CONSCIOUS YOUTH BEHAVIOURS IN EMERGING REALITIES

R5. Documento de Recomendações Políticas sobre Segurança de Dados e Cibersegurança, especificamente adaptado às escolas, seguindo as normas ISO 27001, 27002, 27701, 22301 e 31000

Comportamentos Conscientes dos Jovens em Realidades Emergentes

Parceiro responsável: SIGMA BUSINESS NETWORK, Grécia

Co-funded by the European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

Informação do Documento

Contrato nº	**2023-1-EL01-KA220-SCH-000156982**
Acrónimo	**C.Y.B.E.R.**
Título	**Conscious Youth Behaviours in emerging realities**
Data de início:	16/11/2023
Resultado:	Documento de Recomendações Políticas R5
Atividades Relacionadas:	A4.5 - Conceção e desenvolvimento do R5
Organização responsável:	SIGMA Tournis Symvouleftiki EE, Grécia
Parceiros Contribuintes:	• PRISM IMPRESA SOCIALE S.R.L., Itália • Centro Distrital de Recursos e Assistência Educativa de Botoşani, Roménia • CPM-Centrum Prevencie Mladeze, Eslováquia • Casa Do Professor, Portugal • Vitale Tecnologie Comunicazione - VITECO SRL, Itália • EUROCERT Eyropaiki Etaireia Emeghon Kai Pistopoihseon Anonymos Etaireia, Grécia
Nível de Divulgação	Público
Aviso Legal	O apoio da Comissão Europeia à produção desta publicação não constitui um aval do seu conteúdo, que reflete apenas as opiniões dos autores, e a Comissão não pode ser responsabilizada por qualquer uso que possa ser feito das informações nela contidas

Histórico do Documento

Data	Submetido por	Revisto por	Versão (Notas)
26/06/2026	SIGMA	Theodora Ntinou	1.0

Sobre o projeto CYBER	
Tipo de ação	Erasmus+ KA220-SCH - Parcerias de cooperação no ensino escolar
Prioridade	EDUCAÇÃO ESCOLAR: Desenvolvimento de competências-chave ▪ Responder à transformação digital através do desenvolvimento da preparação, resiliência e capacidade digitais ▪ Inclusão e diversidade em todos os domínios da educação, formação, juventude e desporto

O projeto visa responder a uma questão fundamental: de que forma o ciberespaço influencia o comportamento humano, em particular o dos jovens? Na era digital atual, o comportamento em linha tornou-se profundamente enraizado no ambiente psicológico do ciberespaço. Este oferece oportunidades únicas para moldar a interação humana, mas também suscita preocupações devido à sua natureza sem fronteiras. Embora a internet traga inegáveis benefícios sociais e económicos, tem colocado em causa valores europeus fundamentais como a igualdade, os direitos humanos e a democracia. Para construir uma internet mais segura, é essencial um esforço coletivo. Partilhar boas práticas e educar as gerações mais jovens, os professores e os pais são passos fundamentais para promover um ambiente em linha mais seguro.

O CYBER procura desenvolver a resiliência cibernética das escolas europeias, criando procedimentos de qualidade da UE adaptados ao sistema escolar e dotando professores e alunos das ferramentas e conhecimentos necessários para discutir os comportamentos conscientes e inconscientes dos adolescentes em linha, a ciberpsicologia e as desvantagens do uso excessivo da internet, de modo a reforçar, em sala de aula, a compreensão dos comportamentos de risco emergentes a que um jovem utilizador pode estar exposto.

O CYBER irá estruturar uma metodologia para integrar, na sala de aula e no sistema escolar, os temas fundamentais das ciberameaças e da ciberpsicologia, promovendo o diálogo entre os alunos sobre os comportamentos de risco emergentes em relação a si próprios e aos seus pares. Além disso, o projeto define procedimentos claros em matéria de cibersegurança e proteção de dados, para que as escolas possam obter a certificação CYBER, com requisitos para estabelecer, implementar, manter e melhorar a gestão da segurança da informação na escola.

Os resultados do projeto destinam-se a beneficiar todos os adolescentes em todos os países europeus, especialmente os que nasceram na era digital. O contexto social nestas matérias (pirataria de perfis, notícias falsas, identidades falsas, fraude/burla em linha, chantagem em linha, pornografia de vingança, hikikomori, ciberbullying, etc.) assume um valor acrescido, em que a educação e a sensibilização dos jovens para o problema têm um impacto muito maior do que uma regra nacional.

Índice

Conteúdo

Introdução

Este documento é a Política de Resiliência Cibernética para Escolas, desenvolvida no âmbito do projeto C.Y.B.E.R. (Comportamentos Conscientes dos Jovens em Realidades Emergentes). O projeto é cofinanciado pela União Europeia ao abrigo do Programa Erasmus+ e reúne organizações parceiras da Grécia, Itália, Portugal, Roménia e Eslováquia.

As escolas de hoje dependem fortemente da tecnologia digital. Os alunos utilizam plataformas em linha para aprender, os professores comunicam através de ferramentas digitais e o pessoal administrativo gere registos em sistemas ligados em rede. Trata-se de um desenvolvimento positivo, mas significa também que as escolas enfrentam riscos que antes não existiam: ciberataques, violações de dados, ciberbullying e o impacto da vida digital na saúde mental dos alunos.

Esta política foi concebida para ajudar todas as escolas dos cinco países parceiros a enfrentar estes desafios de forma prática. Reúne, num único documento que qualquer escola pode ler e utilizar, a legislação europeia, as regras nacionais de cada país, as normas de segurança reconhecidas internacionalmente e a melhor investigação disponível.

Este não é um manual técnico. É um guia para todas as pessoas que trabalham numa escola: a direção, os professores, o pessoal administrativo e os coordenadores de informática. Não é necessária formação jurídica ou técnica para o utilizar. A política explica o que a lei exige, o que constitui boa prática e o que a sua escola precisa de fazer.

Os modelos e as ferramentas disponibilizados nos anexos foram concebidos como pontos de partida adaptáveis. As escolas são encorajadas a adaptá-los ao seu contexto legal nacional, aos seus procedimentos internos e às suas circunstâncias específicas.

A Quem se Destina Esta Política

Esta política destina-se a todos os que participam na gestão de uma escola: a direção, a subdireção, os professores, os coordenadores de informática, o pessoal administrativo e os órgãos de gestão escolar. Foi redigida para ser compreendida por qualquer pessoa, independentemente da sua formação.

Como Está Organizado Este Documento

Parte	Conteúdo
Parte 1: O Quadro Legal	O que a legislação europeia exige que as escolas façam, explicado em linguagem simples.
Parte 2: As Regras do Seu País	As regras nacionais específicas aplicáveis em cada um dos cinco países.
Normas Internacionais e Escolas	Como cinco normas de gestão reconhecidas internacionalmente moldam as recomendações práticas desta política.
Parte 3: O Que a Sua Escola Deve Fazer	Passos práticos organizados por tema, com base em normas internacionais e na legislação da UE.

Parte	Conteúdo
Parte 4: O Que a Evidência Demonstra	O que a investigação científica nos diz sobre o que realmente funciona nas escolas.
Anexos	Documentos-modelo e ferramentas práticas de implementação para as escolas adaptarem e utilizarem diretamente.
Referências	Os instrumentos legislativos nacionais e as fontes oficiais utilizados na preparação da Parte 2.

Parte 1: O Quadro Legal

As escolas dos cinco países parceiros devem cumprir a legislação europeia que rege o tratamento de dados e a proteção dos alunos em linha. Esta parte explica, em linguagem simples, o que essa legislação exige. Existem seis instrumentos legais principais que todas as escolas precisam de conhecer. Em conjunto, abrangem a proteção de dados, a cibersegurança, a inteligência artificial, as plataformas em linha, as comunicações digitais e a segurança dos produtos digitais.

1.1 Regulamento Geral sobre a Proteção de Dados (RGPD)

O RGPD é a base da proteção de dados na Europa. Aplica-se a todas as organizações que tratam dados pessoais, incluindo as escolas. Numa escola, os dados pessoais incluem nomes e números de identificação dos alunos, registos de assiduidade, notas, informações de saúde, fotografias e qualquer outra informação relativa a uma pessoa identificável.

O RGPD reconhece as crianças como um grupo particularmente vulnerável. As escolas devem, por isso, aplicar um padrão de cuidado mais elevado no tratamento dos dados dos alunos do que aplicariam no caso de adultos.

O que o RGPD exige das escolas:

- As escolas devem ter uma base jurídica clara para cada atividade de tratamento de dados. Na maioria dos casos, tratar-se-á de uma obrigação legal exigida pela legislação nacional de educação, de uma missão de interesse público necessária ao funcionamento da escola ou, nalguns casos, do consentimento.
- As escolas só devem recolher os dados de que realmente necessitam. Não devem recolher informação adicional apenas porque pode vir a ser útil um dia.
- As escolas devem nomear um Encarregado de Proteção de Dados (EPD). Consoante o país, esta função pode ser assegurada a nível de agrupamento ou de autoridade, em vez de individualmente por cada escola.
- As escolas devem realizar uma Avaliação de Impacto sobre a Proteção de Dados (AIPD) antes de introduzir qualquer novo sistema digital que envolva o tratamento em grande escala de dados dos alunos ou a monitorização comportamental. O Anexo V inclui um modelo.
- As escolas devem comunicar as violações de dados pessoais à autoridade de supervisão nacional no prazo de 72 horas após terem conhecimento das mesmas.
- As escolas devem informar os alunos e os pais sobre a forma como os seus dados são utilizados, em linguagem clara e simples.

- Os alunos e os pais têm o direito de aceder aos dados que lhes dizem respeito, de solicitar correções e, nalgumas circunstâncias, de solicitar o seu apagamento.

Idade de Consentimento Digital

O RGPD permite que cada país da UE fixe a idade a partir da qual um jovem pode consentir na utilização de plataformas digitais sem aprovação parental. Esta idade varia entre os 13 e os 16 anos nos cinco países parceiros. Para os alunos abaixo da idade nacional de consentimento digital, as escolas devem obter o consentimento escrito dos pais ou encarregados de educação antes de os inscrever em plataformas digitais. A idade específica para cada país está indicada na Parte 2.

1.2 Diretiva NIS2

A Diretiva NIS2 estabelece um quadro europeu comum para a cibersegurança. Exige que as organizações disponham de medidas de cibersegurança adequadas, gerem os riscos colocados pelos seus fornecedores digitais e comuniquem os incidentes de cibersegurança significativos à autoridade nacional.

As escolas nem sempre são diretamente classificadas como entidades essenciais ou importantes ao abrigo da NIS2. No entanto, as escolas dependem fortemente de sistemas digitais, e os incidentes de cibersegurança que afetem esses sistemas podem perturbar o ensino e colocar em risco os dados dos alunos. O quadro da NIS2 estabelece o padrão que todas as escolas devem procurar alcançar, independentemente de estarem ou não formalmente classificadas.

O que a NIS2 significa para as escolas:

- As escolas devem implementar medidas de cibersegurança proporcionais aos riscos que enfrentam. No mínimo, isto significa palavras-passe fortes, cópias de segurança regulares e redes protegidas.
- As escolas devem verificar as práticas de cibersegurança dos seus fornecedores digitais. Uma plataforma utilizada para registos de alunos deve ser tão segura como a própria escola.
- As escolas devem dispor de um procedimento para detetar e responder a incidentes de cibersegurança. O pessoal deve saber a quem contactar e que passos seguir.
- As escolas devem proporcionar formação regular de sensibilização para a cibersegurança a todo o pessoal.
- Os incidentes significativos devem ser comunicados à autoridade nacional de cibersegurança. Os prazos e as autoridades variam consoante o país. Ver Parte 2.

1.3 Regulamento da UE sobre Inteligência Artificial

O Regulamento da IA é a primeira lei europeia abrangente que rege a utilização da inteligência artificial. Entrou em vigor em agosto de 2024 e aplica-se progressivamente até à sua implementação total em agosto de 2026. As escolas utilizam cada vez mais ferramentas apoiadas em IA: plataformas de aprendizagem adaptativa, sistemas automáticos de avaliação, chatbots e análise de dados de aprendizagem. O Regulamento da IA estabelece regras claras sobre como estas ferramentas podem e não podem ser utilizadas.

O que o Regulamento da IA exige das escolas:

- Determinados usos da IA nas escolas são totalmente proibidos. Incluem-se aqui os sistemas de reconhecimento de emoções utilizados para monitorizar os alunos, a categorização biométrica dos alunos e o reconhecimento facial em tempo real em contextos educativos. Não existem exceções para as escolas.
- Os sistemas de IA utilizados para avaliação de alunos, admissões ou monitorização são classificados como de risco elevado e devem cumprir requisitos rigorosos de transparência, supervisão humana e documentação.
- Os alunos e os pais devem ser informados quando as ferramentas de IA são utilizadas de forma a afetar decisões educativas.
- Um professor deve sempre rever e assumir a responsabilidade por qualquer recomendação gerada por IA que afete um aluno. A IA não pode tomar decisões finais sobre os alunos.
- As escolas devem manter uma lista escrita de todas as ferramentas de IA em uso, incluindo o que cada ferramenta faz e que dados processa.

1.4 Regulamento dos Serviços Digitais (DSA)

O DSA regula as plataformas em linha e os serviços digitais. Exige que as plataformas sejam mais transparentes, disponibilizem formas acessíveis de denunciar conteúdos nocivos e reforcem a proteção dos jovens. As escolas têm um papel importante em ajudar os alunos a compreender como funcionam as plataformas em linha e como se proteger.

O que o DSA significa para as escolas:

- As escolas devem ensinar os alunos a reconhecer e denunciar conteúdos nocivos nas plataformas que utilizam.
- As escolas devem ajudar os alunos a compreender como funcionam os algoritmos de recomendação e como estes moldam o que os jovens veem em linha.
- Os professores devem estar cientes das obrigações que o DSA impõe às grandes plataformas e ser capazes de as discutir com os alunos no âmbito da literacia digital.

1.5 Diretiva ePrivacy

A Diretiva ePrivacy protege a confidencialidade das comunicações eletrónicas. Aplica-se a sistemas de correio eletrónico, plataformas de mensagens, ferramentas de videoconferência e a qualquer outro serviço de comunicação digital utilizado nas escolas.

O que a Diretiva ePrivacy significa para as escolas:

- As comunicações digitais entre alunos, pais, professores e pessoal administrativo devem ser seguras e confidenciais.
- As ferramentas de videoconferência utilizadas para o ensino à distância devem ser configuradas de modo a impedir acessos não autorizados. As salas de aula virtuais devem exigir autenticação antes de qualquer pessoa poder entrar.
- As aulas e reuniões não devem ser gravadas sem o consentimento explícito de todos os participantes.
- Os sítios web e plataformas escolares que utilizem cookies devem apresentar um aviso de cookies em conformidade.

1.6 Regulamento sobre a Cibersegurança

O Regulamento sobre a Cibersegurança reforça o papel da ENISA, a Agência da UE para a Cibersegurança, e estabelece um quadro europeu para a certificação da segurança de produtos e serviços digitais. Apoia a adoção de tecnologias fiáveis em toda a UE, incluindo nas escolas.

O que o Regulamento sobre a Cibersegurança significa para as escolas:

- Ao escolherem ferramentas, plataformas ou equipamentos digitais, as escolas devem ter em conta a cibersegurança e privilegiar, sempre que possível, produtos certificados ou aprovados.
- Os dispositivos de sala de aula ligados em rede, como quadros interativos, tablets e câmaras, devem ser configurados de forma segura e mantidos atualizados.
- As escolas podem consultar as orientações e ferramentas da ENISA para as ajudar a planear a sua abordagem em matéria de cibersegurança.

1.7 Como Estas Leis Funcionam em Conjunto

Estes seis instrumentos legais não são obrigações separadas a tratar uma a uma. Formam um quadro integrado. Uma escola que proteja os dados dos alunos ao abrigo do RGPD, gere a cibersegurança ao abrigo da NIS2, utilize a IA de forma responsável ao abrigo do Regulamento da IA, ensine literacia digital em conformidade com o DSA, proteja as suas comunicações ao abrigo da Diretiva ePrivacy e selecione tecnologias fiáveis em conformidade com o Regulamento sobre a Cibersegurança terá cumprido a totalidade das suas obrigações legais.

