CONSCIOUS YOUTH BEHAVIOURS
IN EMERGING REALITIES

R5. Documento di raccomandazioni sulle politiche in materia di sicurezza dei dati e sicurezza informatica, specificamente pensato per le scuole, in linea con le norme ISO 27001, 27002, 27701, 22301 e 31000

Comportamenti consapevoli dei giovani nelle realtà emergenti

Capofila: SIGMA BUSINESS NETWORK, Grecia

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.

Informazioni sul documento

Accordo di sovvenzione n.	**2023-1-EL01-KA220-SCH-000156982**
Acronimo	**C.Y.B.E.R.**
Titolo	**Comportamenti consapevoli dei giovani nelle realtà emergenti**
Data di inizio:	16/11/2023
Risultato:	Documento di raccomandazioni politiche R5
Attività correlate:	A4.5 - Progettazione e sviluppo di R5
Organizzazione capofila:	SIGMA Tournis Symvouleftiki EE, Grecia
Partner collaboratori:	• PRISM IMPRESA SOCIALE S.R.L., Italia • Centro provinciale per le risorse educative e l'assistenza di Botoșani, Romania • CPM-Centrum Prevencie Mladeze, Slovacchia • Casa Do Professor, Portogallo • Vitale Tecnologie Comunicazione - VITECO SRL, Italia • EUROCERT Eyropaiki Etaireia Emeghon Kai Pistopoihseon Anonymos Etaireia, Grecia
Livello di diffusione	Pubblico
Dichiarazione di non responsabilità	Il sostegno della Commissione europea alla realizzazione della presente pubblicazione non costituisce un'approvazione dei contenuti, che riflettono esclusivamente le opinioni degli autori, e la Commissione non può essere ritenuta responsabile per l'uso che possa essere fatto delle informazioni ivi contenute

Cronologia del documento

Data	Inviato da	Revisionato da	Versione (Note)
26/06/2026	SIGMA	Theodora Ntinou	1.0

Informazioni su CYBER	
Tipo di azione	Erasmus+ KA220-SCH - Partenariati di cooperazione nell'istruzione scolastica
Priorità	ISTRUZIONE SCOLASTICA: Sviluppo delle competenze chiave ▪ Affrontare la trasformazione digitale attraverso lo sviluppo della preparazione, della resilienza e delle capacità digitali ▪ Inclusione e diversità in tutti i settori dell'istruzione, della formazione, della gioventù e dello sport

Il progetto mira ad affrontare una questione cruciale: in che modo il cyberspazio influenza il comportamento umano, in particolare tra i giovani? Nell'odierna era digitale, il comportamento online è diventato profondamente radicato nell'ambiente psicologico del cyberspazio. Esso offre opportunità uniche per plasmare l'interazione umana, ma solleva anche preoccupazioni a causa della sua natura senza confini. Sebbene Internet apporti innegabili benefici sociali ed economici, ha messo in discussione valori europei fondamentali quali l'uguaglianza, i diritti umani e la democrazia. Per costruire un Internet più sicuro, è essenziale uno sforzo collettivo. La condivisione delle migliori pratiche e l'educazione delle giovani generazioni, degli insegnanti e dei genitori sono passi fondamentali verso la promozione di un ambiente online più sicuro.

CYBER si propone di sviluppare la resilienza informatica delle scuole europee creando procedure di qualità UE su misura per il sistema scolastico e fornendo a docenti e studenti gli strumenti e le conoscenze necessari per discutere dei comportamenti online, consci e inconsci, degli adolescenti, della cyberpsicologia e degli aspetti negativi dell'uso eccessivo di Internet, al fine di migliorare la comprensione in classe dei comportamenti pericolosi emergenti in cui un giovane utente potrebbe incorrere.

CYBER intende strutturare una metodologia per integrare i temi cruciali delle minacce informatiche e della cyberpsicologia all'interno delle classi e del sistema scolastico, promuovendo il dialogo tra gli studenti sui comportamenti pericolosi emergenti nei confronti di se stessi e dei propri coetanei. Inoltre, il progetto definisce procedure chiare in materia di sicurezza informatica e protezione dei dati affinché le scuole possano ottenere la certificazione CYBER, che stabilisce i requisiti per l'istituzione, l'attuazione, il mantenimento e il miglioramento della gestione della sicurezza delle informazioni a scuola.

I risultati del progetto sono destinati a beneficio di tutti gli adolescenti in ogni paese europeo, in particolare di coloro che sono nati nell'era digitale. Il contesto sociale in materia (hacking di profili, fake news, identità false, frodi/truffe online, ricatti online, revenge porn, hikikomori, cyberbullismo, ecc.) riveste un'importanza fondamentale, in quanto l'educazione e la sensibilizzazione dei giovani sul problema hanno un impatto di gran lunga maggiore rispetto a una normativa nazionale.

Indice

Introduzione

Il presente documento costituisce la Politica di resilienza informatica per le scuole, elaborata nell'ambito del progetto C.Y.B.E.R. (Conscious Youth Behaviours in Emerging Realities). Il progetto è cofinanziato dall'Unione europea nell'ambito del programma Erasmus+ e riunisce organizzazioni partner provenienti da Grecia, Italia, Portogallo, Romania e Slovacchia.

Oggi le scuole fanno ampio ricorso alla tecnologia digitale. Gli studenti utilizzano piattaforme online per apprendere, gli insegnanti comunicano tramite strumenti digitali e il personale gestisce i dati in sistemi interconnessi. Si tratta di uno sviluppo positivo, ma comporta anche che le scuole si trovino ad affrontare rischi che prima non esistevano: attacchi informatici, violazioni dei dati, cyberbullismo e l'impatto della vita digitale sulla salute mentale degli studenti.

