Ensino e aprendizagem

A IMPORTÂNCIA DA UTILIZAÇÃO DA INTERNET

Devendo fazer parte integrante do currículo como uma ferramenta essencial na aprendizagem, a utilização da Internet no Agrupamento 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 um direito dos alunos que demonstrem responsabilidade e maturidade na sua utilização.

Os níveis de acesso à Internet serão estabelecidos de acordo com os requisitos do currículo, idade e capacidades dos alunos, bem como das necessidades educativas, devidamente fundamentadas.

Todas as atividades escolares que impliquem o uso da Internet devem integrar a apresentação das referências bibliográficas e a salvaguarda dos direitos de autor.

BENEFÍCIOS DA UTILIZAÇÃO DA INTERNET NO ENSINO

- Acesso a recursos pedagógicos e educativos diversificados;
- Intercâmbio cultural e educativo entre alunos de vários países e regiões;
- Desenvolvimento profissional dos professores através do acesso a materiais pedagógicos e aplicações eficazes para o desenvolvimento do currículo;
- Maior acesso a apoio técnico, designadamente gestão remota de redes e atualizações automáticas de programas;
- Possibilidade de aprendizagem quando e onde for mais conveniente;
- Desmaterialização dos suportes e instrumentos de aprendizagem (ex. manuais, testes …).

UTILIZAÇÃO DA INTERNET COM VISTA À MELHORIA DA APRENDIZAGEM

O acesso à Internet no Agrupamento deve ser pensado com vista a alargar e reforçar a educação.

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.

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.

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.

AVALIAÇÃO DE CONTEÚDOS

Os alunos devem ser ensinados a serem críticos em relação aos materiais que leem e a saber como validar uma informação antes de aceitar a sua exatidão.

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

Gestão de sistemas de informação

MANUTENÇÃO DA SEGURANÇA DOS SISTEMAS DE INFORMAÇÃO DO AET

A segurança dos sistemas informáticos do Agrupamento e dos utilizadores é revista anualmente.

A proteção antivírus é atualizada frequentemente.

Os dados pessoais enviados através da Internet ou transferidos para fora da escola estão protegidos pelos sistemas de segurança lógicos e físicos.

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

Os dispositivos amovíveis são utilizados de acordo com as autorizações específicas de cada serviço, estando os sistemas preparados para uma análise automática de prevenção. Os utilizadores não podem instalar qualquer *software*. A instalação de *software* para fins educativos deve ser autorizada pelo Coordenador da Segurança Digital e feita, preferencialmente, por ele mesmo ou por quem ele designe.

Após a utilização, nomeadamente para atividades letivas, todos os ficheiros devem ser removidos, salvo se forem imprescindíveis no tempo.

A capacidade e o funcionamento dos sistemas informáticos serão analisados, pelo menos, uma vez por ano letivo.

É obrigatória a autenticação para aceder à rede da escola.

A página inicial de navegação de cada computador 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.

De forma a reforçar e evitar as alterações anteriormente mencionadas os sistemas estão protegidos com permissões por utilizadores.

GESTÃO DO CORREIO ELETRÓNICO

É atribuída uma conta de correio institucional a todos os trabalhadores do Agrupamento para fins profissionais. Esta conta apenas permanece ativada durante a permanência do funcionário na instituição, sendo eliminada no momento da sua saída.

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

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

As mensagens de correio eletrónico enviadas para organizações externas devem obedecer a procedimentos de escrita e de protocolo similares aos do envio de ofícios por correio físico.

O reencaminhamento de mensagens em cadeia deve ser evitado e a difusão de informação em grupo dever ser cuidadosa, de modo a evitar ser objeto de *spam*.

GESTÃO DOS CONTEÚDOS PUBLICADOS

As informações de contacto no(s) sítio(s) do Agrupamento de Escolas das Taipas devem ser a morada, os números de telefone e o *e-mail* do Agrupamento. Não deve ser publicada qualquer informação pessoal de alunos ou professores.

O responsável editorial (geral) pelos conteúdos digitais publicados pelo Agrupamento na Internet é nomeado pelo Diretor e deve assegurar que os conteúdos publicados são corretos e adequados.

Todas as publicações em formato digital da responsabilidade de membros do Agrupamento devem respeitar os direitos de propriedade intelectual, as políticas de privacidade e os direitos de autor.

Ao AETaipas reserva-se o direito de autorizar e de escrutinar todas as páginas, perfis de página, *sites*, portais ou aplicações *online* que utilizem o logótipo e o nome das escolas que o integram. As páginas, perfis de página, *sites*, portais e aplicações *online* criados no âmbito desta organização educativa, são obrigados a comunicar ao Diretor (diretor@aetaipas.pt) e ao coordenador da PSD (carlosmanuelsilva@aetaipas.pt) a natureza e objetivos pretendidos, cumprindo escrupulosamente a Política de Segurança Digital do AET. Esta comunicação deve ser feita, pela primeira vez, no mês de setembro de 2022.