Legislação	A obrigação-chave para as escolas
RGPD	Proteger os dados pessoais, nomear um EPD, obter consentimento quando necessário, comunicar violações no prazo de 72 horas.
Diretiva NIS2	Dispor de medidas de cibersegurança, verificar os fornecedores, comunicar incidentes, formar o pessoal.
Regulamento da UE sobre IA	Não utilizar IA proibida, manter as pessoas no controlo das decisões, informar alunos e pais.
Regulamento dos Serviços Digitais	Ensinar os alunos a denunciar conteúdos nocivos e a compreender como funcionam os algoritmos.
Diretiva ePrivacy	Proteger as comunicações digitais, proteger as salas de aula virtuais, cumprir as regras relativas a cookies.
Regulamento sobre a Cibersegurança	Ter em conta a segurança ao adquirir tecnologia, proteger os dispositivos ligados em rede, utilizar as orientações da ENISA.

Parte 2: O Que se Aplica no Seu País

A legislação europeia estabelece o quadro comum, mas cada país tem também as suas próprias leis e orientações nacionais que as escolas devem seguir. Esta parte resume as regras nacionais mais

importantes de cada um dos cinco países parceiros. Encontre o seu país e verifique o que se aplica ao seu caso.

2.1 Grécia

A Grécia opera um modelo altamente centralizado de governação digital escolar. A cibersegurança, a proteção de dados e a infraestrutura digital são geridas essencialmente a nível nacional pelo Ministério da Educação e pelo Ministério da Governação Digital. As escolas individuais funcionam sobretudo como utilizadoras de sistemas geridos centralmente, incluindo o sistema de informação de alunos MySchool, a plataforma de aprendizagem e-Class e a Rede Escolar Pan-Helénica (PSN).

Área	O Que Significa para as Escolas
Transposição da NIS2 Lei 5160/2024 Despacho Ministerial 1689/2025 Despacho Ministerial 1899/2025	• As escolas devem implementar medidas de gestão de risco e assegurar que as plataformas digitais de terceiros (por exemplo, Webex) cumprem as normas de cibersegurança. • Comunicação obrigatória de incidentes: as escolas devem notificar a EAKE de incidentes de cibersegurança significativos. • São exigidas políticas de segurança formais que abranjam o controlo de acesso aos dados dos alunos, os procedimentos de cópia de segurança, a encriptação das comunicações e a segurança da cadeia de fornecimento de software e hardware utilizados nas escolas. • É exigida formação do pessoal e higiene cibernética: o pessoal escolar é frequentemente alvo de ataques de phishing e de engenharia social. • As escolas devem manter documentação que inclua políticas de segurança, registos de formação, diagramas de rede e resultados de auditorias de segurança periódicas. • O Despacho Ministerial 1899/2025 exige a designação de um responsável pela cibersegurança e procedimentos formais de resposta a incidentes e de escalonamento.
Proteção de Dados Lei 4624/2019	• Rege o tratamento de dados pessoais por organismos do setor público, incluindo escolas, em conformidade com os princípios do RGPD. • Estabelece o papel e os poderes de supervisão da Autoridade Helénica de Proteção de Dados (HDPA). • As responsabilidades do EPD são geridas a nível de autoridade, e não individualmente por cada escola. • As escolas devem notificar a HDPA (Autoridade Helénica de Proteção de Dados) no prazo de 72 horas relativamente a qualquer violação de dados pessoais suscetível de criar um risco para os titulares dos dados. • As escolas devem implementar medidas de segurança adequadas para os dados de alunos, pais e pessoal.
Idade de Consentimento Digital	• 15 anos. • As escolas devem obter o consentimento escrito dos pais ou encarregados de educação antes de inscrever alunos com

Área	O Que Significa para as Escolas
	menos de 15 anos em qualquer plataforma digital que trate os seus dados pessoais.
Ciberbullying Lei 5029/2023	• Estabelece um quadro jurídico estruturado para a prevenção e gestão do ciberbullying nas escolas. • Cria a plataforma nacional de denúncia stop-bullying.gov.gr para a submissão formal e o acompanhamento de incidentes. • As escolas devem participar ativamente na identificação, comunicação e gestão de casos de ciberbullying. • As escolas devem dispor de um procedimento escrito para responder a incidentes de ciberbullying.
Telemóveis	• É proibido aos alunos possuir ou utilizar telemóveis nas instalações escolares. • Política de tolerância zero em vigor desde 2024. • As infrações têm consequências disciplinares imediatas, incluindo a suspensão.
IA na Educação	• Não foram emitidas orientações nacionais específicas sobre a utilização da IA nas escolas. • O Regulamento da UE sobre IA aplica-se diretamente. • As escolas devem ter cautela ao utilizar ferramentas de IA que tratam dados dos alunos.
Infraestrutura Digital	• MySchool: sistema nacional de informação de alunos, gerido centralmente. • e-Class: plataforma nacional de gestão da aprendizagem. • Rede Escolar Pan-Helénica (PSN): infraestrutura nacional de conectividade segura para todas as escolas públicas.
Contactos Principais	• Cibersegurança: EAKE (cyber.gov.gr) • Proteção de Dados: HDPA (dpa.gr) • Cyberbullying: stop-bullying.gov.gr

2.2 Itália

A Itália opera um modelo predominantemente centralizado, embora as escolas mantenham um certo grau de autonomia organizacional. A Agência Nacional de Cibersegurança (ACN) desempenha um papel central na coordenação e na gestão de incidentes. As escolas dependem fortemente das orientações ministeriais e das plataformas geridas centralmente, incluindo a plataforma nacional Unica. O Garante emitiu orientações e perguntas frequentes específicas para as escolas, que estas devem consultar em conjunto com o RGPD.

Área	O Que Significa para as Escolas
Transposição da NIS2	• O Decreto Legislativo 138/2024 define expectativas em matéria de avaliação de risco, segurança dos fornecedores e

Área	O Que Significa para as Escolas
Decreto Legislativo 138/2024 Lei 109/2021	comunicação de incidentes, mesmo para escolas não diretamente classificadas como entidades NIS. • As escolas devem gerir os serviços de TIC de terceiros e manter canais de comunicação estruturados quando os incidentes afetam as atividades educativas ou os dados dos alunos. • A Lei 109/2021 cria a Agência Nacional de Cibersegurança (ACN), que desempenha um papel central de coordenação da governação da cibersegurança nas instituições públicas, incluindo as escolas.
Proteção de Dados Decreto Legislativo 196/2003 (com as alterações introduzidas pelo Decreto 101/2018)	• Rege o tratamento dos dados de alunos, pais, professores e pessoal no âmbito das atividades escolares. • A autoridade de supervisão é o Garante per la protezione dei dati personali. • A designação de EPD é obrigatória para as escolas públicas, podendo ser organizada a nível de escola ou através de acordos partilhados entre várias escolas. • É exigida autorização parental para o tratamento de dados de crianças sempre que os serviços digitais sejam oferecidos diretamente a alunos abaixo da idade de consentimento digital. • As escolas devem informar os alunos e os pais sobre os seus direitos em matéria de dados e gerir as violações de dados em conformidade com os requisitos do RGPD.
Idade de Consentimento Digital	• 14 anos. • É exigido o consentimento parental para alunos com menos de 14 anos relativamente à inscrição em sistemas de gestão da aprendizagem, à publicação de fotografias e a qualquer tratamento que envolva menores em contexto educativo.
Ciberbullying Lei 71/2017	• Estabelece um quadro jurídico para o combate ao ciberbullying nas escolas. • As escolas devem dispor de procedimentos escritos para lidar com incidentes e apoiar as vítimas. • As escolas podem solicitar a remoção de conteúdos nocivos das plataformas em linha.
Telemóveis Nota MIM 5274/2024 Circular MIM 3392/2025	• Os smartphones são restringidos durante todas as atividades escolares em todos os ciclos de ensino. • As restrições visam proteger o ambiente educativo e promover uma utilização das ferramentas digitais adequada à idade. • Aplicam-se exceções limitadas para atividades educativas específicas ou necessidades de acessibilidade.

Área	O Que Significa para as Escolas
IA na Educação Decreto Ministerial 166/2025	• As orientações nacionais exigem transparência quanto à utilização da IA nas escolas. • A supervisão humana das decisões educativas apoiadas por IA é obrigatória. • As ferramentas de IA que tratam dados dos alunos devem cumprir os requisitos do RGPD.
Plataformas Digitais	• Unica: plataforma nacional para funções administrativas e educativas. • Microsoft 365 for Education: pacote gerido institucionalmente para o ensino e a comunicação. • O quadro de Ensino Digital Integrado (DDI) (Decreto Ministerial 89/2020) exige que as escolas regulem a utilização de plataformas digitais, o acesso dos alunos e as responsabilidades dos professores em ambientes educativos em linha.
Contactos Principais	• Cibersegurança: ACN (acn.gov.it) • Proteção de Dados: Garante (garanteprivacy.it)

2.3 Portugal

Portugal possui um dos quadros nacionais mais estruturados de governação digital escolar entre os cinco países. As escolas beneficiam do PADDE obrigatório (Plano de Ação para o Desenvolvimento Digital da Escola), do programa de apoio SeguraNet e do CERT.PT para a resposta a incidentes. A Diretiva NIS2 foi transposta através do Decreto-Lei n.º 125/2025, que entrou em vigor a 3 de abril de 2026.

Área	O Que Significa para as Escolas
Transposição da NIS2 Decreto-Lei n.º 125/2025 (em vigor desde 3 de abril de 2026) Lei n.º 46/2018	• As escolas classificadas como Entidades Públicas Relevantes (Grupo A ou B) devem implementar medidas de gestão de risco em matéria de cibersegurança. • Designação obrigatória de um responsável pela cibersegurança. • Os incidentes significativos devem ser comunicados ao CNCS no prazo de 24 horas. • As escolas devem identificar os ativos digitais críticos, estabelecer procedimentos de resposta a incidentes e assegurar a continuidade das operações. • A Lei n.º 46/2018 continua a ser o quadro fundador que estabelece o CNCS como autoridade nacional de cibersegurança.
Proteção de Dados Lei n.º 58/2019	• É obrigatória a existência de um EPD a nível de cada agrupamento de escolas, e não de cada escola individual. • O EPD deve estar registado junto da CNPD (Comissão Nacional de Proteção de Dados) e é responsável por monitorizar a

Área	O Que Significa para as Escolas
	conformidade com o RGPD, aconselhar o pessoal, realizar formação e assegurar a ligação com a CNPD. ● As escolas devem notificar a CNPD no prazo de 72 horas relativamente a uma violação de dados pessoais suscetível de criar um risco para os titulares dos dados. ● As escolas devem manter um registo das atividades de tratamento e implementar medidas de segurança adequadas.
Idade de Consentimento Digital	● 13 anos. Este é o limiar mais baixo entre os cinco países. ● É exigido consentimento parental ou do encarregado de educação verificável antes de inscrever alunos com menos de 13 anos em qualquer plataforma digital ou ferramenta em linha que trate dados pessoais. ● Isto aplica-se aos sistemas de gestão da aprendizagem, à publicação de fotografias e a qualquer tratamento que envolva menores.
Ciberbullying Programa SeguraNet	● O SeguraNet (gerido pela DGE em parceria com o CNCS) fornece orientações específicas sobre a prevenção e resposta ao ciberbullying. ● As escolas devem integrar a prevenção do ciberbullying no seu PADDE e no regulamento interno. ● Modelos de procedimentos de resposta a incidentes e de Política de Utilização Aceitável estão disponíveis através do SeguraNet.
Telemóveis Decreto-Lei n.º 95/2025 (em vigor desde setembro de 2025)	● Os smartphones são legalmente proibidos para todos os alunos do 1.º ao 6.º ano, em todas as escolas públicas e privadas. ● Para o 3.º ciclo e o ensino secundário, o Ministério emitiu recomendações que incentivam restrições, mantendo as escolas autonomia para formalizar regras no seu regulamento interno. ● Qualquer gravação de alunos exige consentimento explícito nos termos do RGPD.
Plano Digital de Escola Obrigatório Quadro do PADDE	● Cada agrupamento de escolas deve elaborar e manter um PADDE (Plano de Ação para o Desenvolvimento Digital da Escola). ● O PADDE deve incluir explicitamente medidas de cibersegurança e abrange três dimensões: organizacional (liderança e governação), pedagógica (cidadania digital e educação para uma internet segura) e tecnológica (infraestrutura e segurança). ● As escolas devem adotar uma Política de Utilização Aceitável e estabelecer procedimentos de resposta a incidentes com referência ao CERT.PT.
IA na Educação	● Ainda não foram emitidas orientações nacionais específicas.

Área	O Que Significa para as Escolas
	• O Regulamento da UE sobre IA aplica-se diretamente. • A DGE reconheceu a necessidade de um quadro nacional, prevendo-se a emissão de recomendações. • As escolas devem ter cautela ao utilizar ferramentas de IA que tratam dados dos alunos.
Infraestrutura Digital	• RCTS (gerida pela FCCN): rede nacional segura de alta velocidade para todos os agrupamentos de escolas públicas. • Microsoft 365 for Education: pacote gerido nacionalmente para o ensino e a comunicação. • CERT.PT (operado pelo CNCS): CSIRT nacional e ponto de contacto para a resposta a incidentes no setor da educação.
Contactos Principais	• Cibersegurança: CNCS (cncs.gov.pt) • Resposta a Incidentes: CERT.PT • Proteção de Dados: CNPD (cnpd.pt) • Segurança Digital: SeguraNet (seguranet.pt)

2.4 Roménia

O quadro nacional é coordenado pelo Ministério da Educação em colaboração com a Diretoria Nacional de Cibersegurança (DNSC), no âmbito do quadro mais amplo de política de cibersegurança nacional e europeia. Em muitas escolas, as responsabilidades relacionadas com a cibersegurança são assumidas pela direção da escola, pelo coordenador de TIC ou por um professor designado, uma vez que a existência de pessoal dedicado à cibersegurança é pouco comum. A Roménia enfrenta algumas das maiores lacunas de implementação entre os cinco países parceiros, mas há um impulso crescente para as colmatar.

Área	O Que Significa para as Escolas
Transposição da NIS2 OUG 155/2024 (aprovada pela Lei 124/2025) Lei 58/2023	• A OUG 155/2024 aplica-se diretamente ao ensino superior. No caso das escolas do ensino pré-universitário, a aplicabilidade não é totalmente clara, mas espera-se que as escolas que interagem com redes governamentais (por exemplo, o SIIIR) sigam os protocolos da NIS2. • Espera-se que as escolas comuniquem incidentes significativos à DNSC no prazo de 24 horas através da plataforma PNRISC. • As medidas exigidas incluem: segmentação de rede (Wi-Fi separado para a administração e para os alunos), autenticação multifator para o acesso a plataformas oficiais, políticas de análise de risco e formação obrigatória de higiene cibernética para todo o pessoal. • Segurança da cadeia de fornecimento: os fornecedores privados de plataformas de e-learning ou de software de contabilidade utilizados pelas escolas devem estar em conformidade com a NIS2.

Área	O Que Significa para as Escolas
	• A Lei 58/2023 estabelece que a responsabilidade pela cibersegurança recai sobre a entidade que detém ou gere a rede, tornando a direção da escola diretamente responsável.
Proteção de Dados Lei 190/2018	• As escolas são classificadas como responsáveis pelo tratamento independentes e devem assegurar o cumprimento integral do RGPD. • É permitido um regime de EPD partilhado a nível do inspetorado distrital ou central. • As escolas devem implementar procedimentos obrigatórios de consentimento parental para plataformas de aprendizagem em linha e para a utilização de imagens de alunos. • A videovigilância só é permitida para proteção de pessoas e bens, com notificação obrigatória de alunos, professores e visitantes. As gravações não devem ser conservadas por mais de 30 dias, exceto no caso de incidentes objeto de investigação. • Os resultados dos exames devem ser publicados com recurso a anonimização ou pseudonimização, em conformidade com as orientações da ANSPDCP.
Idade de Consentimento Digital	• 16 anos. Este é o limiar mais elevado entre os cinco países. • É exigido o consentimento dos pais ou do encarregado de educação antes de inscrever alunos com menos de 16 anos em qualquer plataforma digital. • Na prática, isto aplica-se a praticamente todas as ferramentas educativas digitais utilizadas nas escolas romenas.
Ciberbullying ROFUIP 2025/2026 Estatuto do Aluno (Despacho 5707/2024)	• O ROFUIP define e pune o ciberbullying como um comportamento proibido no ambiente escolar. • É proibida a gravação de vídeo ou áudio não autorizada das atividades letivas. • O pessoal deve utilizar apenas ferramentas digitais oficialmente aprovadas e tratar os dados dos alunos com estrita confidencialidade. • O Estatuto do Aluno proíbe explicitamente qualquer forma de agressão no ambiente virtual. • Não existe uma plataforma nacional de denúncia dedicada. Os incidentes são tratados pela escola e encaminhados para a ANSPDCP quando estão em causa dados pessoais.
Telemóveis Lei 198/2023 ROFUIP	• A utilização de telemóveis durante as aulas é proibida para alunos do pré-escolar, do ensino básico e do 3.º ciclo, exceto quando autorizada pelo professor para fins educativos. • Os telemóveis devem estar desligados ou em modo silencioso durante as aulas e guardados num local designado, nos termos do ROFUIP. • As regras de utilização do telemóvel durante os intervalos são definidas pelo regulamento interno de cada escola.