La presente politica è stata concepita per aiutare ogni scuola dei cinque paesi partner ad affrontare queste sfide in modo concreto. Essa riunisce la legislazione europea, le norme nazionali di ciascun paese, gli standard di sicurezza riconosciuti a livello internazionale e le migliori ricerche disponibili, il tutto in un unico documento che qualsiasi scuola può consultare e utilizzare.

Non si tratta di un manuale tecnico, bensì di una guida destinata a tutti coloro che operano all'interno di una scuola: il dirigente scolastico, gli insegnanti, il personale amministrativo e i coordinatori informatici. Non è necessario possedere competenze giuridiche o tecniche per utilizzarla. La linea guida illustra i requisiti di legge, le buone pratiche e le azioni che la vostra scuola deve intraprendere.

I modelli e gli strumenti forniti nelle appendici sono concepiti come punti di partenza adattabili. Le scuole sono incoraggiate a modificarli per adeguarli al proprio contesto giuridico nazionale, alle procedure interne e alle circostanze specifiche.

A chi è rivolta questa politica

La presente politica è rivolta a tutti coloro che sono coinvolti nella gestione di una scuola: il preside, il vicepreside, gli insegnanti, i coordinatori informatici, il personale amministrativo scolastico e i consigli scolastici. È redatta in modo da essere comprensibile a chiunque, indipendentemente dal proprio background.

Come è strutturato il presente documento

Parte	Contenuto
Parte 1: Il quadro giuridico	Cosa prevede la normativa europea in materia di istruzione, spiegato in un linguaggio semplice.
Parte 2: Le norme del tuo paese	Le norme nazionali specifiche applicabili in ciascuno dei cinque paesi.
Standard internazionali e scuole	In che modo cinque standard di gestione riconosciuti a livello internazionale influenzano le raccomandazioni pratiche contenute in questa linea guida.

Parte	Contenuto
Parte 3: Cosa dovrebbe fare la tua scuola	Misure pratiche organizzate per argomento, basate sugli standard internazionali e sul diritto dell'UE.
Parte 4: Cosa dimostrano i dati	Cosa ci dice la ricerca scientifica su ciò che funziona davvero nelle scuole.
Appendici	Modelli di documenti e strumenti pratici di attuazione che le scuole possono adattare e utilizzare direttamente.
Riferimenti	Gli strumenti legislativi nazionali e le fonti ufficiali utilizzati nella stesura della Parte 2.

Parte 1: Il quadro giuridico

Le scuole di tutti e cinque i paesi partner devono attenersi alle leggi europee che regolano il trattamento dei dati e la protezione degli studenti online. Questa parte spiega, in un linguaggio semplice, cosa prevedono tali leggi. Esistono sei principali strumenti giuridici che ogni scuola deve conoscere. Insieme, essi riguardano la protezione dei dati, la sicurezza informatica, l'intelligenza artificiale, le piattaforme online, le comunicazioni digitali e la sicurezza dei prodotti digitali.

1.1 Regolamento generale sulla protezione dei dati (GDPR)

Il GDPR costituisce il fondamento della protezione dei dati in Europa. Si applica a ogni organizzazione che tratta dati personali, comprese le scuole. In ambito scolastico, i dati personali includono nomi e numeri di identificazione degli studenti, registri delle presenze, voti, informazioni sanitarie, foto e qualsiasi altra informazione relativa a una persona identificabile.

Il GDPR riconosce i minori come un gruppo particolarmente vulnerabile. Le scuole devono quindi applicare uno standard di diligenza più elevato nel trattamento dei dati degli studenti rispetto a quello applicato per gli adulti.

Cosa richiede il GDPR alle scuole:

- Le scuole devono disporre di una chiara base giuridica per ogni attività di trattamento dei dati. Nella maggior parte dei casi si tratterà di un obbligo di legge previsto dalla normativa nazionale in materia di istruzione, di un compito pubblico necessario per la gestione della scuola o, in alcuni casi, del consenso.
- Le scuole dovrebbero raccogliere solo i dati di cui hanno effettivamente bisogno. Non devono raccogliere informazioni aggiuntive semplicemente perché potrebbero tornare utili un giorno.
- Le scuole dovrebbero nominare un responsabile della protezione dei dati (DPO). A seconda del paese, tale figura può essere gestita a livello di autorità o di raggruppamento scolastico piuttosto che per ogni singola scuola.
- Le scuole dovrebbero effettuare una valutazione d'impatto sulla protezione dei dati (DPIA) prima di introdurre qualsiasi nuovo sistema digitale che comporti il trattamento su larga scala dei dati degli studenti o il monitoraggio comportamentale. Un modello è incluso nell'Appendice V.

- Le scuole dovrebbero segnalare le violazioni dei dati personali all'autorità di controllo nazionale entro 72 ore dal momento in cui ne vengono a conoscenza.
- Le scuole dovrebbero informare gli studenti e i genitori su come vengono utilizzati i loro dati, con un linguaggio chiaro e semplice.
- Gli studenti e i genitori hanno il diritto di accedere ai dati in loro possesso, di richiederne la rettifica e, in alcune circostanze, di richiederne la cancellazione.