PUBLICAÇÃO DE FOTOGRAFIAS E DE TRABALHOS DE ALUNOS

Na publicação de imagens e/ou gravações vídeo que incluam alunos, deve ser garantida a proteção da imagem dos alunos, de acordo com a legislação aplicável.

O nome completo do aluno não deve ser utilizado em parte alguma do sítio do Agrupamento, em especial junto a fotografias ou vídeos.

A publicação de qualquer imagem e/ou vídeo de alunos, será feita, apenas, depois de obtida autorização por escrito dos pais e /ou encarregados de educação.

Os trabalhos de alunos podem ser publicados, desde que não estejam identificados, ou após obtida autorização por escrito dos pais e /ou encarregados de educação e desde que não estejam comprometidos os direitos de autoria.

GESTÃO DE COMUNIDADES SOCIAIS VIRTUAIS, REDES SOCIAIS E PUBLICAÇÕES PESSOAIS

Através de atividades dinamizadas pelos professores em sala de aula, pelo Clube de Proteção Civil e pelo Serviço das Bibliotecas Escolares, os alunos serão ensinados 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 e verificarem os termos e condições dos mesmos, antes de os utilizarem, de modo a garantir que são adequados às idades dos alunos.

GESTÃO DOS SISTEMAS DE FILTRAGEM

O acesso à Internet fornecido pelo Agrupamento inclui sistemas de filtragem adequados à idade e à maturidade dos alunos. Contudo, este sistema não impede situações de má utilização ou assegura, em absoluto, a segurança no acesso a conteúdos.

Se sítios indesejáveis chegarem ao conhecimento de alunos, professores ou outros elementos da comunidade educativa, o endereço será comunicado ao Coordenador de Segurança Digital que, por sua vez, documentará o incidente e fá-lo-á chegar ao Diretor.

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

O Agrupamento toma todas as precauções possíveis para garantir que os utilizadores acedam apenas a conteúdo digital apropriado. No entanto, devido à natureza global e diversidade disponível nas redes, para além do facto de os alunos poderem utilizar equipamento pessoal, nem sempre é possível evitar, atempadamente, o seu uso indevido.

Todos os membros da comunidade escolar que violarem os sistemas de filtragem ou acederem a sítios com conteúdos inadequados ao espaço escolar serão alvo de procedimento disciplinar, de acordo com o prescrito no Regulamento Interno.

São feitas verificações semestrais, ou sempre que detetada alguma anomalia, para comprovar a eficácia dos métodos de filtragem adotados.

Decisões quanto às Políticas

AUTORIZAÇÃO DO ACESSO À INTERNET

O Agrupamento manterá um registo atualizado de todos os alunos e professores que são autorizados a aceder às comunicações eletrónicas da escola.

Todos os elementos da comunidade terão conhecimento da Política de Segurança Digital e dos recursos para a utilização segura da Internet, disponíveis no sítio *Web* do Agrupamento e serão incentivados a analisá-los com os seus educados.

RESOLUÇÃO DE INCIDENTES RELATIVOS À SEGURANÇA DIGITAL

Todos os elementos da comunidade escolar deverão informar o Coordenador da Segurança Digital caso tenham conhecimento de situações preocupantes, do ponto de vista da segurança digital (tais como violações do sistema de filtragem, *Ciberbullying*, conteúdos ilícitos, utilização inadequada de equipamento tecnológico, etc.).

As queixas relativas à utilização indevida da Internet serão tratadas no quadro dos procedimentos de apresentação de queixas ou denúncias adotadas pelo Agrupamento.

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.

Sempre que houver razões para crer ou recear que ocorreu ou está a ocorrer alguma atividade ilegal, o Agrupamento contactará a Equipa de Proteção de Menores, através do Diretor e/ou Coordenador da Segurança Digital, encaminhando a situação para as autoridades competentes.

GESTÃO DOS CASOS DE CIBERBULLYING

O *Ciberbullying* (assim como todas as outras formas de *bullying*) não será tolerado e todos os incidentes detetados serão comunicados ao Diretor e/ou Coordenador da Segurança Digital e às autoridades competentes, quando necessário.

Alunos, professores e pais/encarregados de educação serão aconselhados a manter um registo como prova.

Serão adotados procedimentos claros para investigar incidentes ou alegados casos de *Ciberbullying*.

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

Todos os elementos do Agrupamento serão sensibilizados para a importância de manterem uma conduta adequada na Internet e de não publicarem comentários, conteúdos, imagens ou vídeos na Internet que possam causar dano, prejuízo ou sofrimento a outros elementos da comunidade escolar ou atentem contra a sua idoneidade/dignidade.

As sanções para os envolvidos em *Ciberbullying* 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; a implementação de sanções, devidamente informada aos pais / encarregados de educação; o contacto e denúncia às autoridades judiciais, caso se suspeite de ação ilícita.