Área	O Que Significa para as Escolas
IA na Educação	• Não foram emitidas orientações nacionais específicas. O Regulamento da UE sobre IA aplica-se diretamente. • O Ministério da Educação não emitiu orientações sobre ferramentas de IA generativa, como o ChatGPT, o que cria uma lacuna significativa. • As escolas devem aplicar os requisitos do Regulamento da IA em matéria de transparência, supervisão humana e proteção de dados sempre que utilizem qualquer ferramenta de IA com os alunos.
Infraestrutura Digital	• Não existe uma rede escolar nacional unificada. As escolas dependem de fornecedores comerciais de internet, o que resulta em normas de cibersegurança não uniformes. • O SIIIR (gerido centralmente pelo Ministério) é a principal base de dados nacional de dados de alunos. • As escolas utilizam plataformas comerciais (Google Workspace, Microsoft 365) ao abrigo de contratos individuais.
Contactos Principais	• Cibersegurança: DNSC (dnsc.ro) • Proteção de Dados: ANSPDCP (dataprotection.ro)

2.5 Eslováquia

A Eslováquia tem demonstrado um forte impulso legislativo na governação digital escolar. A Lei da Cibersegurança 366/2024, as restrições aos telemóveis em vigor desde janeiro de 2025, orientações específicas sobre ciberbullying (Orientação 1/2025) e um plano nacional de IA na educação para 2025-2027 refletem uma abordagem abrangente e estruturada. A direção da escola detém responsabilidade legal direta pela cibersegurança nos termos da lei eslovaca. O programa de infraestrutura DigiEDU/DigiNET disponibiliza conetividade à internet segura e centralizada a todas as escolas eslovacas.

Área	O Que Significa para as Escolas
Transposição da NIS2 Lei 366/2024 Lei 69/2018	• A Lei 366/2024 associa diretamente as obrigações de cibersegurança à responsabilidade estatutária da direção da escola nos termos da Lei 596/2003 sobre as Escolas. A direção é pessoal e legalmente responsável pela proteção dos sistemas de informação escolares e dos dados pessoais. • As escolas devem implementar medidas de segurança básicas: palavras-passe fortes, software antivírus, atualizações regulares, cópias de segurança dos dados e controlos de acesso. • As escolas devem estar preparadas para responder a ataques de phishing, ransomware, fugas de dados e comprometimento de sistemas. • Devem ser seguidos procedimentos de comunicação obrigatórios para incidentes de cibersegurança graves.

Área	O Que Significa para as Escolas
	• A Lei 69/2018 estabelece o quadro fundador para a proteção dos sistemas de informação e redes, assegurando a segurança dos dados dos alunos e a utilização segura das tecnologias digitais nas escolas.
Proteção de Dados Lei 18/2018	• É obrigatória a existência de um EPD nas escolas públicas, não sendo necessário um por escola: é permitido um EPD partilhado entre várias escolas. • As escolas devem aplicar a minimização dos dados: recolher e utilizar apenas os dados pessoais dos alunos estritamente necessários para o ensino e a administração. • O acesso aos dados deve limitar-se às pessoas autorizadas (professores, direção, administração), conforme necessário. • Os sistemas eletrónicos, os correios eletrónicos, os documentos em papel e os dispositivos de armazenamento devem estar protegidos contra a perda ou o acesso não autorizado. • As fotografias, listas de alunos, resultados ou informações sensíveis não devem ser publicados sem uma base jurídica ou consentimento explícito. • Qualquer violação da proteção de dados deve ser comunicada à autoridade competente no prazo de 72 horas, caso represente um risco para os titulares dos dados.
Idade de Consentimento Digital	• 16 anos. • É exigido o consentimento dos pais ou do encarregado de educação antes de inscrever alunos com menos de 16 anos em plataformas digitais.
Ciberbullying Orientação 1/2025	• A Orientação 1/2025 estabelece regras específicas sobre a prevenção e resolução do ciberbullying nas escolas e estabelecimentos de ensino. • Define os sinais, formas e manifestações básicas do ciberbullying. • Estabelece procedimentos de prevenção e métodos para lidar com incidentes. • Inclui procedimentos de apoio às vítimas. • As escolas devem implementar os procedimentos estabelecidos nesta orientação.
Telemóveis Lei 245/2008 (alterada a partir de janeiro de 2025)	• Os alunos do 1.º ao 3.º ano não podem utilizar telemóveis ou dispositivos semelhantes durante o período escolar. • Os alunos do 4.º ao 9.º ano só os podem utilizar para fins educativos quando o professor o permita especificamente. • Aplica-se uma exceção aos alunos com deficiência que utilizem o dispositivo em relação com a sua condição de saúde. • Em caso de infração, a escola pode confiscar temporariamente o dispositivo.

Área	O Que Significa para as Escolas
	• As condições detalhadas são regidas pelo regulamento interno da escola.
IA na Educação Plano de IA 2025-2027	• O Plano do Ministério da Educação para a Utilização Responsável da IA na Educação 2025-2027 fornece orientações nacionais práticas para as escolas. • As escolas devem utilizar este plano em conjunto com o Regulamento da UE sobre IA para avaliar e reger quaisquer ferramentas de IA que introduzam. • É dada ênfase à segurança, à utilização ética e à transparência.
Infraestrutura Digital	• DigiEDU/DigiNET: programa de conetividade à internet seguro e gerido centralmente para todas as escolas eslovacas. • A cibersegurança é supervisionada pelo Gabinete Nacional de Segurança (NBU), que opera o SK-CERT para a resposta a incidentes. • O NBU fornece orientação e apoio às instituições públicas, incluindo as escolas.
Contactos Principais	• Cibersegurança: NBU/SK-CERT (nbu.gov.sk) • Proteção de Dados: UOOU (dataprotection.gov.sk)

Normas Internacionais e Escolas

As recomendações práticas da Parte 3 desta política assentam num conjunto de normas de gestão reconhecidas internacionalmente. Esta breve secção explica o que são essas normas e porque são importantes para as escolas. Não é necessário conhecer as próprias normas para seguir as orientações da Parte 3. O que as normas proporcionam é uma base testada e amplamente aceite, que confere a esta política a sua estrutura e credibilidade.

São cinco as normas relevantes neste contexto. Cada uma delas aborda uma dimensão diferente da forma como as escolas podem proteger os seus alunos, os seus dados e os seus sistemas.

A norma ISO/IEC 27001 é a norma internacional para a gestão da segurança da informação. Fornece um quadro para identificar que informação uma escola detém, compreender os riscos que essa informação enfrenta e implementar as medidas adequadas para a proteger. Num contexto escolar, isto abrange os registos dos alunos, os dados do pessoal, as plataformas digitais e todos os sistemas que apoiam o ensino e a administração. A ISO 27001 não prescreve soluções técnicas específicas. Em vez disso, estabelece uma forma sistemática de pensar sobre a segurança, garantindo que nada de importante é esquecido. As ações práticas das Secções 3.1 a 3.7 assentam todas neste quadro.

A norma ISO/IEC 27002 complementa a ISO 27001 e fornece os controlos detalhados que colocam a segurança da informação em prática. Enquanto a ISO 27001 descreve o quadro de gestão, a ISO 27002 descreve as medidas específicas: como controlar o acesso aos sistemas, como gerir palavras-passe, como lidar com incidentes, como configurar dispositivos de forma segura. As Secções 3.2 e 3.3 baseiam-se mais diretamente nesta norma.

A norma ISO/IEC 27701 alarga o quadro de segurança da informação para abranger especificamente a proteção de dados pessoais. Está diretamente ligada ao RGPD e ajuda as escolas a demonstrar que gerem os dados de alunos e pessoal de forma responsável. A Secção 3.1 assenta nesta norma.

A norma ISO 22301 é a norma para a gestão da continuidade de negócio. Para as escolas, isto significa estar preparado para perturbações: um ciberataque, uma falha de sistema, um incidente de ransomware que bloqueia o acesso aos registos dos alunos. A ISO 22301 incentiva as organizações a planear antecipadamente estas situações, a dispor de procedimentos de cópia de segurança e recuperação e a testá-los regularmente para que funcionem quando necessário. Uma escola que siga esta abordagem consegue recuperar rapidamente de um incidente, em vez de enfrentar semanas de perturbação. A Secção 3.2 e o procedimento de resposta a incidentes do Anexo IV refletem esta norma.

A norma ISO 31000 é a norma para a gestão do risco. Proporciona uma forma de pensar sobre o risco que se aplica a todas as áreas da vida escolar, não apenas à cibersegurança. Antes de adotar uma nova plataforma digital, antes de introduzir uma ferramenta de IA, antes de alterar a forma como os dados dos alunos são tratados, uma escola deve perguntar-se: o que pode correr mal, qual a probabilidade de acontecer e quais seriam as consequências? É este o raciocínio subjacente ao processo de AIPD do Anexo V, à abordagem de avaliação de plataformas da Secção 3.3 e à abordagem mais ampla de consciência do risco ao longo de toda a Parte 3.

Em conjunto, estas cinco normas constituem a espinha dorsal da Parte 3. São a razão pela qual as recomendações desta política não são arbitrárias. Representam décadas de conhecimento acumulado sobre a forma como as organizações podem proteger a sua informação, gerir os seus riscos e continuar a funcionar quando algo corre mal. As orientações que se seguem traduzem esse conhecimento em passos práticos que qualquer escola pode adotar.

Parte 3: O Que a Sua Escola Deve Fazer

Esta parte está organizada em sete áreas. Cada área começa com uma breve explicação da sua importância, seguida de uma tabela que mostra o que a sua escola precisa de fazer, por que razão cada ação é importante e como a executar.

As recomendações desta secção são mais eficazes quando envolvem toda a comunidade escolar. A direção da escola, os professores, o pessoal administrativo, os alunos, os pais e as organizações de apoio externas têm todos um papel a desempenhar na criação de um ambiente digital seguro. A comunicação regular, a educação prática e canais de denúncia de confiança ajudam as escolas a construir uma cultura de resiliência cibernética, em vez de se limitarem a responder a incidentes.

3.1 Proteger os Dados Pessoais

As escolas detêm uma grande quantidade de informação pessoal sobre alunos, pais e pessoal. Isto inclui nomes, números de identificação, registos de assiduidade, notas, informações de saúde e contactos familiares. Proteger estes dados é uma obrigação legal. É também uma questão de confiança. As famílias partilham informação sensível com as escolas porque são obrigadas a fazê-lo. As escolas têm a responsabilidade de a tratar com cuidado.

Quando a proteção de dados falha, as consequências podem ser graves. A informação dos alunos pode ficar exposta a pessoas que não deveriam ter acesso a ela. A escola pode enfrentar uma investigação formal. E a confiança dos alunos e das famílias pode ser difícil de reconstruir. Fazer bem o essencial desde o início é muito mais fácil do que lidar com as consequências de uma violação.

O quê	Porque é Importante	Como Fazê-lo
Nomear um Encarregado de Proteção de Dados (EPD)	O EPD é a pessoa responsável por assegurar que a sua escola cumpre a legislação de proteção de dados. Sem esta figura, não há uma responsabilização clara quando algo corre mal. O EPD é também o principal ponto de contacto para alunos, pais e a autoridade de supervisão nacional.	Consulte a Parte 2 para saber se a sua escola precisa do seu próprio EPD ou se a função é assegurada a nível de agrupamento ou de autoridade. O EPD deve ser acessível ao pessoal, aos alunos e aos pais. É responsável por monitorizar a conformidade, aconselhar sobre questões de proteção de dados, formar o pessoal e assegurar a ligação com a autoridade de supervisão.
Manter um registo de todas as atividades de tratamento de dados	Este registo é exigido por lei nos termos do artigo 30.º do RGPD. Mostra que dados pessoais a sua escola detém, por que razão os detém, quem lhes pode aceder e durante quanto tempo são conservados. Se a autoridade de supervisão o solicitar, tem de estar em condições de o apresentar.	O registo deve abranger todas as categorias de dados pessoais tratados pela sua escola: registos de alunos, contactos dos pais, dados do pessoal, informações de saúde, entre outros. Para cada categoria, registe a finalidade, a base jurídica, quem tem acesso, durante quanto tempo é conservada e o que acontece quando deixa de ser necessária. O EPD é responsável por o manter atualizado.
Recolher apenas os dados de que realmente necessita	Cada dado que recolhe constitui um risco. Em caso de violação, só pode ser exposto o que efetivamente detém. Recolher mais do que o necessário implica também mais trabalho de gestão e maior potencial de incumprimento.	Reveja todos os formulários de recolha de dados, processos de inscrição e definições das plataformas. Remova quaisquer campos que solicitem informação de que a escola não necessite genuinamente. Se uma plataforma solicitar mais dados do que o necessário, contacte o fornecedor ou escolha uma plataforma diferente. Estabeleça como regra que a recolha opcional de dados esteja desativada por defeito.
Assinar acordos com todos os fornecedores que tratam dados de alunos	Quando uma empresa trata dados de alunos ou de pessoal em nome da sua escola, por exemplo uma plataforma na nuvem, uma ferramenta de avaliação ou uma aplicação de comunicação, a sua escola continua legalmente	Antes de qualquer fornecedor colocar em funcionamento um serviço que envolva dados pessoais, deve assinar um Acordo de Tratamento de Dados. Este deve especificar que dados são tratados, para que finalidade, que medidas de segurança estão em vigor e o que acontece aos dados quando o contrato

O quê	Porque é Importante	Como Fazê-lo
	responsável pela forma como esses dados são tratados. Sem um acordo escrito, não é possível demonstrar que cumpriu as suas obrigações.	termina. Conserve cópias de todos os acordos em arquivo.
Limitar quem pode aceder aos dados pessoais	Quanto mais pessoas tiverem acesso aos dados, maior é o risco de utilização indevida, divulgação acidental ou roubo. Cada ponto de acesso desnecessário constitui uma vulnerabilidade.	Configure o acesso com base em funções, de modo a que cada membro do pessoal só possa ver os dados de que necessita para a sua função específica. Um professor deve ver os registos dos seus próprios alunos, e não os de toda a escola. O pessoal administrativo deve aceder a dados administrativos, e não a ficheiros de saúde ou psicológicos. Reveja quem tem acesso pelo menos uma vez por ano e remova o acesso imediatamente quando alguém muda de função ou sai da escola.
Informar alunos e pais sobre a forma como os seus dados são utilizados	Os alunos e os pais têm o direito legal de saber que dados são detidos sobre eles e como são utilizados. Fornecer esta informação não é opcional. As escolas transparentes quanto à utilização dos dados tendem também a ter menos litígios e reclamações.	Redija um aviso de privacidade em linguagem simples, que qualquer pai ou aluno mais velho consiga compreender. Deve explicar que dados são recolhidos, porquê, quem lhes pode aceder e durante quanto tempo são conservados. Disponibilize-o no momento da inscrição e sempre que ocorra uma alteração significativa. Torne-o permanentemente disponível, por exemplo no sítio web da escola. Um modelo de carta encontra-se no Anexo II.
Obter o consentimento parental para alunos abaixo da idade de consentimento digital	No caso de alunos abaixo da idade nacional de consentimento digital, não é possível inscrevê-los numa plataforma digital sem o consentimento escrito de um pai ou encarregado de educação. Trata-se de um requisito legal. A idade varia entre os 13 e os 16 anos consoante os cinco países, o que significa que a mesma plataforma pode exigir consentimento num país mas não noutro.	Estabeleça um processo claro para recolher, registar e renovar o consentimento parental. O consentimento deve ser específico para cada plataforma, livremente dado e fácil de retirar. Não presuma que a assinatura de um formulário de inscrição geral cobre todas as plataformas digitais. Consulte a idade de consentimento digital para o seu país na Parte 2.
Comunicar violações de dados no prazo de 72 horas	O prazo de 72 horas é um requisito legal rigoroso. Se a sua escola descobrir uma violação e não a comunicar a	Estabeleça um procedimento escrito de resposta a violações antes de qualquer ocorrência. Quando ocorre uma violação, o EPD deve avaliar de imediato se esta cria um

O quê	Porque é Importante	Como Fazê-lo
	tempo, ou tentar geri-la discretamente sem informar a autoridade de supervisão, as consequências podem ser significativamente piores do que se a violação tivesse sido comunicada prontamente.	risco para os titulares dos dados. Em caso afirmativo, a autoridade de supervisão nacional deve ser notificada no prazo de 72 horas. Se o risco for elevado, as pessoas afetadas devem também ser notificadas diretamente. Utilize o registo de incidentes do Anexo IV para documentar cada passo.