Età del consenso digitale

Il GDPR consente a ciascun paese dell'UE di stabilire l'età a partire dalla quale un giovane può acconsentire all'utilizzo delle piattaforme digitali senza l'approvazione dei genitori. Tale età varia dai 13 ai 16 anni nei cinque paesi partner. Per gli studenti al di sotto dell'età nazionale di consenso digitale, le scuole devono ottenere il consenso scritto dei genitori o del tutore prima di iscriverli alle piattaforme digitali. L'età specifica per ciascun paese è indicata nella Parte 2.

1.2 Direttiva NIS2

La direttiva NIS2 definisce un quadro comune europeo per la sicurezza informatica. Essa impone alle organizzazioni di adottare misure adeguate di sicurezza informatica, di gestire i rischi posti dai propri fornitori digitali e di segnalare gli incidenti significativi di sicurezza informatica all'autorità nazionale.

Le scuole non sono sempre classificate direttamente come entità essenziali o importanti ai sensi della NIS2. Tuttavia, le scuole dipendono fortemente dai sistemi digitali e gli incidenti di sicurezza informatica che colpiscono tali sistemi possono compromettere l'istruzione e mettere a rischio i dati degli studenti. Il quadro normativo della NIS2 definisce lo standard a cui tutte le scuole dovrebbero aspirare, indipendentemente dal fatto che siano formalmente classificate o meno.

Cosa comporta la direttiva NIS2 per le scuole:

- Le scuole dovrebbero attuare misure di sicurezza informatica adeguate ai rischi che devono affrontare. Ciò significa, come minimo, password complesse, backup regolari e reti protette.
- Le scuole dovrebbero verificare le pratiche di sicurezza informatica dei propri fornitori di servizi digitali. Una piattaforma utilizzata per i dati degli studenti deve essere sicura quanto la scuola stessa.
- Le scuole dovrebbero disporre di una procedura per individuare e rispondere agli incidenti di sicurezza informatica. Il personale deve sapere chi contattare e quali passaggi seguire.
- Le scuole dovrebbero fornire una formazione periodica sulla sicurezza informatica a tutto il personale.
- Gli incidenti significativi devono essere segnalati all'autorità nazionale per la sicurezza informatica. Le scadenze e le autorità competenti variano da paese a paese. Si veda la Parte 2.

1.3 Legge dell'UE sull'intelligenza artificiale

La legge sull'IA è la prima normativa europea completa che disciplina l'uso dell'intelligenza artificiale. È entrata in vigore nell'agosto 2024 e si applica progressivamente fino alla piena attuazione nell'agosto 2026. Le scuole utilizzano sempre più spesso strumenti basati sull'IA: piattaforme di apprendimento adattivo, sistemi di valutazione automatizzati, chatbot e analisi dei dati di apprendimento. La legge sull'IA stabilisce regole chiare su come questi strumenti possono e non possono essere utilizzati.

Cosa richiede la legge sull'IA alle scuole:

- Alcuni utilizzi dell'IA nelle scuole sono completamente vietati. Tra questi figurano i sistemi di riconoscimento delle emozioni utilizzati per monitorare gli studenti, la classificazione biometrica degli studenti e il riconoscimento facciale in tempo reale in contesti educativi. Non sono previste eccezioni per le scuole.
- I sistemi di IA utilizzati per la valutazione, l'ammissione o il monitoraggio degli studenti sono classificati come ad alto rischio e devono soddisfare requisiti rigorosi in materia di trasparenza, supervisione umana e documentazione.
- Gli studenti e i genitori devono essere informati quando gli strumenti di IA vengono utilizzati in modi che influenzano le decisioni educative.
- Un insegnante deve sempre esaminare e assumersi la responsabilità di qualsiasi raccomandazione generata dall'IA che abbia un impatto su uno studente. L'IA non può prendere decisioni definitive sugli studenti.
- Le scuole devono tenere un elenco scritto di tutti gli strumenti di IA in uso, specificando le funzioni di ciascuno e i dati che tratta.

1.4 Digital Services Act (DSA)

Il DSA disciplina le piattaforme online e i servizi digitali. Esso impone alle piattaforme una maggiore trasparenza, l'obbligo di fornire modalità accessibili per segnalare contenuti dannosi e di rafforzare le tutele a favore dei giovani. Le scuole svolgono un ruolo importante nell'aiutare gli studenti a comprendere il funzionamento delle piattaforme online e come proteggersi.

Cosa comporta il DSA per le scuole:

- Le scuole dovrebbero insegnare agli studenti come riconoscere e segnalare i contenuti dannosi sulle piattaforme che utilizzano.
- Le scuole dovrebbero aiutare gli studenti a comprendere come funzionano gli algoritmi di raccomandazione e in che modo influenzano ciò che i giovani vedono online.
- Gli insegnanti dovrebbero essere a conoscenza degli obblighi che il DSA impone alle principali piattaforme ed essere in grado di discuterne con gli studenti nell'ambito dell'educazione all'alfabetizzazione digitale.

1.5 Direttiva ePrivacy

La direttiva ePrivacy tutela la riservatezza delle comunicazioni elettroniche. Si applica ai sistemi di posta elettronica, alle piattaforme di messaggistica, agli strumenti di videoconferenza e a qualsiasi altro servizio di comunicazione digitale utilizzato nelle scuole.

Cosa comporta la direttiva ePrivacy per le scuole:

- Le comunicazioni digitali tra studenti, genitori, insegnanti e personale amministrativo devono essere sicure e riservate.
- Gli strumenti di videoconferenza utilizzati per la didattica a distanza devono essere configurati in modo da impedire accessi non autorizzati. Le aule virtuali devono richiedere un accesso prima che chiunque possa partecipare.
- Le lezioni e le riunioni non dovrebbero essere registrate senza il consenso esplicito di tutti i partecipanti.