GESTÃO DE TELEMÓVEIS E EQUIPAMENTOS PESSOAIS

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 pelo Diretor, orientados e supervisionados pelo professor.

Os utilizadores são responsáveis por qualquer tipo de dispositivo eletrónico que traga para a escola. A escola não assume qualquer responsabilidade pela perda, roubo ou dano em tais objetos, nem por quaisquer efeitos prejudiciais para a saúde causados por estes dispositivos, sejam eles reais ou potenciais.

Não sendo autorizado o uso de telemóveis dentro da escola, os professores, outros responsáveis e os assistentes operacionais, podem solicitar o telemóvel ou outro equipamento eletrónico, conforme o estabelecido no Regulamento Interno, ou se se suspeitar que o equipamento pessoal contém materiais que podem constituir prova de uma ação ilícita. O telemóvel será entregue na direção e posteriormente entregue ao respetivo Encarregado de Educação.

Não é permitido levar telemóveis e outros equipamentos para os exames e / ou outras provas de avaliação. Os alunos que tenham um telemóvel na sua posse durante um exame estarão sujeitos às normas estabelecidas pelo Júri Nacional de Exames.

Se um aluno necessitar de contactar os pais ou encarregado de educação, deve usar o telefone da escola, sem qualquer encargo económico.

Os pais e encarregados de educação não devem contactar os filhos/educandos através do telemóvel durante a sua permanência na escola, evitando situações problemáticas para o seu educando, na medida em que os obrigam a incumprirem os deveres ou regras estabelecidas. Em caso de necessidade de contacto urgente devem usar o número de telefone da escola respetiva.

Os professores e educadores não devem utilizar os seus telemóveis ou equipamentos pessoais para contactar crianças ou jovens dentro ou fora da escola na sua qualidade de profissionais, a não ser em situações de emergência e quando outros meios de contato não estejam operacionais.

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

A captura de imagem e / ou vídeo deverá ser feita com equipamentos disponíveis em cada escola do Agrupamento de Escolas das Taipas.

Conhecimento das políticas

CONHECIMENTO DAS POLÍTICAS PELO PESSOAL DOCENTE, NÃO DOCENTE, PAIS E ENCARREGADOS DE EDUCAÇÃO

A Política de Segurança Digital está disponível, para conhecimento e consulta, no sítio *Web* do Agrupamento.

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

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

O Clube de Proteção Civil desencadeará ações que concretizem os objetivos desta Política de Segurança Digital.

POLÍTICA DE UTILIZAÇÃO ACEITÁVEL DAS INFRAESTRUTURAS TECNOLÓGICAS E DE SERVIÇOS DE TIC

A Política de Utilização Aceitável (PUA) das infraestruturas tecnológicas e de serviços de TIC do Agrupamento de Escolas das Taipas, doravante designada simplesmente PUA, complementa-se com a Política de Segurança Digital e com a Política de Privacidade e de Proteção de Dados Pessoais, em conformidade com o Regulamento Geral de Proteção de Dados (RGPD - Regulamento 2016/679 do Parlamento Europeu e do Conselho de 27 de abril de 2016) e com a Lei 58/2019 de 8 de agosto, e cumpre as exigências legalmente prescritas pelos artigos 136.º, n.º 1, e 136.º, n.º 4 do Código de Procedimento Administrativo (aprovado pelo Decreto-Lei n.º 4/2015, de 07 de Janeiro), tendo em vista a aplicação efetiva do RGPD no quadro das características do AETaipas, uma conduta digital ética e legal da comunidade escolar e a proteção dos sistemas e serviços para segurança de todos.

A garantia do respeito das regras que sustentam a PUA possibilita o correto funcionamento dos dispositivos e serviços digitais do Agrupamento.

As linhas de conduta da PUA constituem direitos e deveres dos utilizadores das redes e dos sistemas informáticos do AETaipas.

1. Objeto, âmbito de aplicação e utilizadores

A PUA tem como objetivo estabelecer os princípios orientadores da utilização adequada dos sistemas informáticos e redes de telecomunicações do Agrupamento salvaguardando o seu desígnio educativo, a sua reputação institucional e a segurança digital da organização e dos seus utilizadores. A PUA é aplicável a docentes, discentes ou alunos, assistentes operacionais, assistentes técnicos, encarregados de educação, convidados e a todos os que utilizam recursos digitais, equipamentos, redes e serviços de TIC da instituição ou na instituição.