O que é uma violação de dados?

Uma violação de dados é qualquer incidente que resulte na perda, destruição, alteração, divulgação ou acesso acidental ou ilícito a dados pessoais por alguém que não deveria ter acesso a eles. Isto inclui uma pen USB com registos de alunos que se perde, um e-mail enviado à pessoa errada, um ataque de ransomware que bloqueia os dados da escola ou uma definição de plataforma que torna acidentalmente públicos os registos dos alunos. Muitas das violações mais comuns nas escolas são causadas por erro humano, e não por ataques externos.

3.2 Manter os Sistemas Escolares Seguros

Cibersegurança significa proteger os computadores, as redes e os dados da sua escola contra ataques e acessos não autorizados. As escolas são um alvo atrativo para os cibercriminosos, pois detêm dados sensíveis sobre crianças e dispõem frequentemente de recursos de segurança limitados. Um ataque bem-sucedido pode paralisar os sistemas escolares, expor os registos dos alunos, perturbar o ensino durante semanas e causar danos duradouros à reputação da escola.

A boa notícia é que a maioria dos ciberataques bem-sucedidos explora fragilidades simples, que podem ser corrigidas sem conhecimentos especializados nem orçamentos elevados. Palavras-passe fracas, software não atualizado, pessoal que não reconhece e-mails de phishing e a ausência de cópias de segurança estão na origem da maioria dos incidentes. Corrigir estes aspetos básicos faz uma enorme diferença.

Igualmente importante é estar preparado para o momento em que algo corre mal. Ter uma cópia de segurança testada e um procedimento de recuperação claro faz a diferença entre uma interrupção que dura algumas horas e uma que dura semanas. É este o raciocínio subjacente ao planeamento da continuidade de negócio: não apenas prevenir incidentes, mas assegurar que a escola pode continuar a funcionar e recuperar rapidamente quando estes ocorrem.

O quê	Porque é Importante	Como Fazê-lo
Utilizar palavras-passe fortes e autenticação multifator	As palavras-passe fracas são a forma mais comum de os atacantes acederem aos sistemas escolares. Uma palavra-passe fácil de adivinhar, ou utilizada em	Todas as contas do pessoal devem utilizar palavras-passe fortes com pelo menos 12 carateres, combinando letras, números e símbolos. As palavras-passe devem ser alteradas sempre que haja razões para crer que foram comprometidas. A autenticação multifator deve

O quê	Porque é Importante	Como Fazê-lo
	múltiplas contas, significa que uma única palavra-passe roubada pode dar a um atacante acesso a tudo. A autenticação multifator acrescenta uma segunda verificação que protege as contas mesmo quando uma palavra-passe é roubada.	estar ativada em todos os sistemas que contenham dados de alunos. Depois de introduzir a palavra-passe, o membro do pessoal deve confirmar a sua identidade através de um segundo método, como um código enviado para o telemóvel.
Manter todo o software e dispositivos atualizados	As atualizações de software incluem frequentemente correções para fragilidades de segurança que os atacantes exploram ativamente. Muitos dos piores ataques de ransomware a escolas visaram sistemas a executar software desatualizado. Trata-se de uma das vulnerabilidades mais evitáveis que existem.	Estabeleça um calendário regular para aplicar atualizações a todos os dispositivos, sistemas operativos, aplicações e software de segurança da escola. Aplique as correções de segurança críticas assim que estejam disponíveis. Se um dispositivo já não puder receber atualizações, remova-o da rede ou substitua-o. Atribua a um membro específico do pessoal a responsabilidade de assegurar que as atualizações são feitas.
Efetuar regularmente cópias de segurança de todos os dados importantes	Os ataques de ransomware funcionam encriptando os dados e exigindo pagamento para restaurar o acesso. A única forma fiável de recuperar sem pagar é dispor de uma cópia de segurança feita antes do ataque. Sem uma cópia de segurança testada, uma escola pode perder semanas de trabalho e registos permanentes.	Configure cópias de segurança diárias automatizadas para todos os dados escolares críticos. Mantenha pelo menos uma cópia de cada cópia de segurança num local não ligado à rede principal da escola, para que não possa ser encriptada no mesmo ataque. Teste o processo de recuperação pelo menos uma vez por ano para confirmar que as cópias de segurança funcionam efetivamente e que os dados podem ser restaurados num prazo razoável.
Utilizar redes separadas para a administração e para os alunos	Se a rede utilizada pelo pessoal administrativo, onde são geridos os registos e as notas dos alunos, for a mesma utilizada pelos alunos e visitantes, um dispositivo de aluno comprometido ou um portátil de visitante infetado poderá potencialmente alcançar os sistemas administrativos da escola. Trata-se de um risco	Configure redes Wi-Fi separadas: uma para uso administrativo e outra para alunos e visitantes. Assegure-se de que a rede administrativa não é visível nem acessível a partir da rede dos alunos. Configure controlos de acesso para que apenas os dispositivos escolares autorizados possam ligar-se à rede administrativa.

O quê	Porque é Importante	Como Fazê-lo
	básico que a separação de redes elimina.	
Proteger todos os dispositivos escolares	Os dispositivos com palavras-passe de fábrica por defeito, que nunca foram atualizados ou não têm proteção antivírus instalada são alvos fáceis. Muitas escolas têm dispositivos em salas de aula ou gabinetes que foram configurados há anos e nunca mais foram revistos.	Instale software antivírus e antimalware em todos os dispositivos escolares e mantenha-o atualizado. Altere todas as palavras-passe por defeito de routers, câmaras, impressoras e qualquer outro equipamento ligado logo após a instalação. Realize uma auditoria regular a todos os dispositivos ligados. Antes de eliminar dispositivos antigos, assegure-se de que todos os dados foram apagados de forma permanente e segura.
Dispor de um plano escrito para lidar com incidentes	Sem um plano escrito, o pessoal que se depare com um ciberataque não saberá o que fazer. Decisões tomadas em pânico ou bem-intencionadas mas erradas, como desligar imediatamente um dispositivo ou tentar pagar um resgate, podem agravar muito uma situação já má.	Redija um procedimento de resposta a incidentes cibernéticos que defina quem coordena a resposta, que passos tomar e por que ordem, que autoridades nacionais contactar e dentro de que prazo, e como comunicar com alunos, pais e pessoal durante e após um incidente. Assegure-se de que todo o pessoal relevante conhece o procedimento antes de ocorrer um incidente. O Anexo IV disponibiliza um modelo.
Formar todo o pessoal pelo menos uma vez por ano	Os e-mails de phishing estão na origem da maioria dos ciberataques bem-sucedidos a escolas. Um membro do pessoal que não consiga reconhecer um e-mail de phishing é uma vulnerabilidade que nenhum sistema técnico consegue proteger totalmente. Um único clique numa ligação maliciosa pode dar a um atacante acesso total aos sistemas escolares.	Proporcione formação anual obrigatória de sensibilização para a cibersegurança a todo o pessoal. A formação deve abranger como identificar um e-mail de phishing, como criar e gerir palavras-passe fortes, o que fazer se um dispositivo se perder ou for roubado e a quem contactar se algo parecer estranho. Acrescente lembretes periódicos ao longo do ano. Sempre que possível, realize exercícios simulados de phishing: são uma das formas mais eficazes de mudar o comportamento do pessoal.

O que é um ataque de phishing?

Phishing é quando um atacante envia um e-mail, mensagem ou notificação que parece vir de uma fonte de confiança, como o Ministério da Educação, um fornecedor de software ou um colega. O objetivo é levar o destinatário a clicar numa ligação maliciosa, a introduzir os seus dados de acesso num sítio web falso ou a abrir um ficheiro infetado. O phishing é a forma mais comum de ciberataque contra as escolas. Qualquer mensagem inesperada que peça uma palavra-passe, que

peça a alguém para clicar urgentemente numa ligação ou que peça uma ação invulgar deve ser tratada com suspeita e verificada através de um canal separado antes de qualquer resposta.

3.3 Escolher e Utilizar Plataformas Digitais com Segurança

As escolas utilizam um número crescente de plataformas digitais para o ensino, a comunicação e a administração. Cada plataforma que trata dados de alunos é uma fonte potencial de risco. Uma plataforma com segurança fraca, que partilhe dados com anunciantes ou armazene informação de alunos fora da UE sem salvaguardas adequadas pode causar danos reais. As escolas têm o dever legal de verificar as plataformas antes de as adotar e de as gerir cuidadosamente enquanto estiverem em uso.

O mesmo se aplica às ferramentas de inteligência artificial. A IA está cada vez mais presente na educação, mas nem todas as ferramentas são seguras para utilizar com os alunos. O Regulamento da UE sobre IA traça linhas claras, e as escolas precisam de saber onde se situam essas linhas antes de introduzir qualquer ferramenta de IA na sala de aula ou em processos que afetem os alunos.

O quê	Porque é Importante	Como Fazê-lo
Verificar cada plataforma antes de a utilizar	Uma plataforma adotada sem as devidas verificações pode tratar os dados dos alunos de formas que a escola não aprovou, armazenar dados fora da UE ou ter fragilidades de segurança. Uma vez partilhados os dados com o fornecedor errado, é muito difícil reverter a situação.	Antes de adotar qualquer nova plataforma, verifique se cumpre o RGPD, se não utiliza os dados dos alunos para publicidade nem os partilha com terceiros sem consentimento, e se armazena os dados dentro da UE. Se a plataforma envolver o tratamento em grande escala de dados de alunos, realize uma AIPD antes de entrar em funcionamento (ver Anexo V). Assine um acordo de tratamento de dados com o fornecedor antes de qualquer partilha de dados.
Manter uma lista de plataformas aprovadas	Sem um registo central, as escolas perdem o controlo sobre que plataformas estão em uso, quando foram verificadas pela última vez ou quem as aprovou. O pessoal pode começar a utilizar plataformas informalmente, sem qualquer avaliação. Os alunos podem utilizar contas pessoais em ferramentas não aprovadas para trabalhos escolares, retirando dados do controlo da escola.	Mantenha um registo escrito de todas as plataformas e ferramentas digitais aprovadas para utilização na sua escola. Registe o nome da plataforma, para que é utilizada, quando foi avaliada e quando está prevista a próxima revisão. Reveja o registo pelo menos uma vez por ano. O pessoal não deve introduzir novas plataformas para uso escolar sem primeiro seguir o processo de aprovação.

O quê	Porque é Importante	Como Fazê-lo
Configurar as plataformas de forma segura	As definições por defeito das plataformas destinam-se geralmente à facilidade de utilização, e não à segurança. Uma sala de aula virtual à qual qualquer pessoa possa aceder sem iniciar sessão, uma função de gravação ativada por defeito ou contas de alunos com permissões excessivas criam riscos fáceis de evitar.	Todas as plataformas devem ser configuradas de forma segura antes de os alunos ou o pessoal começarem a utilizá-las. As ferramentas de videoconferência devem exigir autenticação antes de qualquer pessoa poder entrar numa sala de aula virtual. A gravação deve estar desativada por defeito e só ser ativada com o consentimento explícito de todos os presentes. As contas dos alunos devem ter apenas as permissões de que necessitam para as suas atividades educativas. Verifique as definições pelo menos uma vez por ano.
Conhecer que utilizações de IA são proibidas	Algumas práticas de IA em contextos educativos são proibidas pela legislação da UE. Isto aplica-se independentemente da forma como a ferramenta foi comercializada ou do que o fornecedor afirma. A proibição é absoluta e aplica-se a todas as escolas nos cinco países.	Não utilize qualquer ferramenta de IA que envolva o reconhecimento de emoções dos alunos, a sua categorização biométrica ou a sua identificação em tempo real através de reconhecimento facial. Estas utilizações são proibidas nos termos do artigo 5.º do Regulamento da UE sobre IA. Se um fornecedor oferecer estas funcionalidades, a escola não as deve utilizar. Se a escola já estiver a utilizar uma ferramenta deste tipo, deve cessar essa utilização.
Manter as pessoas no controlo das decisões sobre os alunos	As ferramentas de IA podem produzir recomendações erradas, enviesadas ou injustas. Quando estas recomendações influenciam o que acontece a um aluno, como uma nota, um encaminhamento ou uma avaliação de necessidades de aprendizagem, as consequências podem ser graves. É precisamente por esta razão que a lei exige que uma pessoa esteja no controlo.	Um professor ou adulto responsável deve sempre rever e assumir a responsabilidade por qualquer resultado de uma ferramenta de IA que afete um aluno. As ferramentas de IA podem ajudar, mas não podem tomar decisões finais. Documente como é aplicada a supervisão humana para cada ferramenta de IA utilizada na tomada de decisões educativas.
Informar alunos e pais quando a IA está a ser utilizada	Os alunos e os pais têm o direito de saber quando as ferramentas de IA são utilizadas de forma a	Quando uma ferramenta de IA é utilizada de forma a afetar a aprendizagem ou a avaliação de um aluno, informe os alunos e os pais de forma clara e em linguagem

O quê	Porque é Importante	Como Fazê-lo
	afetar a educação de um aluno. Utilizar ferramentas de IA sem os informar constitui provavelmente uma violação tanto do Regulamento da IA como do RGPD.	simples: o que a ferramenta faz, que dados utiliza, como os seus resultados são utilizados e como funciona a supervisão humana. Forneça esta informação antes de a ferramenta ser utilizada e mantenha-a permanentemente acessível.
Manter um registo de todas as ferramentas de IA em uso	As escolas que não saibam que ferramentas de IA estão a utilizar, que dados essas ferramentas tratam ou que avaliação foi feita antes da adoção não conseguem cumprir as suas obrigações legais nos termos do Regulamento da IA ou do RGPD.	Mantenha um registo de ferramentas de IA como parte da sua lista de plataformas aprovadas. Para cada ferramenta de IA, registe o que faz, em que categoria de risco se enquadra nos termos do Regulamento da IA, que dados trata, que avaliação foi realizada antes da adoção e quem é responsável pela supervisão. Reveja este registo pelo menos uma vez por ano.

3.4 Gerir Telemóveis e Dispositivos Pessoais

Todos os cinco países parceiros introduziram restrições legais à utilização de telemóveis nas escolas. As regras específicas variam consoante o país (ver Parte 2), mas as razões são as mesmas em todo o lado: os telemóveis nas salas de aula distraem os alunos da aprendizagem, criam riscos para a privacidade e a proteção de dados, facilitam o ciberbullying e acrescentam às pressões digitais que afetam a saúde mental dos alunos.

Uma política de telemóveis é mais do que uma regra disciplinar. É uma medida de proteção de dados, uma medida de bem-estar e uma afirmação daquilo que a escola valoriza. Uma política claramente redigida, genuinamente compreendida por alunos, pais e pessoal, e aplicada de forma consistente, é muito mais eficaz do que uma que exista apenas no papel.

O quê	Porque é Importante	Como Fazê-lo
Dispor de uma política de telemóveis clara e escrita	Sem uma política escrita, as regras são aplicadas de forma diferente por diferentes professores. Os alunos e os pais não podem ser responsabilizados por regras que não lhes foram claramente comunicadas. Uma aplicação inconsistente gera conflitos e mina a	Redija uma política de telemóveis que abranja quando os telemóveis podem e não podem ser utilizados, onde devem ser guardados durante os períodos restritos, que exceções existem por motivos de saúde ou atividades educativas específicas, e o que acontece se as regras forem infringidas. Partilhe a política com alunos e pais no início de cada ano letivo através da Política de Utilização Aceitável (Anexo III). Inclua-a no regulamento interno da escola.