- I siti web e le piattaforme scolastiche che utilizzano i cookie devono visualizzare un avviso sui cookie conforme alla normativa.

1.6 Legge sulla sicurezza informatica

La legge sulla sicurezza informatica rafforza il ruolo dell'ENISA, l'Agenzia dell'UE per la sicurezza informatica, e istituisce un quadro europeo per la certificazione della sicurezza dei prodotti e dei servizi digitali. Essa sostiene l'adozione di tecnologie affidabili in tutta l'UE, comprese le scuole.

Cosa comporta la legge sulla sicurezza informatica per le scuole:

- Quando le scuole scelgono strumenti, piattaforme o attrezzature digitali, devono tenere conto della sicurezza informatica e, ove possibile, privilegiare prodotti certificati o approvati.
- I dispositivi connessi presenti in classe, quali lavagne interattive, tablet e telecamere, devono essere configurati in modo sicuro e mantenuti aggiornati.
- Le scuole possono consultare le linee guida e gli strumenti dell'ENISA per pianificare il proprio approccio alla sicurezza informatica.

1.7 Come queste leggi interagiscono tra loro

Questi sei strumenti giuridici non costituiscono obblighi separati da affrontare uno per uno. Essi formano un quadro integrato. Una scuola che protegga i dati degli studenti ai sensi del GDPR, gestisca la sicurezza informatica ai sensi della direttiva NIS2, utilizzi l'intelligenza artificiale in modo responsabile ai sensi della legge sull'IA, insegni l'alfabetizzazione digitale in linea con la DSA, garantisca la sicurezza delle proprie comunicazioni ai sensi della direttiva ePrivacy e selezioni tecnologie affidabili in linea con la legge sulla sicurezza informatica avrà adempiuto a tutti i propri obblighi giuridici.

Legge	L'obbligo fondamentale per le scuole
GDPR	Proteggere i dati personali, nominare un responsabile della protezione dei dati (DPO), ottenere il consenso ove necessario, segnalare le violazioni entro 72 ore.
Direttiva NIS2	Adottare misure di sicurezza informatica, verificare i propri fornitori, segnalare gli incidenti, formare il personale.
Legge UE sull'IA	Non utilizzare l'IA vietata, mantenere il controllo delle decisioni nelle mani degli esseri umani, informare studenti e genitori.
Legge sui servizi digitali	Insegnare agli studenti a segnalare i contenuti dannosi e a comprendere il funzionamento degli algoritmi.
Direttiva ePrivacy	Garantire la sicurezza delle comunicazioni digitali, proteggere le aule virtuali, rispettare le norme sui cookie.
Legge sulla sicurezza informatica	Tenete conto della sicurezza quando acquistate tecnologia, proteggete i dispositivi connessi, seguite le linee guida dell'ENISA.

Parte 2: Cosa si applica nel tuo paese

Il diritto europeo definisce il quadro comune, ma ogni paese dispone anche di leggi e linee guida nazionali che le scuole devono seguire. Questa parte riassume le norme nazionali più importanti per ciascuno dei cinque paesi partner. Trova il tuo paese e verifica quali norme si applicano al tuo caso.

2.1 Grecia

La Grecia adotta un modello altamente centralizzato per la governance digitale delle scuole. La sicurezza informatica, la protezione dei dati e le infrastrutture digitali sono gestite principalmente a livello nazionale dal Ministero dell'Istruzione e dal Ministero della Governance Digitale. Le singole scuole operano principalmente come utenti di sistemi gestiti a livello centrale, tra cui il sistema informativo sugli studenti MySchool, la piattaforma didattica e-Class e la Rete Scolastica Panellenica (PSN).

Ambito	Cosa significa per le scuole
Recepimento della direttiva NIS2 Legge 5160/2024 Decreto Ministeriale 1689/2025 Decreto Ministeriale n. 1899/2025	• Le scuole devono attuare misure di gestione dei rischi e garantire che le piattaforme digitali di terze parti (ad esempio Webex) siano conformi agli standard di sicurezza informatica. • Obbligo di segnalazione degli incidenti: le scuole devono notificare all'EAKE gli incidenti significativi relativi alla sicurezza informatica. • Sono richieste politiche di sicurezza formali che coprano il controllo dell'accesso ai dati degli studenti, le procedure di backup, la crittografia delle comunicazioni e la sicurezza della catena di fornitura per il software e l'hardware utilizzati nelle scuole. • Sono richiesti la formazione del personale e l'igiene informatica: il personale scolastico è spesso bersaglio di attacchi di phishing e di ingegneria sociale. • Le scuole devono conservare la documentazione, comprese le politiche di sicurezza, i registri di formazione, gli schemi di rete e i risultati degli audit periodici sulla sicurezza. • Il decreto MD 1899/2025 richiede la designazione di un responsabile della sicurezza informatica e l'adozione di procedure formali di risposta agli incidenti e di escalation.
Protezione dei dati Legge 4624/2019	• Regola il trattamento dei dati personali da parte degli enti del settore pubblico, comprese le scuole, in linea con i principi del GDPR. • Stabilisce il ruolo e i poteri di vigilanza dell'Autorità ellenica per la protezione dei dati (HDPA). • Le responsabilità del responsabile della protezione dei dati (DPO) sono gestite a livello dell'Autorità piuttosto che a livello di singola scuola. • Le scuole devono notificare all'HDPA (Autorità ellenica per la protezione dei dati) entro 72 ore qualsiasi violazione dei dati personali che possa comportare un rischio per le persone. • Le scuole devono attuare misure di sicurezza adeguate per i dati degli studenti, dei genitori e del personale.