2. Princípios de uso ético das infraestruturas tecnológicas e restrições

Na utilização das infraestruturas tecnológicas do Agrupamento aplica-se o princípio da responsabilidade. Tal implica a não aceitação de comportamentos que interfiram ou possam interferir, de forma lesiva, com outros utilizadores ou serviços, sejam eles internos ou externos ao Agrupamento, nomeadamente com o propósito do exercício de atividades ilegais ou ilegítimas, do desrespeito da integridade física e moral dos membros da comunidade escolar e de outros (tais como atos ofensivos ou discriminatórios por motivos de religião, sexo, ou género, atos de assédio sexual, pedofilia, de *bullying, cyberbullying*, racismo, xenofobia, terrorismo, difamação, *fishing*, etc.), da criação, da transmissão ou do acesso a conteúdos sem respeito pelos direitos de propriedade intelectual, de autor e conexos, de acesso não autorizado a sistemas ou infraestruturas tecnológicas das escolas do Agrupamento que vulnerabilize a sua segurança.

Ao Agrupamento reserva-se o direito de aplicar medidas de contenção nas situações onde entender que a utilização dos recursos tecnológicos não está de acordo com a sua PUA.

Assim sendo, assume-se que nenhum recurso tecnológico do Agrupamento pode ser usado:

a. Para fins não éticos ou ilegais por natureza, ou que violem o espírito de leis locais ou internacionais;
b. Para fins que entrem em conflito com a missão educativa ou políticas do AET, tais como a promoção de causas de política partidária ou a transferência ou armazenamento de

material que contenha referências obscenas ou pornográficas, propaganda e discurso de ódio;

c. Para fins comerciais, pondo em causa o nome, a reputação e a missão educativa do AET;
d. Para fins pessoais ou de terceiros, sem a permissão do Diretor;
e. Para obstrução do trabalho de terceiros, danificando equipamento deliberadamente ou consumindo quantidades exageradas dos recursos do sistema;
f. Para aceder a computadores ou sistemas confidenciais do AET;
g. Para usar os mecanismos de acesso atribuídos a outra pessoa, sem o seu consentimento e assunção de responsabilidade;
h. Para partilhar ou emprestar contas ou senhas/ palavras-passe de outros, violando o sigilo das contas e pondo em causa a segurança digital;
i. Para copiar *software* e recursos digitais do AET sem autorização do Diretor ou coordenador da PSD, tendo em vista a partilha, a cedência, ou a venda;
j. Para fins que atentem contra a segurança, a privacidade e a proteção de dados pessoais, e que se enquadrem no âmbito da criminalidade informática;
k. Para a divulgação de informação contrária aos princípios, objetivos e metas do AET, nomeadamente na criação e gestão de páginas, sites e portais associados às diferentes escolas desta unidade orgânica.

Espera-se que a conduta dos utilizadores esteja de acordo com as leis aplicáveis e com o disposto nesta PUA, sendo que a ignorância delas não serve de justificação para a sua violação.

Qualquer utilização não autorizada ou abusiva dos recursos disponibilizados pelas infraestruturas tecnológicas do AET é considerada indevida e, como tal, passível de procedimento disciplinar e, eventualmente, também criminal.

3. Identificação e autorização de utilizadores

Com exceção dos conteúdos disponibilizados publicamente, o acesso aos recursos digitais específicos do AET é efetuado mediante a atribuição de credenciais de acesso específicas.

O princípio base de criação de contas de utilizadores para acesso às infraestruturas tecnológicas do AET atende ao perfil do utilizador, bem como ao recurso e/ou serviço que o mesmo necessita de aceder, tornando-se essencial garantir um processo de atribuição de credenciais com elevado grau de confiabilidade e segurança, obrigando a uma maior responsabilização dos intervenientes em todo o processo.

O AET no processo de atribuição de identidade a utilizadores recolhe os seguintes dados: nome, telefone, *e-mail* e número de identificação do titular. As contas associadas a um utilizador são sempre acompanhadas de uma data de expiração adequada ao seu perfil, ao motivo de criação (o direito de acesso) e ao términus do vínculo.

As contas de utilizadores são criadas pelo responsável das infraestruturas tecnológicas do AET (administrador) no âmbito das suas atribuições.

As autorizações atribuídas são pessoais e intransmissíveis, competindo ao utilizador manter a confidencialidade e a proteção das credenciais fornecidas.

Para proteger a integridade dos sistemas informáticos ou para observar utilizadores suspeitos de uso não autorizado, o administrador do AET pode, quando necessário, suspender ou remover o acesso à rede ou computadores do AET, comunicando tal ao Diretor.

Todo o utilizador que encontrar uma possível quebra de segurança em qualquer sistema informático do AET deve relatá-la ao Diretor e ao coordenador da PSD. Não deve tentar usar o sistema sob estas circunstâncias até que o administrador do sistema investigue o problema.

Todo o utilizador ciente do uso não ético ou proibido de recursos informáticos do AET deve informar, de imediato, o Diretor e o coordenador da PSD.

Não é ética a conduta frívola, imprópria ou perturbadora no uso dos recursos digitais do AET. As violações das regras estabelecidas podem conduzir à suspensão da(s) conta(s) de utilizador, sem compromisso de eventual aplicação de procedimento disciplinar e/ou criminal.