O quê	Porque é Importante	Como Fazê-lo
	confiança nas regras da escola.	
Restringir a utilização do telemóvel durante as aulas	A utilização irrestrita do telemóvel durante as aulas perturba a aprendizagem, cria oportunidades para o ciberbullying e a gravação não autorizada, e acrescenta às pressões digitais que afetam o bem-estar dos alunos. A investigação demonstra consistentemente que os alunos de escolas com restrições claras ao telemóvel obtêm melhores resultados académicos e relatam maior bem-estar.	Os alunos não devem utilizar telemóveis pessoais durante as aulas, salvo se um professor o tiver especificamente autorizado para uma atividade educativa concreta. Nos países onde existe uma proibição legal, esta deve ser aplicada. Seja claro sobre onde os telemóveis devem ser guardados durante os períodos restritos. As exceções por motivos de saúde devem ser documentadas.
Proibir a gravação não autorizada	As gravações não autorizadas de alunos, professores ou outro pessoal constituem uma grave violação da privacidade e podem configurar um crime nos termos da lei nacional. As gravações partilhadas em linha podem causar danos duradouros às pessoas envolvidas e à escola. A popularidade das plataformas de vídeos curtos torna este um risco crescente.	Deixe absolutamente claro a alunos e pessoal que é proibido gravar qualquer pessoa na escola sem o seu consentimento explícito, seja durante as aulas, nos corredores, em visitas de estudo ou em eventos. Indique claramente as consequências. Trate qualquer gravação não autorizada envolvendo alunos ou pessoal como uma questão disciplinar grave e, se necessário, encaminhe-a para as autoridades competentes.
Aplicar normas de segurança aos dispositivos pessoais utilizados para trabalho escolar	Quando um professor utiliza um dispositivo pessoal para aceder aos sistemas escolares, a proteção de dados da escola é tão forte quanto o elo mais fraco. Um dispositivo pessoal com uma palavra-passe fraca, software desatualizado ou	O pessoal que utilize dispositivos pessoais para trabalho escolar deve protegê-los com uma palavra-passe ou PIN forte, manter o software atualizado, utilizar uma ligação segura ao trabalhar remotamente e não armazenar dados de alunos localmente em dispositivos pessoais. Forneça ao pessoal orientações claras sobre o que se espera.

O quê	Porque é Importante	Como Fazê-lo
	dados de alunos armazenados localmente constitui uma vulnerabilidade real.	

3.5 Prevenir e Responder ao Ciberbullying

O ciberbullying é a intimidação que ocorre através de dispositivos e plataformas digitais. Inclui o envio de mensagens ameaçadoras ou humilhantes, a partilha de imagens privadas sem consentimento, a divulgação de informação falsa em linha e a exclusão deliberada de alguém de grupos em linha. O ciberbullying pode causar danos graves e duradouros à saúde mental, ao desempenho académico e às relações sociais dos alunos.

As escolas têm tanto uma obrigação legal como um dever de cuidado no que respeita a prevenir o ciberbullying e a responder quando este ocorre. O ciberbullying não termina à porta da escola. O que acontece em linha em casa à noite pode afetar a experiência de um aluno na escola na manhã seguinte, e vice-versa. As escolas devem tratar o ciberbullying com a mesma seriedade que o bullying físico, mesmo quando ocorre fora do horário escolar.

O quê	Porque é Importante	Como Fazê-lo
Incluir explicitamente o ciberbullying na política antibullying	Uma política antibullying geral que não mencione o ciberbullying deixa margem para dúvidas sobre se o comportamento em linha está abrangido. Os alunos vítimas de bullying em linha podem não o denunciar por pensarem que a escola dirá que não é um problema seu.	Atualize a sua política antibullying para incluir uma secção dedicada ao ciberbullying. Deve definir o que é o ciberbullying, deixar claro que é tratado com a mesma seriedade que o bullying físico e confirmar que a política se aplica ao comportamento em linha fora do horário escolar quando este afeta diretamente a comunidade escolar. Reveja a política pelo menos uma vez por ano.
Ensinar os alunos sobre o ciberbullying	Os alunos que compreendem o que é o ciberbullying, por que razão causa danos e o que fazer quando o presenciam têm maior probabilidade de o denunciar e de apoiar um colega que esteja a ser visado. Ensinar os alunos a serem espectadores ativos e solidários é uma das	Proporcione educação sobre ciberbullying adequada à idade como parte regular do currículo, e não como um evento pontual. Aborde o que é o ciberbullying nas diferentes plataformas, os danos que causa, como apoiar alguém que esteja a ser visado e como o denunciar. Envolva os alunos na definição do conteúdo: estes envolvem-se mais com mensagens que ajudaram a criar.

O quê	Porque é Importante	Como Fazê-lo
	abordagens mais eficazes que existem.	
Dar aos alunos uma forma clara e segura de denunciar	Muitos alunos vítimas de ciberbullying não o denunciam. Receiam não ser acreditados, que a denúncia agrave a situação ou que percam o acesso ao telemóvel. Sem um canal de denúncia de confiança e acessível, os incidentes permanecem ocultos e agravam-se.	Ofereça mais do que uma forma de denunciar o ciberbullying: um adulto de confiança, um formulário ou caixa anónima e, quando disponível, a plataforma nacional de denúncia (ver Parte 2). Promova ativamente estas opções ao longo de todo o ano letivo, e não apenas em setembro. Quando um aluno faz uma denúncia, responda rapidamente e deixe claro que a leva a sério.
Formar todo o pessoal para reconhecer e responder ao ciberbullying	Muitos professores sentem-se inseguros quanto à forma de responder ao ciberbullying, especialmente quando envolve plataformas com as quais não estão familiarizados. A incerteza leva a respostas inconsistentes, o que prejudica tanto a vítima como a capacidade da escola de gerir os incidentes de forma eficaz.	Proporcione a todo o pessoal formação que abranja como identificar sinais de que um aluno pode estar a sofrer ciberbullying, qual é o procedimento da escola e qual o seu papel nele, como preservar provas, incluindo capturas de ecrã, quando envolver o psicólogo escolar, os pais ou as autoridades externas, e como apoiar um aluno sem inadvertidamente agravar a situação.
Responder rapidamente e documentar tudo	Uma resposta lenta ou inconsistente transmite a mensagem de que a escola não leva o ciberbullying a sério. Permite também que os incidentes se agravem e que as provas se percam. As escolas que não mantêm registos adequados têm dificuldade em identificar padrões ou em demonstrar que agiram de forma adequada, caso seja apresentada uma reclamação formal.	Quando um incidente de ciberbullying é denunciado, a primeira prioridade é a segurança e o bem-estar do aluno visado. Registe de imediato os detalhes: a data e a hora, o que aconteceu, que plataformas estiveram envolvidas, quem esteve envolvido, as provas recolhidas e todas as ações tomadas. Aplique o procedimento disciplinar de forma consistente. Acompanhe o aluno visado nos dias e semanas seguintes ao incidente.

O quê	Porque é Importante	Como Fazê-lo
Envolver os pais como parceiros	Os pais que compreendem o ciberbullying, sabem como falar com os filhos sobre o tema e se sentem envolvidos na abordagem da escola são muito mais eficazes tanto na prevenção de incidentes como no apoio aos filhos quando estes ocorrem.	Informe os pais no início do ano sobre a abordagem da escola ao ciberbullying, o que fazer se o seu filho for afetado e como a escola comunicará com eles. Utilize o modelo do Anexo II. Quando ocorrem incidentes, envolva os pais de todos os alunos afetados, seguindo os procedimentos da escola.

As escolas não têm de enfrentar estes desafios sozinhas. O Dia da Internet Mais Segura (fevereiro) e o Mês Europeu da Cibersegurança (outubro) disponibilizam às escolas materiais de sensibilização já preparados e validados a nível da UE. O programa Better Internet for Kids (BIK+) da UE e a rede Insafe de Centros de Internet Mais Segura disponibilizam linhas de ajuda, ferramentas de denúncia e recursos educativos nos cinco países parceiros, que as escolas podem utilizar diretamente.

3.6 Apoiar o Bem-Estar Digital dos Alunos

Os alunos enfrentam em linha riscos que vão além do ciberbullying e das violações de dados. Muitos vivenciam ansiedade, baixa autoestima e pressão social relacionadas com a sua vida digital. O medo de ficar de fora, a pressão para apresentar uma versão idealizada de si próprios em linha, a comparação constante com os outros, o tempo excessivo de ecrã e a conceção das plataformas de redes sociais, que privilegiam o envolvimento em detrimento do bem-estar, contribuem todos para os desafios de saúde mental que afetam um número significativo de jovens.

Restringir o acesso, por si só, não resolve estes problemas. Os alunos a quem simplesmente se diz para utilizar menos a tecnologia, sem os ajudar a compreender porquê ou lhes dar ferramentas para gerir o seu próprio comportamento, tendem a regressar aos antigos hábitos assim que as restrições são levantadas. As escolas que registam mudanças positivas duradouras são as que combinam limites claros com uma educação honesta e baseada em evidências e uma cultura em que os alunos se sentem seguros para falar sobre o que vivenciam em linha.

O quê	Porque é Importante	Como Fazê-lo
Integrar o bem-estar digital no apoio socioeducativo	Os alunos com dificuldades na sua vida em linha estão a enfrentar dificuldades na sua saúde mental e experiência social em geral. Se o bem-estar digital for tratado como um tema separado de informática, os alunos que necessitam de apoio podem ficar sem	O bem-estar digital deve constituir uma parte identificada do programa mais amplo de bem-estar e apoio ao aluno. O pessoal que apoia os alunos noutros desafios deve estar igualmente preparado para os apoiar nos desafios digitais. Os circuitos de encaminhamento devem ser claros: qualquer professor que identifique um aluno com dificuldades deve saber exatamente quem envolver e o que acontece a seguir.

O quê	Porque é Importante	Como Fazê-lo
	resposta entre os diferentes serviços.	
Ensinar aos alunos hábitos digitais saudáveis	Os alunos que compreendem como as plataformas de redes sociais são concebidas para os manter a percorrer conteúdos, que conseguem distinguir uma imagem em linha cuidadosamente construída da realidade e que desenvolveram as suas próprias estratégias para gerir os seus hábitos digitais estão mais bem preparados para navegar com segurança no mundo em linha.	Inclua a educação para o bem-estar digital como parte regular do currículo. Ensine os alunos a compreender como funcionam os algoritmos de recomendação e por que razão mostram frequentemente conteúdos que despoletam emoções fortes. Discuta os efeitos do consumo passivo de redes sociais no humor e na autoestima. Ajude os alunos a desenvolver estratégias práticas para estabelecer limites na sua própria utilização da tecnologia.
Assegurar que os alunos sabem onde obter ajuda	Muitos alunos com dificuldades relacionadas com algo em linha não pedem ajuda porque não sabem que esta está disponível, por vergonha ou por receio de que lhes tirem o telemóvel. Se o apoio não for ativamente promovido, torna-se invisível para os alunos que mais dele necessitam.	Recorde regularmente aos alunos com quem podem falar se algo em linha os estiver a incomodar. Mencione-o em assembleias, nas aulas e nas interações do dia a dia, e não apenas num manual. A pessoa a quem um aluno recorre não precisa de ser especialista em tecnologia. Precisa apenas de ser alguém em quem o aluno confie, que o escute sem julgamento e o encaminhe para a ajuda adequada.
Não acrescentar à pressão digital através das práticas escolares	As escolas podem, sem se aperceberem, criar as mesmas pressões digitais que procuram reduzir. Grupos de conversa escolares obrigatórios, a expectativa de que os alunos respondam a mensagens fora do horário escolar e comparações públicas entre alunos em linha podem transmitir mensagens contraproducentes.	Reveja a forma como a escola comunica digitalmente e se alguma das suas próprias práticas contribui para a pressão digital. Evite grupos de conversa obrigatórios que diluam a fronteira entre o tempo escolar e o tempo pessoal. Não espere que alunos ou pais respondam a mensagens fora do horário normal. Evite publicar classificações ou comparações em linha.

O quê	Porque é Importante	Como Fazê-lo
Reconhecer quando um aluno está com dificuldades	Os alunos com dificuldades na sua vida digital podem não o expressar diretamente. Os sinais são frequentemente comportamentais e fáceis de passar despercebidos, a menos que o pessoal saiba o que procurar.	Forneça ao pessoal orientações sobre os sinais de que um aluno pode estar com dificuldades na sua vida digital: ansiedade invulgar por não poder consultar o telemóvel, alterações de humor após interações em linha, afastamento de atividades sociais após algo que aconteceu em linha, sofrimento relacionado com a sua aparência ou com a forma como é visto em linha, relutância em ir à escola após um incidente em linha, ou qualquer sinal de estar a ser pressionado ou visado em linha. Quando estes sinais surgem, o pessoal deve seguir o procedimento de encaminhamento para o apoio socioeducativo da escola.

3.7 Diversidade, Inclusão e Equidade Digital

Nem todos os alunos enfrentam os mesmos riscos digitais nem têm o mesmo acesso a apoio. O género, a orientação sexual, a deficiência, o rendimento familiar e as preocupações com a imagem corporal moldam todos a experiência em linha de um aluno e a sua capacidade de obter ajuda quando algo corre mal. Uma política que funcione bem para a maioria dos alunos, mas que ignore a experiência de outros, não está completa.

Construir uma abordagem inclusiva à segurança digital significa pensar ativamente sobre quais os alunos que correm maior risco e assegurar que as políticas, a educação e os sistemas de apoio da escola os alcançam.

O quê	Porque é Importante	Como Fazê-lo
Abordar explicitamente os danos em linha baseados no género e na identidade	As raparigas enfrentam taxas desproporcionadamente elevadas de assédio sexual em linha, abuso baseado em imagens e ciberbullying relacionado com a aparência. Os alunos LGBTQ+ têm uma probabilidade significativamente maior de sofrer assédio em linha e de, em consequência, apresentar dificuldades de saúde mental. A investigação mostra que a prevalência comunicada de ciberbullying entre alunos LGBTQ+ varia amplamente: de aproximadamente 10% a mais de 70%, consoante o contexto, e que os alunos LGB relatam ser vítimas	Atualize a política antibullying da escola para abranger explicitamente o assédio em linha baseado no género, o assédio sexual, a partilha de imagens íntimas sem consentimento e o assédio baseado na orientação sexual ou identidade de género. Assegure-se de que a formação do pessoal aborda estas formas específicas de dano e como responder-lhes. Crie um ambiente escolar em que todos os alunos se sintam igualmente seguros para denunciar o que lhes está a acontecer.

O quê	Porque é Importante	Como Fazê-lo
	de ciberbullying a uma taxa aproximadamente o dobro da dos seus pares heterossexuais. A investigação mostra que o ciberbullying medeia estatisticamente grande parte da ansiedade, depressão e solidão elevadas relatadas por alunos de minorias sexuais, o que significa que a prevenção inclusiva é um mecanismo central para proteger a saúde mental deste grupo. Uma política que não nomeie estas formas específicas de dano deixa os alunos mais vulneráveis sem proteção adequada.	
Tornar a educação para a segurança digital acessível a alunos com deficiência	Os alunos com deficiência, incluindo diferenças de aprendizagem, podem estar mais vulneráveis à manipulação e exploração em linha. Podem também ter mais dificuldade em aceder a uma educação para a segurança digital que não tenha sido concebida a pensar nas suas necessidades. Se os mecanismos de denúncia não lhes forem acessíveis, deixam efetivamente de existir para eles.	Assegure-se de que toda a educação para a segurança digital é ministrada de formas adequadas a alunos com diferentes necessidades de aprendizagem. Verifique se as plataformas digitais utilizadas na escola cumprem as normas de acessibilidade. Assegure-se de que os mecanismos de denúncia são acessíveis a alunos que comunicam de forma diferente. Trabalhe com o pessoal de educação especial para identificar alunos que possam necessitar de apoio adicional na compreensão e gestão dos riscos em linha.
Reconhecer e combater a exclusão digital	Os alunos de famílias com menores rendimentos podem ter acesso limitado ou pouco fiável à internet em casa, dispositivos mais antigos ou partilhados, e menos apoio de adultos na navegação do mundo em linha. Os alunos que utilizam dispositivos partilhados enfrentam riscos de privacidade acrescidos. Estes alunos podem também ter menor probabilidade de reconhecer ou denunciar problemas.	Não conceba atividades digitais ou práticas de comunicação que pressuponham um nível de conetividade doméstica que nem todos os alunos têm. Tenha presente que os alunos que utilizam dispositivos partilhados enfrentam riscos de privacidade específicos e forneça orientações adequadas. Assegure-se de que a educação para a segurança digital chega a todos os alunos. Identifique os alunos sem conetividade doméstica adequada e resolva esta situação através dos programas nacionais disponíveis.
Ajudar os alunos a desenvolver	As redes sociais expõem constantemente os alunos a	Inclua educação sobre a imagem corporal e a aparência em linha como parte do

O quê	Porque é Importante	Como Fazê-lo
consciência crítica sobre a imagem corporal em linha	imagens editadas e filtradas, que estabelecem padrões de aparência irrealistas. Isto está associado a uma menor autoestima e a ansiedade, particularmente nas adolescentes, e nalguns casos a perturbações alimentares.	currículo de bem-estar digital. Ensine os alunos a compreender como as imagens são editadas e filtradas antes de serem publicadas, e ajude-os a entender que o que veem em linha é uma representação e não a realidade. Discuta como os algoritmos das plataformas amplificam conteúdos centrados na aparência. Aborde este tema com sensibilidade. Alguns alunos podem já estar a passar por dificuldades. Assegure-se de que existem circuitos de encaminhamento para apoio especializado.
Aplicar uma perspetiva inclusiva a toda esta política	Uma política concebida sem considerar as experiências de diferentes grupos de alunos refletirá a experiência da maioria e deixará outros menos protegidos. Os alunos que enfrentam os maiores riscos em linha são frequentemente aqueles cujas experiências foram menos consideradas.	Reveja todas as secções desta política e pergunte: isto alcança os alunos que correm maior risco? Os nossos circuitos de denúncia são acessíveis a todos? A nossa formação do pessoal aborda as vulnerabilidades específicas dos diferentes grupos? Envolva os alunos, incluindo os de grupos sub-representados, na revisão e melhoria da abordagem da escola à segurança digital.