Ambito	Cosa significa per le scuole
Età del consenso digitale	• 15 anni. • Le scuole devono ottenere il consenso scritto dei genitori o del tutore prima di iscrivere gli studenti di età inferiore ai 15 anni su qualsiasi piattaforma digitale che tratti i loro dati personali.
Cyberbullismo Legge n. 5029/2023	• Fornisce un quadro giuridico strutturato per la prevenzione e la gestione del cyberbullismo nelle scuole. • Introduce la piattaforma nazionale di segnalazione stop-bullying.gov.gr per la segnalazione formale e il monitoraggio degli episodi. • Le scuole devono partecipare attivamente all'identificazione, alla segnalazione e alla gestione dei casi di cyberbullismo. • Le scuole devono disporre di una procedura scritta per la gestione degli episodi di cyberbullismo.
Cellulari	• Agli studenti è vietato possedere o utilizzare telefoni cellulari all'interno dei locali scolastici. • Politica di tolleranza zero in vigore dal 2024. • Le violazioni comportano immediate conseguenze disciplinari, compresa la sospensione.
L'intelligenza artificiale nell'istruzione	• Non sono state emanate linee guida nazionali specifiche per l'uso dell'IA nelle scuole. • Si applica direttamente la legge dell'UE sull'IA. • Le scuole dovrebbero prestare attenzione nell'utilizzo di strumenti di IA che trattano i dati degli studenti.
Infrastruttura digitale	• MySchool: sistema informativo nazionale sugli studenti, gestito a livello centrale. • e-Class: piattaforma nazionale di gestione dell'apprendimento. • Rete scolastica panellenica (PSN): infrastruttura nazionale di connettività sicura per tutte le scuole pubbliche.
Contatti principali	• Sicurezza informatica: EAKE (cyber.gov.gr) • Protezione dei dati: HDPA (dpa.gr) • Cyberbullismo: stop-bullying.gov.gr

2.2 Italia

L'Italia adotta un modello prevalentemente centralizzato, sebbene le scuole mantengano un certo grado di autonomia organizzativa. L'Agenzia nazionale per la sicurezza informatica (ACN) svolge un ruolo centrale nel coordinamento e nella gestione degli incidenti. Le scuole dipendono in larga misura dalle linee guida ministeriali e dalle piattaforme gestite a livello centrale, tra cui la piattaforma nazionale Unica. Il Garante ha pubblicato linee guida specifiche per le scuole e una sezione di domande frequenti che le scuole dovrebbero consultare insieme al GDPR.

Area	Cosa significa per le scuole
Recepimento della direttiva NIS2 Decreto legislativo 138/2024 Legge 109/2021	• Il decreto legislativo 138/2024 definisce le aspettative in materia di valutazione dei rischi, sicurezza dei fornitori e segnalazione degli incidenti anche per le scuole non classificate direttamente come entità NIS. • Le scuole devono gestire i servizi ICT di terze parti e mantenere canali di segnalazione strutturati quando gli incidenti incidono sulle attività didattiche o sui dati degli studenti. • La legge n. 109 del 2021 istituisce l'Agenzia nazionale per la sicurezza informatica (ACN), che svolge un ruolo centrale di coordinamento per la governance della sicurezza informatica in tutte le istituzioni pubbliche, comprese le scuole.
Protezione dei dati Decreto legislativo 196/2003 (modificato dal decreto 101/2018)	• Regola il trattamento dei dati di studenti, genitori, insegnanti e personale nell'ambito delle attività scolastiche. • L'autorità di controllo è il Garante per la protezione dei dati personali. • La nomina del Responsabile della protezione dei dati (DPO) è obbligatoria per le scuole pubbliche, ma può essere organizzata a livello scolastico o tramite accordi condivisi tra più scuole. • È richiesta l'autorizzazione dei genitori per il trattamento dei dati dei minori qualora i servizi digitali siano offerti direttamente agli studenti al di sotto dell'età del consenso digitale. • Le scuole devono informare gli studenti e i genitori dei loro diritti in materia di dati e gestire le violazioni del trattamento dei dati in linea con i requisiti del GDPR.
Età del consenso digitale	• 14 anni. • È richiesto il consenso dei genitori per gli studenti di età inferiore ai 14 anni per l'iscrizione a sistemi di gestione dell'apprendimento, la pubblicazione di fotografie e qualsiasi trattamento che coinvolga minori in ambito educativo.
Cyberbullismo Legge n. 71/2017	• Fornisce un quadro giuridico per la lotta al cyberbullismo nelle scuole. • Le scuole devono disporre di procedure scritte per la gestione degli incidenti e il sostegno alle vittime. • Le scuole possono richiedere la rimozione di contenuti dannosi dalle piattaforme online.
Telefoni cellulari Nota MIM n. 5274/2024	• L'uso degli smartphone è limitato durante tutte le attività scolastiche in tutti i cicli educativi. • Le restrizioni mirano a proteggere l'ambiente educativo e a promuovere un uso degli strumenti digitali adeguato all'età.