4. Segurança de sistemas e redes

Não é permitido aos utilizadores a violação ou tentativa de violação dos sistemas, em especial do sistema de segurança e das redes da infraestrutura tecnológica do AET.

Assim, não são permitidas as seguintes ações:

a. Disseminação intencional de vírus, *Trojans, Malware* ou qualquer outro *software* prejudicial ou nocivo aos utilizadores da Internet;
b. Utilização de *Software* desatualizado ou com falhas conhecidas que possibilitem a sua exploração para tomar controlo do servidor, ou de *Software* sem o devido licenciamento;
c. Partilha e/ou troca de *Software* ou informação protegida por direitos de autor;
d. Recurso a *software* que permita o uso dos servidores como *Open Relay* ou *Open Proxy*;
e. Instalação de *Proxies* ou NAT - *Network Address Translation*;
f. Instalação de anonimizadores (manter suas atividades de navegação privadas);
g. Entrada ou tentativa de entrada em servidores sem autorização;
h. Uso de *cracking* (quebrar códigos de segurança), *brute-force* (ataques em massa para rastrear credenciais) ou ataques de dicionário para acessos não autorizados;
i. Deteção automática de serviços em servidores/mapear portas TCP (*Port scan*);
j. Pesquisa não autorizada de vulnerabilidades em servidores, serviços e redes;
k. Interferência intencional no bom funcionamento de servidores, serviços ou redes (ação de sobrecarga dos serviços - *Denial of service*, envio em massa de pacotes - *Flooding* e tentativas de bloqueio ou perturbação de serviço, servidores ou redes);
l. Falsificação de dados com a intenção de ludibriar e induzir em erro os recetores de dados (alterações de endereços IP - *IP Spoofing*, alterações de endereços ARP - *ARP Spoofing* e alterações dos cabeçalhos das mensagens de correio eletrónico).

5. Uso de sistemas informáticos administrativos

Os sistemas dos Serviços Administrativos do AET contêm dados escolares, financeiros e pessoais sensíveis e confidenciais. O acesso a esses sistemas é limitado unicamente a utilizadores explicitamente autorizados. Este privilégio é uma confiança e uma responsabilidade. O emprego errado do privilégio de acesso ou o acesso não autorizado aos sistemas é uma violação desta PUA.

Todo o utilizador (professor, assistente técnico, assistente operacional, aluno, ou encarregado de educação) que tenha conhecimento de uma violação desta PUA deve relatá-la ao Diretor e/ou fazer o registo do incidente pelo método estabelecido para o efeito pelo Agrupamento. A falha em relatar tal conhecimento é uma ocultação ou negligência grave, passível de procedimento disciplinar.

Os utilizadores digitais do AET que intencionalmente acedam ou facultem o acesso aos sistemas e às redes informáticas, que alterem, falseiem, adicionem, suprimam, danifiquem ou destruam dados neles contidos serão sujeitos a procedimento disciplinar e criminal se tal se justificar.

6. Correio eletrónico (*e-mail*) e política anti-SPAM

O uso abusivo do correio eletrónico poderá causar transtornos e prejuízos à infraestrutura do AET, assim como aos seus utilizadores, ao afetar o normal funcionamento dos sistemas e dos serviços digitais.

O ecossistema da *Google Suite for Education* do AET barra sistemicamente qualquer tipo de SPAM (acrónimo da locução inglesa *Sending and Posting Advertisement in Mass* - enviar e alocar publicidade em massa com intuito comercial e não solicitada pelo destinatário), evitando assim qualquer mensagem por *e-mail* que possa causar impacto negativo nos utilizadores e nas infraestruturas tecnológicas do AET ou colocar endereços IP dos utentes de correio eletrónico em listas negras.

Assim, não é permitido:

a. O envio de *SPAM*;
b. O envio de mensagens por e-mail a quem tenha solicitado o seu cancelamento;
c. O envio massivo de mensagens por *e-mail* não autorizadas (SPAMMING);
d. O envio de mensagens em cadeia (*chain letters*) ou outras mensagens de incómodo ou assédio;
e. O uso dos servidores como *SMTP "Open Proxy"* ou *"Open Relay";*
f. A utilização do *e-mail* institucional para fins ilícitos.

7. Intervenção do administrador das infraestruturas tecnológicas

Sempre que o administrador das infraestruturas tecnológicas do AET detete ou tenha conhecimento de atos abusivos nos seus servidores ou nas redes e for necessária a sua intervenção para os resolver, pode, sem qualquer consulta do(s) utilizador(es) prevaricador(es), optar por: a) avisar o infrator por *e-mail*, telefone ou pessoalmente, concedendo-lhe um prazo muito restrito para parar com o abuso ou a violação da atual PUA; b) efetuar a necessária intervenção para resolução imediata do problema, sendo o infrator sujeito à eventual indemnização de danos causados; c) suspender/ cancelar de imediato o serviço, sem aviso prévio, caso a gravidade da situação o justifique, com consequências disciplinares.