Parte 4: O Que a Evidência Demonstra

Esta parte resume o que a investigação nos diz sobre o que realmente funciona quando as escolas abordam a cibersegurança, o ciberbullying e o bem-estar digital. Utilize esta secção para tomar decisões informadas sobre os programas, abordagens e intervenções que a sua escola adota.

4.1 Sensibilização e Formação em Cibersegurança

A investigação sobre cibersegurança nas escolas identifica de forma consistente o comportamento humano como o fator de risco mais importante. A maioria dos ataques bem-sucedidos começa com um e-mail de phishing ou uma palavra-passe fraca. As defesas técnicas ajudam, mas não conseguem impedir um ataque quando o pessoal não está formado para reconhecer a ameaça. Isto significa que investir na formação do pessoal é, pelo menos, tão importante como investir em ferramentas técnicas.

Os estudos sobre formação do pessoal em cibersegurança mostram que a formação regular e prática funciona significativamente melhor do que uma única sessão de sensibilização. O pessoal que recebe formação anual e lembretes ocasionais tem, de forma mensurável, menor probabilidade de clicar em ligações de phishing ou de utilizar práticas inseguras nos sistemas escolares. A forma como a formação é ministrada também importa: sessões interativas com exemplos reais funcionam melhor do que a leitura passiva de informação ou visualização de um vídeo.

Os exercícios simulados de phishing, em que o pessoal recebe um e-mail de phishing falso cuidadosamente concebido para testar como responde, estão entre os métodos de formação mais eficazes disponíveis. As escolas e organizações que realizam estes exercícios regularmente registam melhorias claras no comportamento do pessoal ao longo do tempo. O exercício é mais eficaz quando é imediatamente seguido de feedback que explica quais eram os sinais e qual teria sido a resposta correta.

No caso dos alunos, a evidência mostra que a educação para a cibersegurança funciona melhor quando é integrada no currículo, em vez de ministrada como um evento isolado. Os alunos que aprendem sobre segurança em linha através de exemplos reais, atividades interativas e discussão com os pares absorvem melhor as lições e aplicam-nas de forma mais consistente na sua própria vida do que os alunos que recebem a mesma informação numa palestra.

4.2 Prevenção do Ciberbullying

A investigação sobre a prevenção do ciberbullying mostra de forma consistente que as abordagens envolvendo toda a escola funcionam melhor. Isto significa programas que reúnem alunos, professores, pais e direção escolar em torno de um objetivo comum de criar um ambiente mais seguro. As escolas que tratam o ciberbullying puramente como uma questão disciplinar, a resolver depois de os incidentes ocorrerem, obtêm consistentemente piores resultados do que as escolas que adotam uma abordagem de prevenção envolvendo toda a comunidade.

Os programas centrados apenas no comportamento de quem pratica bullying são menos eficazes do que os que também desenvolvem a empatia e as competências dos espectadores. Os alunos que compreendem os danos causados pelo ciberbullying e que foram ensinados a apoiar um colega visado têm maior probabilidade de denunciar incidentes e de intervir para ajudar. O facto de os espectadores intervirem ou permanecerem em silêncio é um dos preditores mais fortes de o bullying se agravar ou cessar.

Os sistemas de denúncia anónima levam consistentemente a que mais incidentes sejam denunciados. Os alunos vítimas de ciberbullying frequentemente não contam a ninguém por receio de não serem acreditados, de a situação se agravar ou de haver consequências sociais junto dos pares. As escolas que oferecem um canal de denúncia genuinamente confidencial e de confiança registam taxas mais elevadas de divulgação e uma intervenção mais precoce.

A formação de professores é essencial e frequentemente subestimada. A investigação mostra que muitos professores se sentem inseguros quanto à forma de responder ao ciberbullying, particularmente quando envolve aplicações ou funcionalidades com as quais não estão familiarizados. As escolas que investem em formação prática e estruturada de professores sobre como reconhecer e responder ao ciberbullying registam consistentemente melhores resultados para os alunos.

O envolvimento parental faz também uma diferença consistente. Os pais que compreendem o ciberbullying, que sabem como funcionam as plataformas utilizadas pelos filhos e que se sentem ligados à abordagem da escola são mais eficazes tanto no apoio aos filhos como no reforço das mensagens da escola em casa.

A investigação fornece provas claras da dimensão do problema. De acordo com o estudo Health Behaviour in School-aged Children da OMS (2024), cerca de um em cada seis adolescentes na Europa, aproximadamente 15%, relata ter sofrido ciberbullying, com taxas globalmente semelhantes entre rapazes e raparigas e uma tendência ascendente em comparação com 2018. Os dados da OCDE revelam uma

variação entre países que vai de cerca de 7,5% a 27,1%. Os dados das linhas de ajuda da rede Insafe da UE colocam consistentemente o ciberbullying entre as razões mais comuns pelas quais crianças e adolescentes contactam os serviços de apoio, tendo sido novamente, no quarto trimestre de 2025, a questão mais frequentemente levantada.

Quando consultados pela Comissão Europeia em 2025, mais de 6000 crianças e adolescentes entre os 12 e os 17 anos em toda a UE expressaram expectativas claras em relação às escolas: a maioria pretendia regras e consequências explícitas para o ciberbullying, ensino direto sobre o tema e apoio psicológico para os afetados. As raparigas mostraram consistentemente maior probabilidade do que os rapazes de solicitar estas medidas.

Uma meta-análise de Polanin et al. (2021), abrangendo mais de 45 000 alunos, concluiu que os programas dedicados à prevenção do ciberbullying produziram uma redução estatisticamente significativa tanto na perpetração como na vitimização, e que os programas concebidos especificamente para o ciberbullying superaram as abordagens gerais antibullying.

4.3 Bem-Estar Digital

A investigação sobre a utilização da tecnologia e a saúde mental dos alunos não sustenta conclusões simples. Nem toda a utilização da tecnologia é prejudicial. Utilizar a tecnologia de forma ativa para trabalho criativo, comunicação ou aprendizagem pode ter efeitos positivos. O problema consistente é a utilização passiva: percorrer as redes sociais sem propósito ou interação significativa. Este tipo de utilização está mais fortemente associado à ansiedade, à solidão e a uma menor autoestima, sendo os efeitos particularmente marcados nas adolescentes.

A evidência apoia fortemente a educação em detrimento da restrição. As escolas que se centram exclusivamente em limitar o acesso à tecnologia, sem ajudar os alunos a compreender por que razão certos padrões de utilização são prejudiciais ou lhes dar ferramentas para gerir o seu próprio comportamento, registam mudanças menos duradouras. Os alunos que compreendem o problema e desenvolveram as suas próprias estratégias apresentam melhorias mais sustentadas no bem-estar.

Os programas que ensinam os alunos a pensar de forma crítica sobre os seus hábitos digitais, a compreender como as plataformas de redes sociais são concebidas para maximizar o envolvimento e a reconhecer a diferença entre imagens em linha cuidadosamente construídas e a realidade têm mostrado resultados positivos na redução da ansiedade e na melhoria da autoestima em múltiplos estudos. Estes programas funcionam melhor quando são ministrados ao longo do tempo como parte do currículo, em vez de como um evento único.

Envolver os alunos na criação das regras digitais da escola aumenta consistentemente tanto o grau de cumprimento como o sentido de pertença em relação a essas regras. Os alunos que sentem que as regras são justas e que tiveram uma palavra a dizer na sua definição têm maior probabilidade de as cumprir e de encorajar os pares a fazer o mesmo.

Um resultado particularmente importante diz respeito ao Medo de Ficar de Fora (FOMO). A investigação conceptualiza cada vez mais o FOMO não como um estado de espírito passageiro, mas como uma característica psicológica relativamente estável, uma ansiedade persistente relacionada com perder experiências gratificantes que outros estão a viver. Os estudos associam o FOMO a sintomas depressivos, perturbações do sono e comportamentos compulsivos de verificação. Uma revisão sistemática e meta-

análise de 2025 confirmou uma associação estatística consistente entre a dependência das redes sociais e níveis mais elevados de ansiedade, depressão, solidão e menor autoestima, sendo o FOMO frequentemente identificado como fator mediador. As escolas devem abordar explicitamente o FOMO e os padrões de utilização compulsiva em atividades dirigidas aos alunos, e não apenas através de mensagens genéricas sobre o tempo de ecrã.

A investigação assinala também que os resultados dependem fortemente não apenas da quantidade de utilização das plataformas digitais pelos alunos, mas da forma como as utilizam. As redes sociais podem funcionar como uma fonte de apoio para alguns alunos, particularmente os que estão isolados ou pertencem a grupos minoritários. As abordagens de prevenção devem ajudar os alunos a desenvolver uma relação mais consciente e intencional com a tecnologia.

A identificação e o encaminhamento precoces são importantes. Os alunos que são ligados ao apoio adequado antes de as suas dificuldades se agravarem apresentam resultados significativamente melhores do que aqueles que só são identificados quando os problemas já são visíveis, através da descida das notas ou de alterações comportamentais graves. As escolas que dispõem de circuitos claros e bem conhecidos para identificar e apoiar os alunos com dificuldades estão em muito melhor posição para os ajudar.

Anexo I: Tabela de Referência Nacional

Utilize esta tabela para encontrar os principais parâmetros nacionais do seu país. Sempre que esta política indicar para consultar as regras nacionais, é aqui que deve procurar.

Parâmetro	Grécia	Itália	Portugal	Roménia	Eslováquia
Idade de consentimento digital	15 anos	14 anos	13 anos	16 anos	16 anos
Autoridade de proteção de dados	HDPA dpa.gr	Garante garanteprivacy.it	CNPD cnpd.pt	ANSPDCP dataprotection.ro	UOOU dataprotection.gov.sk
Autoridade de cibersegurança	EAKE cyber.gov.gr	ACN acn.gov.it	CNCS cncs.gov.pt	DNSC dnsc.ro	NBU nbu.gov.sk
Comunicação de incidentes cibernéticos	EAKE	ACN	CERT.PT (24h para a NIS2)	DNSC/PNRISC (24h)	NBU/SK-CERT
Comunicação de violações de dados	HDPA, 72 horas	Garante, 72 horas	CNPD, 72 horas	ANSPDCP, 72 horas	UOOU, 72 horas
Recurso sobre ciberbullying	stop-bullying.gov.gr	Denunciar à escola ou à polícia	seguranet.pt	Escola ou ANSPDCP	Orientação 1/2025
Legislação sobre telemóveis	Proibição rigorosa 2018/2024	Todos os ciclos 2024/25	1.º ao 6.º ano a partir de set. 2025	Durante as aulas, Lei 198/2023	Todos os anos a partir de jan. 2025
Orientações de IA para escolas	Apenas o Regulamento da UE sobre IA	Decreto Ministerial 166/2025	Ainda não emitidas	Ainda não emitidas	Plano de IA 2025-2027

Anexo II: Modelo de Carta aos Pais

As escolas podem adaptar esta carta para informar os pais sobre a forma como a escola trata os dados dos alunos e o que faz para os manter seguros em linha. Envie-a no momento da inscrição e sempre que sejam feitas alterações significativas aos sistemas ou políticas digitais da escola.

[Nome e Morada da Escola]

[Data]

Exmo./a. Encarregado(a) de Educação,

Como Protegemos os Dados do Seu Educando e Apoiamos a Sua Segurança Digital

Escrevemos-lhe para o informar sobre a forma como a nossa escola trata os dados pessoais dos alunos e sobre o que fazemos para manter o seu educando seguro no seu ambiente de aprendizagem digital.

Que dados recolhemos e porquê. Recolhemos informação pessoal sobre o seu educando que é necessária para a educação e a administração. Isto inclui o nome, o número de identificação, os registos de assiduidade e as notas. Nalguns casos, podemos também deter informação relacionada com a saúde, sempre que relevante para a sua educação. Só recolhemos o que é necessário e conservamo-lo pelo período exigido por lei.

Quem lhes pode aceder. O acesso aos dados pessoais do seu educando está limitado ao pessoal autorizado que deles necessite para o exercício das suas funções. Não partilhamos dados com terceiros, salvo se a lei o exigir ou se tiver dado o seu consentimento explícito.

Plataformas digitais. A nossa escola utiliza plataformas digitais para o ensino e a administração. Antes de adotar qualquer plataforma, verificamos se cumpre o RGPD. O seu educando acederá a estas plataformas através de uma conta atribuída pela escola. Uma lista das plataformas atualmente utilizadas está disponível nos serviços administrativos da escola.

O seu consentimento. Para alunos com idade inferior a [inserir a idade nacional de consentimento digital], necessitamos do consentimento parental escrito antes de inscrever o seu educando numa plataforma digital. Ser-lhe-á pedido este consentimento no momento da inscrição e sempre que uma nova plataforma seja introduzida.

Ciberbullying. A nossa escola dispõe de procedimentos claros para prevenir e responder ao ciberbullying. Se o seu educando sofrer ou presenciar ciberbullying, incentive-o a falar com um adulto de confiança na escola ou contacte-nos diretamente através de [dados de contacto].

Os seus direitos. Tem o direito de consultar os dados que detemos sobre o seu educando, de solicitar correções e, nalgumas circunstâncias, de solicitar o seu apagamento. Para o fazer, contacte o nosso Encarregado de Proteção de Dados através de [dados de contacto do EPD].

Apoiar o bem-estar digital em casa. Incentivamo-lo a falar regularmente com o seu educando sobre as suas experiências em linha, sem julgamento. Se o seu educando parecer angustiado ou invulgarmente

ansioso em relação ao telemóvel ou a interações em linha, contacte [psicólogo escolar / contacto designado]. Existem também linhas de ajuda nacionais para crianças e jovens no seu país.

Se tiver alguma questão, não hesite em contactar-nos.

Com os melhores cumprimentos,

[Nome do Diretor(a) e Escola]

Anexo III: Modelo de Política de Utilização Aceitável

Adapte este modelo para criar a Política de Utilização Aceitável da sua própria escola. Deve ser assinada por alunos, pais ou encarregados de educação, e pessoal no início de cada ano letivo. Ajuste-a de modo a refletir os sistemas, as regras nacionais e o contexto da sua escola.

Política de Utilização Aceitável

[Nome da Escola] | Ano Letivo [XXXX-XXXX]

1. Finalidade

Esta política estabelece as regras para a utilização de dispositivos digitais, da internet e de plataformas digitais na nossa escola. Aplica-se a todos os alunos, pessoal e visitantes que utilizem os sistemas escolares. Ao assinar esta política, confirma que leu e compreendeu estas regras e que concorda em cumpri-las.

2. Para que pode utilizar os recursos digitais da escola

- Realizar trabalhos escolares e atividades educativas
- Comunicar com professores e colegas para fins escolares
- Utilizar plataformas aprovadas pela escola
- Atividades educativas especificamente autorizadas por um professor

3. O que não deve fazer

- Aceder a, criar ou partilhar conteúdos ilegais, nocivos, ofensivos ou discriminatórios
- Intimidar, assediar, ameaçar ou humilhar outros alunos ou o pessoal por meios digitais
- Partilhar informação pessoal sobre outros alunos ou pessoal sem o seu consentimento
- Gravar vídeo ou áudio de alunos, professores ou pessoal sem o seu consentimento explícito
- Utilizar a conta de outra pessoa ou partilhar os seus dados de acesso
- Instalar software ou aplicações em dispositivos escolares sem autorização
- Utilizar contas pessoais em plataformas não aprovadas para atividades escolares

4. Telemóveis

[Descreva aqui as regras de telemóveis da sua escola, em conformidade com a legislação nacional do seu país, conforme descrito na Parte 2 desta política. Indique onde os telemóveis devem ser guardados, que exceções se aplicam e o que acontece se as regras forem infringidas.]