Area	Cosa significa per le scuole
Circolare MIM n. 3392/2025	• Sono previste limitate eccezioni per specifiche attività didattiche o esigenze di accessibilità.
L'intelligenza artificiale nell'istruzione Decreto ministeriale n. 166/2025	• Le linee guida nazionali richiedono trasparenza sull'uso dell'IA nelle scuole. • È obbligatorio il controllo umano sulle decisioni didattiche supportate dall'IA. • Gli strumenti di IA che trattano i dati degli studenti devono rispettare i requisiti del GDPR.
Piattaforme digitali	• Unica: piattaforma nazionale per funzioni amministrative e didattiche. • Microsoft 365 for Education: suite gestita a livello istituzionale per l'insegnamento e la comunicazione. • Il quadro di riferimento per la Didattica Digitale Integrata (DDI) (MD 89/2020) impone alle scuole di regolamentare l'uso delle piattaforme digitali, l'accesso degli studenti e le responsabilità dei docenti negli ambienti didattici online.
Contatti chiave	• Sicurezza informatica: ACN (acn.gov.it) • Protezione dei dati: Garante (garanteprivacy.it)

2.3 Portogallo

Il Portogallo dispone di uno dei quadri normativi nazionali più strutturati in materia di governance digitale scolastica tra i cinque paesi. Le scuole beneficiano del PADDE (Piano d'azione per lo sviluppo digitale scolastico), obbligatorio, del programma di supporto SeguraNet e del CERT.PT per la risposta agli incidenti. La direttiva NIS2 è stata recepita tramite il decreto-legge 125/2025, entrato in vigore il 3 aprile 2026.

Area	Cosa significa per le scuole
Recepimento della direttiva NIS2 Decreto-legge n. 125/2025 (in vigore dal 3 aprile 2026) Legge n. 46/2018	• Le scuole che rientrano nella categoria degli Enti Pubblici Rilevanti (Gruppo A o B) devono attuare misure di gestione dei rischi di sicurezza informatica. • È obbligatoria la nomina di un responsabile della sicurezza informatica. • Gli incidenti significativi devono essere segnalati al CNCS entro 24 ore. • Le scuole devono identificare le risorse digitali critiche, stabilire procedure di risposta agli incidenti e garantire la continuità operativa. • La legge n. 46/2018 rimane il quadro di riferimento fondamentale che istituisce il CNCS come autorità nazionale per la sicurezza informatica.
Protezione dei dati	• La figura del responsabile della protezione dei dati (DPO) è obbligatoria a livello di ciascun raggruppamento scolastico (agrupamento de escolas), non a livello delle singole scuole.

Area	Cosa significa per le scuole
Legge n. 58/2019	• Il responsabile della protezione dei dati (DPO) deve essere registrato presso la CNPD (Comissão Nacional de Proteção de Dados) ed è responsabile del monitoraggio della conformità al GDPR, della consulenza al personale, dello svolgimento di attività di formazione e del coordinamento con la CNPD. • Le scuole devono notificare alla CNPD, entro 72 ore, qualsiasi violazione dei dati personali che possa comportare un rischio per le persone. • Le scuole devono tenere un registro delle attività di trattamento e attuare misure di sicurezza adeguate.
Età del consenso digitale	• 13 anni. Si tratta della soglia più bassa tra i cinque paesi. • È richiesto il consenso verificabile dei genitori o del tutore prima di iscrivere studenti di età inferiore ai 13 anni su qualsiasi piattaforma digitale o strumento online che tratti dati personali. • Ciò vale per i sistemi di gestione dell'apprendimento, la pubblicazione di fotografie e qualsiasi trattamento che coinvolga minori.
Cyberbullismo Programma SeguraNet	• SeguraNet (gestito dalla DGE in collaborazione con il CNCS) fornisce indicazioni specifiche sulla prevenzione e la risposta al cyberbullismo. • Le scuole devono integrare la prevenzione del cyberbullismo nel proprio PADDE e nei regolamenti interni. • I modelli delle procedure di risposta agli incidenti e i documenti relativi alla Politica di Utilizzo Accettabile sono disponibili tramite SeguraNet.
Telefoni cellulari Decreto-legge n. 95/2025 (in vigore da settembre 2025)	• L'uso degli smartphone è vietato per legge a tutti gli studenti dal 1° al 6° anno in tutte le scuole pubbliche e private. • Per il ciclo 3 e la scuola secondaria, il Ministero ha emanato raccomandazioni che incoraggiano l'adozione di restrizioni, lasciando alle scuole l'autonomia di formalizzare le norme nei propri regolamenti interni. • Qualsiasi registrazione degli studenti richiede il consenso esplicito ai sensi del GDPR.
Piano digitale scolastico obbligatorio Quadro PADDE	• Ogni polo scolastico deve elaborare e mantenere un PADDE (Piano d'Azione per lo Sviluppo Digitale della Scuola). • Il PADDE deve includere esplicitamente misure di sicurezza informatica e coprire tre dimensioni: organizzativa (leadership e governance), pedagogica (cittadinanza digitale ed educazione all'uso sicuro di Internet) e tecnologica (infrastruttura e sicurezza). • Le scuole devono adottare una Politica di Uso Accettabile e stabilire procedure di risposta agli incidenti facendo riferimento al CERT.PT.