8. Monitorização do uso da Internet de acordo com a Política de Privacidade e de Proteção de dados pessoais

No cumprimento das suas obrigações institucionais e legais, nomeadamente as decorrentes da Política de Privacidade e de Segurança de Dados Pessoais, o AET monitoriza e regista a utilização das infraestruturas tecnológicas sob sua gestão, com o objetivo de conservar os registos considerados necessários para o correto suporte técnico dos equipamentos e garantir segurança das infraestruturas.

Tal monitorização é realizada em consonância com os requisitos mínimos das redes e sistemas de informação preceituados na Resolução de Conselho de Ministros 41/2018, no estrito cumprimento do interesse da organização e dos seus utilizadores.

O AET garante, assim, a não interferência nas comunicações eletrónicas protegidas por algoritmos criptográficos, respeitando os direitos, bem como a privacidade e liberdade dos seus utilizadores.

A monitorização recolhe dados referentes à utilização das infraestruturas de forma pseudonimizada, compreendendo apenas os dados necessários para os efeitos previamente identificados, nomeadamente endereço IP, endereço MAC, impressão digital do navegador, browser ou navegador de Internet utilizado e sistema operativo pelo *browser's user agent string*, portas dos protocolos TCP e UDP, data, hora, metadados relativos às camadas 3 (rede) e 4 (transporte) do modelo *Open System Interconnection* (OSI), ligações de saída e termos de pesquisa.

Na ausência de outro prazo de conservação definido nas condições de utilização próprias do serviço ou por imposição legal, os registos serão mantidos por um período máximo de 24 meses.

É expressamente proibido o acesso a estes registos a qualquer pessoa, além do Diretor e do administrador.

O acesso pelo administrador apenas é autorizado no âmbito do processo de monitorização de segurança das infraestruturas ou em situações excecionais e justificadas para despistes técnicos ou cumprimento de obrigações legais.

9. Responsabilidade de abusos, usos indevidos, ilícitos ou criminosos

O AET não assume qualquer responsabilidade institucional por abusos, usos indevidos, ilícitos ou criminosos das suas infraestruturas tecnológicas.

Tais práticas são da inteira responsabilidade do(s) seu(s) autor(es) e atentam contra a PUA, a Política de Segurança Digital, a Política de Privacidade e de Proteção de Dados Pessoais, o Projeto Educativo e o Regulamento Interno da Escola. Poderão, por isso, ser alvo de procedimento disciplinar instaurado pelo Diretor, de notificação ao Centro Nacional de Cibersegurança (nomeadamente os incidentes de *malware*; de recolha de informação acerca do sistema informático e/ou das redes, de monitorização e leitura não autorizada de tráfego de rede, ou acerca dos utilizadores ou do sistema através de métodos de Disponibilidade: disrupção da capacidade de processamento e resposta dos sistemas e redes de forma a torná-los inoperacionais, ou ação premeditada para danificar um sistema, interromper um processo, alterar ou eliminar informação, etc.. *phishing*; de intrusão[1] ou tentativa de intrusão; de quebra da segurança de informação[2]; de fraude[3]; de conteúdo abusivo[4]; ou de outra natureza), tal como no caso de violação de dados pessoais de notificação ao Centro Nacional de Proteção de Dados (nos termos do artigo 33.º do RGPD), e, em casos de ilícito criminal ou cibercriminalidade, de comunicação à Polícia Judiciária, ou ao órgão de polícia criminal competente cujo procedimento penal dependa de queixa ou de acusação particular.

10. Atualização ou alterações da PUA

O AET reserva-se o direito de, a qualquer momento, proceder a atualizações ou alterações da Política de Utilização Aceitável e de as divulgar em espaço próprio para o efeito.

[1] *Intrusão* para exploração de uma vulnerabilidade no sistema, numa componente ou na rede, ou para fazer *login* em serviços ou mecanismos de autenticação/ controlo de acesso.

[2] *Quebra da segurança de informação: por exemplo, para acesso não autorizado a um determinado conjunto de informações, ou para a sua alteração ou eliminação não autorizada.*

[3] *Fraude*: por exemplo, utilização de recursos da instituição para fins diferentes ou de utilização de nome da instituição sem autorização.