5. Redes sociais

Os alunos não devem publicar conteúdos sobre a escola, outros alunos ou o pessoal que sejam nocivos, enganosos ou que possam prejudicar a reputação de alguém. O comportamento em linha que configure ciberbullying, dentro ou fora do horário escolar, está abrangido por esta política e pelos procedimentos antibullying da escola.

6. Denúncia

Se encontrar conteúdos que o façam sentir-se, a si ou a outro aluno, inseguro, ou se presenciar uma violação desta política, denuncie-a a um adulto de confiança na escola ou a [contacto de denúncia].

7. Consequências

A violação desta política pode resultar na suspensão do acesso aos sistemas escolares, noutras medidas disciplinares ao abrigo do regulamento disciplinar da escola e, em casos graves, no encaminhamento para as autoridades policiais.

Nome completo do aluno	
Assinatura do aluno	
Nome do pai/mãe ou encarregado de educação	
Assinatura do pai/mãe ou encarregado de educação	
Data	

Anexo IV: Procedimento de Resposta a Incidentes Cibernéticos

Siga estes passos sempre que ocorra um incidente cibernético na sua escola. Um incidente cibernético é qualquer evento que comprometa a segurança, a disponibilidade ou a confidencialidade dos dados ou sistemas escolares. Isto inclui um ataque de ransomware, o acesso não autorizado aos sistemas escolares ou uma violação de dados pessoais.

Passo 1: Identificar e conter

Assim que alguém descobrir um incidente, deve informar de imediato o coordenador de informática ou a direção da escola. Não tente resolver o problema sozinho. Desligue o dispositivo afetado da rede, desligando o cabo ou o Wi-Fi. Não desligue o dispositivo, a menos que seja especificamente instruído a fazê-lo, pois isso pode destruir provas. Registe a hora e uma descrição do que observou.

Passo 2: Avaliar

O coordenador de informática e o EPD devem avaliar o incidente em conjunto. Determinem que sistemas, contas ou dados foram afetados. Verifiquem se os dados pessoais foram ou podem ter sido comprometidos. Verifiquem se o incidente ainda está em curso ou já foi contido.

Passo 3: Notificar

Se isto aconteceu...	Deve...
Os dados pessoais foram ou podem ter sido comprometidos	Notificar a autoridade nacional de proteção de dados no prazo de 72 horas. Ver a Parte 2 para a autoridade do seu país.
Ocorreu um incidente de cibersegurança significativo	Notificar a autoridade nacional de cibersegurança. Em Portugal, para as entidades abrangidas pela NIS2, tal deve ser feito no prazo de 24 horas. Ver a Parte 2 para a autoridade do seu país.
Está envolvida atividade criminosa	Contactar a polícia.
Alunos ou pessoal correm risco imediato ou foram diretamente prejudicados	Prestar apoio imediato e notificar os pais ou encarregados de educação, conforme adequado.

Passo 4: Recuperar

Restaure os sistemas a partir de cópias de segurança, quando disponíveis. Redefina de imediato todas as palavras-passe e credenciais de acesso afetadas. Aplique quaisquer atualizações de segurança relevantes antes de colocar os sistemas novamente em funcionamento. Verifique se os sistemas restaurados estão a funcionar corretamente antes de os disponibilizar novamente a alunos e pessoal.

Passo 4a: Apoiar os afetados

Preste apoio psicológico e prático imediato a qualquer aluno ou membro do pessoal diretamente afetado pelo incidente. Isto deve ocorrer em paralelo com a resposta técnica, e não depois desta. Contacte sem demora o psicólogo escolar ou a equipa de apoio socioeducativo. Siga o protocolo de bem-estar da escola.

Passo 5: Rever

Após a resolução do incidente, realize uma revisão completa. Registe o que aconteceu, como ocorreu, o que foi feito e qual foi o resultado. Identifique que alterações reduziriam o risco de repetição. Informe o pessoal relevante sobre as conclusões, especialmente se o incidente envolveu um e-mail de phishing ou erro humano. Atualize o procedimento de resposta a incidentes, se necessário.

Registo de incidentes

Data e hora do incidente	
Como e por quem foi descoberto?	
O que aconteceu?	
Que sistemas e dados foram afetados?	
Ações imediatas tomadas	
Os dados pessoais foram comprometidos?	
Autoridade de proteção de dados notificada? (Data)	
Autoridade de cibersegurança notificada? (Data)	
Polícia contactada? (Data)	
Ações de recuperação tomadas	
Data de restauro dos sistemas	
Revisão concluída? (Data)	
Alterações efetuadas em resultado da revisão	

Anexo V: Modelo de Avaliação de Impacto sobre a Proteção de Dados (AIPD)

É exigida uma AIPD antes de a sua escola introduzir um novo sistema ou plataforma digital que envolva o tratamento de grandes quantidades de dados de alunos, a monitorização sistemática de alunos, a tomada de decisões automatizadas que os afetem, ou categorias sensíveis de dados. Em caso de dúvida sobre a necessidade de uma AIPD, consulte o seu EPD.

Parte A: O que será tratado

Nome do sistema ou plataforma	
Fornecedor	
Que dados pessoais serão tratados?	
Quem são os titulares dos dados? (alunos, pessoal, pais)	
Qual é a finalidade do tratamento?	
Qual é a base jurídica do tratamento?	
Onde serão armazenados os dados? (país, dentro do EEE?)	
Quem terá acesso?	
Durante quanto tempo serão conservados os dados?	
Os dados serão partilhados com terceiros?	

Parte B: Avaliação de risco

Risco	Nível (Baixo / Médio / Elevado) e como será resolvido
Acesso não autorizado aos dados dos alunos	
Dados perdidos ou apagados acidentalmente	
Dados utilizados para fins diferentes dos originais	
Alunos monitorizados ou perfilados sem transparência	

Risco	Nível (Baixo / Médio / Elevado) e como será resolvido
Dados transferidos para fora do EEE sem salvaguardas	
Dados conservados por mais tempo do que o necessário	

Parte C: Decisão

Nível de risco global (Baixo / Médio / Elevado)	
O tratamento pode avançar? (Sim / Sim com medidas de mitigação / Não)	
O que precisa de ser feito antes de o tratamento poder começar?	
EPD consultado? (Sim / Não / Data)	
Avaliação realizada por	
Data da avaliação	
Data da próxima revisão	

Anexo VI: Registo de Riscos da Escola

O Registo de Riscos da Escola ajuda a sua escola a identificar, avaliar e gerir os principais riscos de cibersegurança e proteção de dados que enfrenta. Preencher este registo é um passo prático na implementação da abordagem de gestão de risco descrita na Parte 3 desta política.

Os exemplos na tabela abaixo são indicativos. São disponibilizados para ajudar a sua escola a começar e para ilustrar o tipo de riscos mais comuns num ambiente escolar. A sua escola deve acrescentar, remover ou adaptar entradas de modo a refletir as suas circunstâncias, sistemas e contexto específicos. O registo deve ser revisto pelo menos uma vez por ano e atualizado sempre que ocorra uma alteração significativa, como a introdução de uma nova plataforma digital ou um incidente de cibersegurança.

Como pontuar os riscos

Para cada risco, pontue a Probabilidade e o Impacto numa escala de 1 a 5 (1 = muito baixo, 5 = muito elevado). Multiplique as duas pontuações para obter a Pontuação de Risco.

Risco elevado (15-25): deve ser resolvido de imediato.

Risco médio-elevado (8-14): deve ser resolvido, priorizando os de impacto elevado.

Risco médio-baixo (4-7): deve ser resolvido quando o impacto for significativo.

Risco baixo (1-3): aceitável, monitorizar regularmente.

Uma tabela indicativa de Registo de Riscos encontra-se na página seguinte (formato paisagem).

ID	Risco	O Que Pode Acontecer	Como o Reduzimos	Probabilidade (1-5)	Impacto (1-5)	Pontuação de Risco	Responsável	Se Acontecer
1	E-mail de phishing dirigido ao pessoal	O pessoal clica numa ligação maliciosa, dando a um atacante acesso aos sistemas escolares e aos dados dos alunos	Formação anual do pessoal, exercícios simulados de phishing, autenticação multifator em todas as contas	4	4	16	Direção / Coordenador de Informática	Isolar o dispositivo afetado, notificar a autoridade nacional de cibersegurança, restaurar a partir de cópia de segurança
2	Ataque de ransomware	Os sistemas escolares ficam bloqueados, os registos e as notas dos alunos tornam-se inacessíveis	Cópias de segurança regulares e testadas armazenadas offline, software antivírus atualizado, formação do pessoal	3	5	15	Coordenador de Informática	Restaurar a partir de cópia de segurança, comunicar à autoridade nacional de cibersegurança, notificar a autoridade de proteção de dados se os dados dos alunos forem afetados
3	Dados de alunos enviados por engano à pessoa errada	Dados pessoais de um aluno são partilhados acidentalmente com uma pessoa não autorizada	Formação do pessoal sobre o tratamento de dados, utilização exclusiva de canais de comunicação oficiais da escola	4	3	12	EPD	Contactar o destinatário e solicitar o apagamento, comunicar à autoridade nacional de proteção de dados no prazo de 72

ID	Risco	O Que Pode Acontecer	Como o Reduzimos	Probabilidade (1-5)	Impacto (1-5)	Pontuação de Risco	Responsável	Se Acontecer
								horas se exigido, documentar o incidente
4	Ciberbullying através de plataforma escolar	Um aluno utiliza uma ferramenta de comunicação escolar para assediar outro aluno	Política de Utilização Aceitável assinada por todos os alunos e pais, educação sobre ciberbullying, circuito de denúncia claro	4	3	12	Direção / Diretor de Turma	Seguir o procedimento antibullying da escola, apoiar o aluno afetado, envolver os pais, documentar o incidente

Anexo VII: Registo de Mapeamento de Dados

O Registo de Mapeamento de Dados ajuda a sua escola a registar todos os dados pessoais que trata. Manter este registo é um requisito legal nos termos do artigo 30.º do RGPD. Deve estar disponível para a autoridade nacional de proteção de dados mediante pedido.

Os exemplos abaixo abrangem as categorias mais comuns de dados pessoais tratados pelas escolas. São indicativos: a sua escola deve acrescentar quaisquer categorias adicionais aplicáveis à sua situação e remover as que não se aplicam. Reveja e atualize o registo pelo menos uma vez por ano e sempre que seja introduzido um novo sistema ou plataforma.

O que é uma base jurídica?

Sempre que a sua escola trata dados pessoais, deve ter um motivo lícito. Os mais comuns para as escolas são:

Obrigação legal: tratamento exigido pela legislação nacional de educação (por exemplo, manter registos de assiduidade).

Missão de interesse público: tratamento necessário para a escola exercer as suas funções públicas.

Consentimento: a pessoa concordou com o tratamento (exigido para fotografias, plataformas não essenciais).

Uma tabela indicativa de Registo de Mapeamento de Dados encontra-se na página seguinte (formato paisagem).

Tipo de Dados	Porque os Tratamos	Base Jurídica	Onde é Armazenado	Quem Tem Acesso	Durante Quanto Tempo o Conservamos	Com Cópia de Segurança ?	Partilhado Com
Dados pessoais do aluno (nome, número de identificação, morada, data de nascimento)	Necessário para a administração escolar e o cumprimento da legislação nacional de educação	Obrigação legal	Sistema nacional de informação escolar (por exemplo, MySchool, SIIIR, Unica)	Apenas direção e pessoal administrativo	Conforme exigido pela legislação nacional	Sim	Ministério da Educação, através da plataforma nacional
Registos académicos do aluno (notas, assiduidade, avaliações)	Necessário para acompanhar o progresso do aluno e informar os pais	Obrigação legal / Missão de interesse público	Sistema de informação escolar e caderneta do professor	Diretores de turma, direção, pessoal administrativo	Conforme exigido pela legislação nacional	Sim	Pais (através de canal seguro), Ministério da Educação
Informação de saúde do aluno (alergias, deficiências, necessidades médicas)	Necessário para proteger a saúde e a segurança do aluno durante o período escolar	Obrigação legal / Interesses vitais	Ficheiro em papel seguro ou registo digital encriptado	Apenas direção, enfermeiro escolar e professores relevantes	Duração da matrícula, mais o período exigido por lei	Sim (encriptado)	Prestadores de cuidados de saúde, apenas quando necessário
Fotografias e imagens do aluno	Cartão de identificação escolar, publicações,	Consentim ento parental	Servidor da escola ou	Pessoal administrativo,	Duração da matrícula; apagadas	Sim	Sem partilha com terceiros sem

Tipo de Dados	Porque os Tratamos	Base Jurídica	Onde é Armazenado	Quem Tem Acesso	Durante Quanto Tempo o Conservamos	Com Cópia de Segurança ?	Partilhado Com
	documentação de eventos		plataforma aprovada	professores autorizados	mediante pedido		consentimento adicional

Anexo VIII: Registo de Políticas e Procedimentos Escolares

Este registo ajuda a sua escola a acompanhar as principais políticas de segurança e proteção de dados em vigor. Ter políticas documentadas em cada uma destas áreas é um sinal importante de que a escola gere de forma estruturada as suas responsabilidades em matéria de cibersegurança e proteção de dados.

As políticas listadas abaixo são as mais relevantes para as recomendações desta Política de Resiliência Cibernética. A lista é indicativa: a sua escola pode ter políticas adicionais que também devem ser aqui registadas. Para cada política, anote quem é o responsável, quando foi atualizada pela última vez e quando está prevista a próxima revisão. Quando uma política ainda não existir, registe-o como uma ação prioritária.

Modelos disponíveis

Os anexos desta política incluem modelos para várias das políticas abaixo listadas:

- Política de Utilização Aceitável: Anexo III.
- Procedimento de Resposta a Incidentes: Anexo IV.
- Avaliação de Impacto sobre a Proteção de Dados (AIPD): Anexo V.
- Registo de Riscos: Anexo VI.
- Registo de Mapeamento de Dados: Anexo VII.
- Autoavaliação da Resiliência Cibernética da Escola: Anexo IX

ID	Nome da Política	Principais Áreas Abrangidas	Responsável pela Política	Última Atualização	Próxima Revisão
1	Política de Utilização Aceitável (PUA)	Utilização dos sistemas e dispositivos escolares. Regras sobre telemóveis. Denúncia.	Direção / Coordenador de Informática		
2	Política de Controlo de Acesso	Quem pode aceder a que sistemas e dados. Regras de palavras-passe. Remoção do acesso quando um membro do pessoal sai.	Coordenador de Informática / EPD		
3	Política de Proteção de Dados	Conformidade com o RGPD. Responsabilidades do EPD. Consentimento	EPD / Direção		

ID	Nome da Política	Principais Áreas Abrangidas	Responsável pela Política	Última Atualização	Próxima Revisão
		parental. Avisos de privacidade. Resposta a violações de dados.			
4	Política de Cópias de Segurança	O que é copiado, com que frequência, onde é armazenado e como é testada a recuperação.	Coordenador de Informática		
5	Política de Resposta a Incidentes	Como a escola responde a incidentes de cibersegurança e violações de dados. Quem é responsável. Como notificar as autoridades.	Direção / EPD / Coordenador de Informática		
6	Política Antibullying (incluindo Ciberbullying)	Definição de ciberbullying. Circuito de denúncia. Como a escola responde. Formação do pessoal. Envolvimento dos pais.	Direção		
7	Política de Dispositivos Móveis	Regras de telemóveis dos alunos em conformidade com a legislação nacional. Proibição de gravação não autorizada.	Direção		

ID	Nome da Política	Principais Áreas Abrangidas	Responsável pela Política	Última Atualização	Próxima Revisão

Anexo IX: Autoavaliação da Resiliência Cibernética da Escola

As escolas podem utilizar esta lista de verificação para estabelecer uma compreensão de base da sua resiliência cibernética atual e identificar lacunas prioritárias. Assinale cada item como Sim, Parcialmente ou Não. O objetivo não é aprovar ou reprovar, mas sim identificar onde concentrar os esforços.