Area	Cosa significa per le scuole
L'intelligenza artificiale nell'istruzione	• Non sono state ancora emanate linee guida nazionali specifiche. • Si applica direttamente la legge dell'UE sull'IA. • La DGE ha riconosciuto la necessità di un quadro normativo nazionale e dovrebbe emanare delle raccomandazioni. • Le scuole dovrebbero prestare attenzione nell'utilizzo di strumenti di IA che trattano i dati degli studenti.
Infrastruttura digitale	• RCTS (gestita dalla FCCN): rete nazionale sicura ad alta velocità per tutti i distretti scolastici pubblici. • Microsoft 365 for Education: suite gestita a livello nazionale per l'insegnamento e la comunicazione. • CERT.PT (gestito dal CNCS): CSIRT nazionale e punto di contatto per la risposta agli incidenti nel settore dell'istruzione.
Contatti chiave	• Sicurezza informatica: CNCS (cncs.gov.pt) • Risposta agli incidenti: CERT.PT • Protezione dei dati: CNPD (cnpd.pt) • Sicurezza digitale: SeguraNet (seguranet.pt)

2.4 Romania

Il quadro nazionale è coordinato dal Ministero dell'Istruzione in collaborazione con la Direzione Nazionale per la Sicurezza Informatica (DNSC), nell'ambito del più ampio quadro politico nazionale ed europeo in materia di sicurezza informatica. In molte scuole, le responsabilità relative alla sicurezza informatica sono assunte dal preside, dal coordinatore ICT o da un insegnante designato, poiché è raro che vi sia personale dedicato alla sicurezza informatica. La Romania presenta alcune delle maggiori lacune di attuazione tra i cinque paesi partner, ma si registra un crescente slancio per affrontarle.

Area	Cosa significa per le scuole
Recepimento della direttiva NIS2 OUG 155/2024 (approvato con la Legge 124/2025) Legge 58/2023	• L'OUG 155/2024 si applica direttamente all'istruzione superiore. Per le scuole pre-universitarie, l'applicabilità non è del tutto chiara, ma le scuole che interagiscono con le reti governative (ad esempio SIIIR) sono tenute a seguire i protocolli NIS2. • Gli istituti scolastici sono tenuti a segnalare gli incidenti significativi al DNSC entro 24 ore tramite la piattaforma PNRISC. • Le misure richieste includono: segmentazione della rete (Wi-Fi separato per l'amministrazione e gli studenti), autenticazione a più fattori per l'accesso alle piattaforme ufficiali, politiche di analisi dei rischi e formazione obbligatoria in materia di «cyber-igiene» per tutto il personale. • Sicurezza della catena di approvvigionamento: i fornitori privati di piattaforme di e-learning o di software di contabilità

Area	Cosa significa per le scuole
	utilizzati dalle scuole devono essere conformi alla direttiva NIS2. • La legge 58/2023 stabilisce che la responsabilità della sicurezza informatica ricade sull'ente proprietario o gestore della rete, rendendo la direzione scolastica direttamente responsabile.
Protezione dei dati Legge n. 190/2018	• Le scuole sono classificate come titolari del trattamento indipendenti e devono garantire la piena conformità al GDPR. • È consentito un accordo di condivisione del responsabile della protezione dei dati (DPO) a livello di ispettorato provinciale o centrale. • Le scuole devono attuare procedure obbligatorie di consenso dei genitori per le piattaforme di apprendimento online e per l'utilizzo delle immagini degli studenti. • La videosorveglianza è consentita esclusivamente a fini di protezione delle persone e dei beni, con l'obbligo di informare studenti, docenti e visitatori. Le registrazioni non devono essere conservate per più di 30 giorni, salvo nel caso di incidenti oggetto di indagine. • I risultati degli esami devono essere pubblicati utilizzando l'anonimizzazione o la pseudonimizzazione in linea con le linee guida dell'ANSPDCP.
Età del consenso digitale	• 16 anni. Si tratta della soglia più alta tra i cinque paesi. • È richiesto il consenso dei genitori o del tutore prima di iscrivere studenti di età inferiore ai 16 anni su qualsiasi piattaforma digitale. • In pratica, ciò si applica praticamente a tutti gli strumenti didattici digitali utilizzati nelle scuole rumene.
Cyberbullismo ROFUIP 2025/2026 Statuto dello studente (Ordinanza 5707/2024)	• Il ROFUIP definisce e sanziona il cyberbullismo come comportamento vietato all'interno dell'ambiente scolastico. • È vietata la registrazione video o audio non autorizzata delle attività didattiche. • Il personale deve utilizzare esclusivamente strumenti digitali ufficialmente approvati e trattare i dati degli studenti con la massima riservatezza. • Lo Statuto degli studenti vieta esplicitamente qualsiasi forma di aggressione nell'ambiente virtuale. • Non esiste una piattaforma nazionale dedicata alla segnalazione. Gli incidenti vengono gestiti dalla scuola e segnalati all'ANSPDCP qualora siano coinvolti dati personali.
Telefoni cellulari Legge n. 198/2023 ROFUIP	• L'uso dei telefoni cellulari durante le lezioni è vietato agli studenti della scuola dell'infanzia, primaria e secondaria di primo grado, salvo autorizzazione da parte dell'insegnante a fini didattici.

Area	Cosa significa per le scuole
	• Durante le lezioni i telefoni devono essere spenti o in modalità silenziosa e riposti in un luogo designato, secondo quanto previsto dal ROFUIP. • Le norme relative all'uso dei telefoni durante le pause sono stabilite dal Regolamento Interno di ciascuna scuola.
L'IA nell'istruzione	• Non sono state emanate linee guida nazionali specifiche. Si applica direttamente la legge dell'UE sull'IA. • Il Ministero dell'Istruzione non ha emanato linee guida sugli strumenti di IA generativa come ChatGPT, creando così una lacuna significativa. • Le scuole dovrebbero applicare i requisiti previsti dalla legge sull'IA in materia di trasparenza, supervisione umana e protezione dei dati quando utilizzano qualsiasi strumento di IA con gli studenti.
Infrastruttura digitale	• Non esiste una rete scolastica nazionale unificata. Le scuole si affidano a provider Internet commerciali, il che comporta standard di sicurezza informatica non uniformi. • Il SIIIR (gestito a livello centrale dal Ministero) è la principale banca dati nazionale relativa agli studenti. • Le scuole utilizzano piattaforme commerciali (Google Workspace, Microsoft 365) in base a contratti individuali.
Contatti chiave	• Sicurezza informatica: DNSC (dnsc.ro) • Protezione dei dati: ANSPDCP (dataprotection.ro)