[4] *Conteúdo abusivo*: por exemplo, envio de mensagens de SPAM, de distribuição ou partilha de conteúdos protegidos por direitos de autor, ou de disseminação de conteúdos proibidos por lei

Anexos

Política de Utilização Aceitável das TIC (alunos)

Ao ler esta Política de Utilização Aceitável (PUA) declaro que:

- ☑ Compreendo que estas regras se aplicam quando utilizo a rede de Internet ou qualquer equipamento da escola, seja no seu interior ou exterior.
- ☑ Qualquer equipamento, dispositivo ou ferramenta relacionados com as Tecnologias de Informação e Comunicação, incluindo a Internet, apenas pode ser utilizado para fins escolares e quando autorizados pelo professor responsável.
- ☑ Estou proibido de realizar *downloads* ou instalar *software* em equipamento da escola, exceto com autorização expressa do professor responsável.
- ☑ Não irei revelar as minhas senhas a ninguém, exceto aos meus encarregados de educação ou a alguém responsável por mim.
- ☑ Ao utilizar as TIC irei comunicar com alunos, professores ou outras pessoas de modo responsável, respeitoso e sensato, sendo responsável pela correção do meu comportamento ao utilizar a Internet, incluindo os sites a que acedo e a linguagem que utilizo.
- ☑ De acordo com o Regulamento Interno estou proibido de utilizar telemóvel ou outro dispositivo móvel.
- ☑ Não vou deliberadamente navegar, fazer *download*, *upload* ou partilhar material que possa ser considerado ofensivo ou ilegal. Ao deparar-me com esse tipo de material irei comunicar o facto imediatamente ao professor responsável ou ao Diretor.
- ☑ Irei respeitar os direitos de autor e a propriedade intelectual do trabalho de outros.
- ☑ Não darei nenhuma informação pessoal, como nome, número de telefone ou endereço, nem vou marcar encontros com alguém conforme consta da Política de Segurança Digital.
- ☑ Vou garantir que a minha atividade *online*, tanto na escola como fora desta, não desrespeite ou ofenda de algum modo a minha escola, funcionários, alunos, professores ou outros.
- ☑ Estou proibido e serei penalizado se publicar fotos/vídeos não autorizados de colegas, funcionários, professores ou outros membros da escola.
- ☑ Caso seja vítima de *cyberbullying* ou tenha conhecimento de alguém que o seja é meu dever e obrigação informar um professor, funcionário ou o órgão de gestão.
- ☑ Utilizarei a Internet respeitando os filtros existentes e as regras gerais definidas, sabendo que a minha utilização será monitorizada pelo responsável pela rede.
- ☑ Entendo que estas regras foram criadas para minha segurança e que se as não cumprir serei responsabilizado e penalizado de acordo com a gravidade das minhas ações, além de ser dado conhecimento ao meu encarregado de educação.
- ☑ Entendo que estas são as regras gerais a adotar na escola, mas que cada espaço pode ter regras específicas pelo que devo consultar o regulamento de utilização de cada sala.
- ☑ Em caso de dúvidas sobre assuntos relacionados com a segurança na internet e a utilização responsável e segura dos equipamentos, irei procurar informação ou ajuda junto dos professores, através da Política de Segurança Digital ou em sites adequados como, por exemplo: http://www.internetsegura.pt/ http://seguranet.pt/ http://www.esafetylabel.eu/

Declaro que li (ou foi-me lida), compreendi e aceito cumprir a Política de Utilização Aceitável das TIC destinadas aos alunos.		ANO: TURMA:
Nome	Assinatura	Data

Lista de procedimentos gerais a verificar na infraestrutura da escola

Segurança técnica		Verificado
Procedimento 1	Atualização de *software* (Sistemas Operativos, *firewalls* e aplicações, incluindo antivírus), de todo o parque escolar.	
Procedimento 2	Atualização do documento orientador de Políticas de Utilização de meios digitais, no que respeita à segurança técnica.	
Procedimento 3	Atualização e configuração dos sítios de internet restritos.	
Procedimento 4	Proposta de formação das diferentes estruturas da escola sobre práticas de utilização segura e responsável da Internet.	
Acesso de alunos e professores às tecnologias		
Procedimento 1	Configuração da rede sem fios para o acesso seguro de dispositivos externos. Prosseguir as boas práticas atuais de criação de credenciais de acesso, por utilizador e tipo de utilizador.	
Procedimento 2	Atualização do documento orientador de Políticas de Utilização de meios digitais, no que respeita ao acesso das tecnologias digitais.	
Proteção de dados		
Procedimento 1	Prosseguir as boas práticas atuais de criação de credenciais de acesso à estrutura tecnológica.	
Procedimento 2	Atualizar e criar códigos de conduta, para demonstrar a conformidade com os princípios da proteção de dados (RGPD).	
Procedimento 3	Continuar a monitorar o estado e acesso às infraestruturas.	
Gestão informática		
Procedimento 1	Atualização dos registos de ocorrência/solicitação, tendo em consideração os novos equipamentos e necessidades da estrutura.	
Procedimento 2	Atualização do documento orientador de Políticas de Utilização de meios digitais de forma a contemplar os novos equipamentos institucionais.	
Recursos		
Procedimento 1	Garantir uma informação atualizada de todas as páginas, páginas de perfil, sites, portais e aplicações eletrónicas que utilizem o logótipo e/ou nome do AET ou escolas que integram o AET.	
Procedimento 2	Monitorizar e recomendar a criação/funcionamento e publicação de conteúdos nos suportes anteriores	

Declaração de consentimento prévio do titular dos dados pessoais

Proteção de Dados (RGPD) - Política de Privacidade do AET

Encarregados de Educação

Ao aceitar a Política de Privacidade, está a autorizar o Agrupamento de Escolas das Taipas a proceder ao tratamento dos seus dados pessoais e dos dados pessoais do seu educando.