As escolas são encorajadas a repetir esta autoavaliação pelo menos uma vez por ano. Acompanhar as pontuações ao longo do tempo ajuda a monitorizar o progresso e apoia uma cultura de melhoria contínua.

Os itens listados são indicativos. Adapte-os de modo a refletir o contexto próprio da sua escola, os requisitos nacionais e as circunstâncias específicas.

Domínio	O que verificar	Sim / Parcialmente / Não
Governação	A escola tem um coordenador designado para a cibersegurança ou a segurança digital.	
Governação	A escola tem uma Política de Utilização Aceitável escrita, revista nos últimos 2 anos.	
Governação	A escola tem um procedimento de resposta a incidentes documentado e conhecido pelo pessoal.	
Sensibilização e Formação	O pessoal recebe formação pelo menos anual em cibersegurança e segurança em linha.	
Sensibilização e Formação	Os alunos recebem educação para a cidadania digital e a segurança em linha adequada à idade.	
Sensibilização e Formação	Os pais e encarregados de educação recebem informação sobre riscos digitais pelo menos uma vez por ano letivo.	
Bem-Estar e Prevenção	A escola tem um protocolo específico e identificado para responder ao ciberbullying.	
Bem-Estar e Prevenção	Os alunos sabem como e a quem denunciar confidencialmente incidentes em linha.	

Domínio	O que verificar	Sim / Parcialmente / Não
Bem-Estar e Prevenção	As atividades de prevenção abordam explicitamente grupos diversos e vulneráveis.	
Dados e Privacidade	A escola mantém um registo das plataformas e ferramentas que tratam dados de alunos.	
Dados e Privacidade	O consentimento parental é obtido antes de inscrever os alunos em plataformas digitais, quando legalmente exigido.	
Medidas Técnicas	Os dispositivos e redes escolares utilizam software de proteção atualizado e controlos de acesso.	
Medidas Técnicas	São efetuadas e testadas regularmente cópias de segurança dos dados escolares críticos.	

Como interpretar a sua pontuação

Conte as respostas Sim (1 ponto) e Parcialmente (0,5 pontos). Divida por 13 e multiplique por 100 para obter uma percentagem. Compare com os níveis de maturidade abaixo.

Nível	Pontuação	Descrição
1 - Inicial	0 a 20%	Pouca ou nenhuma governação formal, formação ou procedimentos de incidentes em vigor.
2 - Em Desenvolvimento	21 a 45%	Existem políticas básicas, mas não são aplicadas, revistas ou comunicadas de forma consistente.
3 - Estabelecido	46 a 70%	Os elementos essenciais de governação, formação e resposta a incidentes estão em vigor e são conhecidos pelo pessoal.
4 - Avançado	71 a 90%	Políticas e formação abrangentes e regularmente revistas chegam ao pessoal, aos alunos e aos pais.
5 - Resiliente	91 a 100%	A resiliência cibernética está incorporada na cultura escolar, com formação contínua e prevenção inclusiva.

Estes níveis constituem apenas uma ferramenta de autoavaliação e não constituem certificação formal nem avaliação de conformidade.

Referências

Legislação da União Europeia

Os seguintes instrumentos legais da União Europeia constituem o quadro jurídico comum subjacente a esta Política. Estabelecem os principais requisitos em matéria de proteção de dados, cibersegurança, inteligência artificial, serviços digitais, comunicações eletrónicas e educação digital em todos os Estados-Membros da UE.

- European Union, Regulation (EU) 2016/679 (General Data Protection Regulation – GDPR), Official Journal of the European Union. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679
- European Union, Directive (EU) 2022/2555 (NIS 2 Directive), Official Journal of the European Union. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022L2555
- European Union, Regulation (EU) 2024/1689 (Artificial Intelligence Act), Official Journal of the European Union. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L_202401689
- European Union, Regulation (EU) 2022/2065 (Digital Services Act), Official Journal of the European Union. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022R2065
- European Union, Directive 2002/58/EC (ePrivacy Directive), Official Journal of the European Communities. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32002L0058
- European Union, Regulation (EU) 2019/881 (Cybersecurity Act), Official Journal of the European Union. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019R0881

Instrumentos Legislativos Nacionais

Os seguintes instrumentos legislativos nacionais e fontes oficiais foram utilizados na preparação da Parte 2 desta política. São apresentados por país, em conformidade com a prática de referenciação normalizada para projetos financiados a nível europeu.

Grécia

- Hellenic Republic (2018). Law 4577/2018 on the Security of Network and Information Systems. Government Gazette A' 199/03.12.2018. Available at: https://www.mindigital.gr/wp-content/uploads/2019/09/N.4577_2018.pdf
- Hellenic Republic (2019). Law 4624/2019 on the Protection of Natural Persons with Regard to the Processing of Personal Data (GDPR Implementation). Government Gazette A' 137/29.08.2019. Available at: https://www.dpa.gr/sites/default/files/2020-08/LAW%204624_2019_EN_TRANSLATED%20BY%20THE%20HDPA.PDF
- Hellenic Republic (2020). Law 4727/2020 on Digital Governance and Electronic Communications. Government Gazette A' 184/23.09.2020. Available at: https://adae.gov.gr/images/nomothetiko-plaisio/Nomos_4727_2020_01.pdf
- Hellenic Republic (2022). Law 4961/2022 on Emerging Technologies and Digital Governance. Government Gazette A' 146/27.07.2022. Available at: https://www.mindigital.gr/wp-content/uploads/2024/02/N-4961.pdf

- Hellenic Republic (2023). Law 5029/2023 on the Prevention and Management of School Violence and Cyberbullying. Government Gazette A' 55/10.03.2023. Available at: https://www.iep.edu.gr/wp-content/uploads/2025/01/2024-08-02_N_5029-2023.pdf
- Hellenic Republic (2024). Law 5160/2024 on Cybersecurity (NIS2 Transposition). Government Gazette A' 195/27.11.2024. Available at: https://search.et.gr/el/fek/?fekId=774154
- Ministry of Digital Governance, Hellenic Republic (2025). Ministerial Decision 1689/2025 on Cybersecurity Requirements for Public Sector Entities. Government Gazette B' 2186/06.05.2025. Available at: https://cyber.gov.gr/wp-content/uploads/2025/05/20250202186.pdf
- Ministry of Digital Governance, Hellenic Republic (2025). Ministerial Decision 1899/2025 on Information Security Governance for Public Entities. Government Gazette B' 4250/05.08.2025. Available at: https://cyber.gov.gr/wp-content/uploads/2025/03/KYA_APOFASI_10-Feb-2025_FEK-463_DEFTERO-TEFHOS.pdf

Itália

- Italian Republic (2003). Legislative Decree No. 196/2003 — Personal Data Protection Code, as amended by Legislative Decree No. 101/2018. Available at: https://www.garanteprivacy.it/documents/10160/0/Codice+in+materia+di+protezione+dei+dati+personali.pdf
- Italian Republic (2021). Law No. 109/2021 converting Decree-Law No. 82/2021 — Establishment of the National Cybersecurity Agency (ACN). Gazzetta Ufficiale, 04.08.2021. Available at: https://www.gazzettaufficiale.it/atto/serie_generale/caricaDettaglioAtto/originario?atto.codiceRedazionale=21A04841
- Italian Republic (2024). Legislative Decree No. 138/2024 — NIS2 Transposition. Gazzetta Ufficiale, 01.10.2024. Available at: https://www.gazzettaufficiale.it/eli/id/2024/10/01/24G00155/SG
- Ministry of Education, Italian Republic (2020). Ministerial Decree No. 89/2020 — Guidelines for Digital Integrated Teaching (DDI). Available at: https://www.mim.gov.it/documents/20182/0/Decreto.pdf
- Ministry of Education, Italian Republic (2024). MIM Note No. 5274/2024 — Smartphone Use Restrictions in Schools. Available at: https://www.mim.gov.it/-/nota-n-5274-dell-11-luglio-2024
- Ministry of Education, Italian Republic (2025). MIM Circular No. 3392/2025 — Mobile Phone Restrictions in Schools. Available at: https://www.mim.gov.it/-/circolare-n-3392-del-16-giugno-2025
- Ministry of Education, Italian Republic (2025). Ministerial Decree No. 166/2025 — Guidelines for the Responsible Use of Artificial Intelligence in Schools. Available at: https://www.mim.gov.it/-/decreto-ministeriale-n-166-del-9-agosto-2025

Portugal

- Portuguese Republic (2018). Law No. 46/2018 — Legal Framework for Cyberspace Security (RFSC). Diário da República, 13.08.2018. Available at: https://diariodarepublica.pt/dr/detalhe/lei/46-2018-116029384
- Portuguese Republic (2019). Law No. 58/2019 — Portuguese Data Protection Law (GDPR Implementation). Diário da República, 08.08.2019. Available at: https://diariodarepublica.pt/dr/detalhe/lei/58-2019-123815982
- Council of Ministers, Portuguese Republic (2020). Resolution No. 30/2020 — Digital Transition Action Plan (PATD). Diário da República, 2020. Available at: https://diariodarepublica.pt/dr/detalhe/resolucao-conselho-ministros/30-2020-132133788
- Portuguese Republic (2025). Decree-Law No. 95/2025 — Prohibition of Smartphones in Schools (Years 1-6). Diário da República, 03.07.2025.

- Portuguese Republic (2025). Decree-Law No. 125/2025 — NIS2 Transposition (in force 3 April 2026). Diário da República, 04.12.2025. Available at: Decreto-Lei n.º 125/2025, de 4 de dezembro | DR
- Directorate-General of Education (DGE), Portugal. PADDE — School Digital Development Action Plan Framework. Available at: https://www.dge.mec.pt
- Centro Nacional de Cibersegurança (CNCS) / DGE, Portugal. SeguraNet — Digital Safety and Cybersecurity Resources for Schools. Available at: https://www.seguranet.pt
- Centro Nacional de Cibersegurança (CNCS), Portugal. CERT.PT — National Computer Emergency Response Team. Available at: https://www.cncs.gov.pt/pt/certpt/

Roménia

- Romanian Republic (2018). Law No. 190/2018 — Personal Data Protection (GDPR Implementation). Official Gazette of Romania No. 651/26.07.2018. Available at: https://portal.just.ro/101/Documents/LEGE__190_2018_date_cu_caracter_personal.pdf
- Romanian Republic (2023). Law No. 58/2023 on Cybersecurity Obligations for Network and Information System Operators. Official Gazette of Romania No. 214/15.03.2023. Available at: https://legislatie.just.ro/Public/DetaliiDocument/265677
- Romanian Republic (2023). Law No. 198/2023 — Pre-university Education Law. Official Gazette of Romania No. 613/05.07.2023. Available at: https://edu.ro/sites/default/files/_fisiere/Minister/2023/Legi_educatie_Romania_educata/legi_monitor/Legea_invatamantului_preuniversitar_nr_198.pdf
- Government of Romania (2024). Emergency Ordinance (OUG) No. 155/2024 — NIS2 Transposition (approved by Law No. 124/2025). Official Gazette of Romania No. 1332/31.12.2024. Available at: https://legislatie.just.ro/Public/DetaliiDocumentAfis/293121
- Ministry of Education, Romania (2024). Order No. 5707/2024 — Student Statute. Official Gazette of Romania No. 795/12.08.2024. Available at: https://www.edu.ro/sites/default/files/_fisiere/Legislatie/2024/OM_5707_2024_Statut_elev.pdf
- Ministry of Education, Romania (2025). OMEC 6055-6058 — ROFUIP 2025-2026: Framework Regulation for the Organisation and Functioning of Pre-university Educational Units. Official Gazette of Romania No. 819/04.09.2025. Available at: https://www.edu.ro/ROFUIP

Eslováquia

- Slovak Republic (2003). Act No. 596/2003 Coll. on State Administration in Education and School Self-Government (Schools and School Facilities Act), as amended. Available at: https://www.slov-lex.sk
- Slovak Republic (2008). Act No. 245/2008 Coll. on Education and Training (School Act), as amended by Act No. 323/2025 Coll. effective 1 January 2025 (mobile phone restrictions). Available at: https://www.slov-lex.sk/ezbierky/pravne-predpisy/SK/ZZ/2008/245/
- Slovak Republic (2018). Act No. 18/2018 Coll. on the Protection of Personal Data (GDPR Implementation). Available at: https://www.slov-lex.sk/ezbierky/pravne-predpisy/SK/ZZ/2018/18/
- Slovak Republic (2018). Act No. 69/2018 Coll. on Cybersecurity. Available at: https://www.zakonypreludi.sk/zz/2018-69
- Slovak Republic (2024). Act No. 366/2024 Coll. on Cybersecurity (NIS2 Transposition), effective 1 January 2025. Available at: https://www.slov-lex.sk/ezbierky/pravne-predpisy/SK/ZZ/2024/366/20250101.html

- Ministry of Education, Slovak Republic (2025). Guidance No. 1/2025 on the Prevention and Resolution of Cyberbullying in Schools and Educational Facilities. Available at: https://www.minedu.sk/data/att/d76/32441.fb1a83.pdf
- Ministry of Education, Slovak Republic (2025). Plan for the Responsible Use of Artificial Intelligence in Education 2025-2027. Available at: https://ai.iedu.sk/

Normas ISO

As seguintes normas reconhecidas internacionalmente fundamentaram o desenvolvimento das recomendações práticas e das medidas de governação apresentadas nesta Política.

- International Organization for Standardization (ISO), ISO/IEC 27001:2022, Information security, cybersecurity and privacy protection - Information security management systems - Requirements. Available at: https://www.iso.org/standard/27001
- International Organization for Standardization (ISO), ISO/IEC 27002:2022, Information security, cybersecurity and privacy protection - Information security controls. Available at: https://www.iso.org/standard/75652.html
- International Organization for Standardization (ISO), ISO/IEC 27701:2025, Security techniques - Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management - Requirements and guidelines. Available at: https://www.iso.org/standard/27701
- International Organization for Standardization (ISO), ISO 22301:2019, Security and resilience - Business continuity management systems - Requirements. Available at: https://www.iso.org/standard/75106.html
- International Organization for Standardization (ISO), ISO 31000:2018, Risk management - Guidelines. Available at: https://www.iso.org/standard/65694.html

Investigação e Evidência

As seguintes fontes de investigação e publicações foram utilizadas na preparação da Parte 4 desta política.

- European Commission (2025). Children's Voices on Cyberbullying: Consultation with Children Aged 12-17. Available at: https://eu-for-children.europa.eu/ciberbullying_en
- European Commission (2025). Guidelines on Measures to Ensure a High Level of Privacy, Safety and Security for Minors Online. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:C_202505519
- European Commission / Better Internet for Kids (BIK+) / Insafe network (2025-2026). BIK Policy Monitor and Helpline Statistics. Available at: https://better-internet-for-kids.europa.eu/en
- European Union Agency for Cybersecurity (ENISA) (2022). Cybersecurity Education Initiatives in the EU Member States. Available at: https://www.enisa.europa.eu/publications/cybersecurity-education-initiatives-in-the-eu-member-states
- OECD (2025). How's Life for Children in the Digital Age? Available at: https://www.oecd.org/en/publications/how-s-life-for-children-in-the-digital-age_0854b900-en.html
- Polanin, J. R., Espelage, D. L., Grotpeter, J. K., et al. (2021). A Systematic Review and Meta-analysis of Interventions to Decrease Cyberbullying Perpetration and Victimization. Prevention Science. Available at: https://link.springer.com/article/10.1007/s11121-021-01259-y
- Torgal, C. and Aksoy, C. (2022). A Meta-Analysis of School-Based Cyberbullying Prevention Programs Impact on Cyber-Bystander Behavior. School Psychology Review, 52(2). Available at: https://www.tandfonline.com/doi/full/10.1080/2372966X.2021.1913037
- World Health Organization Regional Office for Europe (2024). Health Behaviour in School-aged Children (HBSC): Findings on Bullying and Cyberbullying. Available at: https://www.who.int/europe/initiatives/health-behaviour-in-school-aged-children-(hbsc)-study

- Cyberbullying and LGBTQ Youth: A Systematic Literature Review and Recommendations for Prevention and Intervention (2018). Available at: https://pmc.ncbi.nlm.nih.gov/articles/PMC7163911/
- Correlations Between Social Media Addiction and Anxiety, Depression, FoMO, Loneliness and Self-Esteem Among Students: A Systematic Review and Meta-Analysis (2025). PLOS ONE. Available at: https://journals.plos.org/plosone/article?id=10.1371/journal.pone.0329466