Declara, ainda:

- Estar ciente e plenamente informado/a de que o tratamento dos seus dados pessoais e os dados pessoais do seu educando inclui todas as operações efetuadas sobre os dados por si transmitidos, por meios automatizados ou não, necessários à frequência do estabelecimento de ensino e ao desenvolvimento de todo o processo educativo, de acordo com a legislação em vigor.
- Aceitar e consentir que os seus dados e os dados pessoais do seu educando sejam transmitidos a outras entidades públicas, ou privadas na condição de subcontratantes, exclusivamente para fins legais e no exercício das atribuições e competências da presente instituição.
- Tomar conhecimento que os seus dados e os dados pessoais do seu educando serão guardados pelo período de tempo fixado em lei, regulamento ou o estritamente necessário às finalidades para que foram recolhidos.
- Tomar conhecimento que, nos termos da legislação aplicável, é garantido, a todo o tempo, o exercício (i) dos direitos de acesso, retificação, atualização e eliminação (apagamento) dos seus dados pessoais e dos dados pessoais do seu educando, podendo ainda opor-se ao tratamento dos mesmos mediante pedido escrito dirigido ao Diretor do Agrupamento, bem como (ii) do direito de apresentar queixa junto Comissão Nacional de Proteção de Dados através do Website - www.cnpd.pt.
- Prestar o presente consentimento de forma livre e voluntária;
- Estar ciente que o tratamento dos dados é necessário ao exercício das funções de interesse público que incumbem ao Agrupamento de Escolas das Taipas, sendo realizado em conformidade com as respetivas obrigações jurídicas previstas na lei.

Data: 3 de setembro de 2022

O/A Encarregado/a de Educação: _____

Regulamento Geral de Proteção de Dados (RGPD)

A proteção dos dados pessoais dos nossos alunos e encarregados de educação sempre foi uma preocupação. Sem prejuízo das adaptações que sejam necessárias introduzir nas nossas práticas em função do RGPD e legislação nacional, os vossos dados sempre estiveram seguros connosco. Todos os dados pessoais de alunos e encarregados de educação que temos em posse, são recolhidos no âmbito da relação de prestação de serviços educativos que estabelecemos com a comunidade educativa e para dar cumprimento a obrigações legais estabelecidas pelo Ministério da Educação.

A instituição, no âmbito da sua atividade, procede ao tratamento dos dados pessoais estritamente necessários à prestação de serviços ou ao exercício da sua missão ou atribuições legais, nomeadamente:

Identificação pessoal do aluno	Dados necessários para o cumprimento da prestação de serviços educativos, cumprindo-nos a obrigação legal de os recolher e transmitir ao Ministério da Educação, ou outras entidades oficiais da administração central e/ou da administração local; estes dados podem ainda ser cedidos, se necessário a entidades de saúde, em caso de acidente escolar, ao Ministério Público e à CPCJ.
Identificação pessoal dos pais e encarregados de educação e dados de contacto	Dados necessários para o cumprimento da prestação de serviços educativos.
Dados de saúde do aluno (vacinas e situações de que padeça)	
Dados de aproveitamento escolar do aluno	Dados necessários para o cumprimento da prestação de serviços educativos, cumprindo-nos a obrigação legal de os recolher e transmitir ao Ministério da Educação no caso de avaliação sumativa final.

Os dados recolhidos são tratados no estrito cumprimento da legislação de proteção de dados pessoais.

Em situação alguma os dados recolhidos serão utilizados para outra finalidade que não seja aquela para a qual se encontra legalmente estabelecida ou para a qual foi dado o consentimento por parte do titular dos dados. Para as situações em que alguns dos dados possam vir a ser necessários, como no caso de vistas de estudo, fotografias/vídeos dos alunos para qualquer uso interno ou externo de representação do AET, ou outra situação particular e pontual, serão pedidas autorizações.

Parecer positivo/Aprovado em Conselho Pedagógico de 1 de junho de 2022	Aprovado em Conselho Geral de 26 de julho de 2022
João Montes - Diretor	Cláudia Vieira – Presidente do CG

O período de tempo, durante o qual os dados são armazenados e conservados, é o legal ou o regulamentarmente fixado, ou o estritamente necessário, de acordo com a finalidade para a qual a informação é tratada, cumprindo as disposições contidas no Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho de 27 de abril de 2016 (Regulamento Geral de Proteção de Dados) e na Resolução do Conselho de Ministros 41/2018 (requisitos técnicos das redes e sistemas de informação).