2.5 Slovacchia

La Slovacchia ha dimostrato un forte slancio legislativo nella governance digitale scolastica. La legge sulla sicurezza informatica 366/2024, le restrizioni sull'uso dei telefoni cellulari in vigore da gennaio 2025, le linee guida specifiche sul cyberbullismo (Linee guida 1/2025) e un piano nazionale sull'intelligenza artificiale nell'istruzione per il periodo 2025-2027 riflettono un approccio completo e strutturato. Secondo la legislazione slovacca, il preside della scuola è direttamente responsabile dal punto di vista legale della sicurezza informatica. Il programma infrastrutturale DigiEDU/DigiNET fornisce una connessione Internet sicura e centralizzata a tutte le scuole slovacche.

Ambito	Cosa significa per le scuole
Recepimento della direttiva NIS2 Legge n. 366/2024 Legge n. 69/2018	• La legge n. 366/2024 collega direttamente gli obblighi in materia di sicurezza informatica alla responsabilità legale del dirigente scolastico ai sensi della legge n. 596/2003 sulle scuole. Il dirigente scolastico è personalmente e legalmente responsabile della protezione dei sistemi informativi scolastici e dei dati personali. • Le scuole devono attuare misure di sicurezza di base: password complesse, software antivirus, aggiornamenti regolari, backup dei dati e controlli di accesso.

Ambito	Cosa significa per le scuole
	• Le scuole devono essere in grado di reagire ad attacchi di phishing, ransomware, fughe di dati e compromissioni del sistema. • In caso di gravi incidenti di sicurezza informatica, devono essere seguite le procedure di segnalazione obbligatorie. • La legge n. 69/2018 fornisce il quadro di riferimento fondamentale per la protezione dei sistemi informativi e delle reti, garantendo la sicurezza dei dati degli studenti e l'uso sicuro delle tecnologie digitali nelle scuole.
Protezione dei dati Legge n. 18/2018	• La figura del responsabile della protezione dei dati (DPO) è obbligatoria per le scuole pubbliche, ma non è necessario che ve ne sia uno per ogni scuola: è consentito un DPO condiviso tra più scuole. • Le scuole devono applicare il principio di minimizzazione dei dati: devono raccogliere e utilizzare solo i dati personali degli studenti strettamente necessari per l'istruzione e l'amministrazione. • L'accesso ai dati deve essere limitato alle persone autorizzate (insegnanti, dirigenti, personale amministrativo) secondo necessità. • I sistemi elettronici, le e-mail, i documenti cartacei e i dispositivi di archiviazione devono essere protetti da perdita o accesso non autorizzato. • Foto, elenchi degli studenti, risultati o informazioni sensibili non devono essere pubblicati senza una base giuridica o un consenso esplicito. • Qualsiasi violazione della protezione dei dati deve essere segnalata all'autorità competente entro 72 ore se comporta un rischio per le persone.
Età del consenso digitale	• 16 anni. • È necessario il consenso dei genitori o del tutore prima di iscrivere studenti di età inferiore ai 16 anni su piattaforme digitali.
Cyberbullismo Linee guida 1/2025	• La Linea guida 1/2025 fornisce norme specifiche sulla prevenzione e la risoluzione del cyberbullismo nelle scuole e nelle strutture educative. • Definisce i segni, le forme e le manifestazioni fondamentali del cyberbullismo. • Stabilisce procedure di prevenzione e metodi per affrontare gli incidenti. • Include procedure per il sostegno alle vittime. • Le scuole devono attuare le procedure stabilite nella presente linea guida.

Ambito	Cosa significa per le scuole
Telefoni cellulari Legge n. 245/2008 (modificata a partire da gennaio 2025)	• Agli studenti delle classi dalla 1ª alla 3ª non è consentito utilizzare in alcun modo telefoni cellulari o dispositivi simili durante l'orario scolastico. • Gli studenti delle classi dalla quarta alla nona possono utilizzarli solo a fini didattici, previa espressa autorizzazione dell'insegnante. • È prevista un'eccezione per gli alunni con disabilità che utilizzano il dispositivo in relazione alle loro condizioni di salute. • In caso di violazione, la scuola può confiscare temporaneamente il dispositivo. • Le condizioni dettagliate sono disciplinate dal regolamento interno della scuola.
L'IA nell'istruzione Piano sull'IA 2025-2027	• Il Piano del Ministero dell'Istruzione per l'uso responsabile dell'IA nell'istruzione 2025-2027 fornisce orientamenti pratici a livello nazionale per le scuole. • Le scuole dovrebbero avvalersi di questo piano, insieme alla legge dell'UE sull'IA, per valutare e regolamentare gli strumenti di IA che introducono. • L'accento è posto sulla sicurezza, sull'uso etico e sulla trasparenza.
Infrastruttura digitale	• DigiEDU/DigiNET: programma di connettività Internet sicura e gestita a livello centrale per tutte le scuole slovacche. • La sicurezza informatica è supervisionata dall'Ufficio nazionale per la sicurezza (NBU), che gestisce SK-CERT per la risposta agli incidenti. • L'NBU fornisce orientamento e supporto alle istituzioni pubbliche, comprese le scuole.
Contatti chiave	• Sicurezza informatica: NBU/SK-CERT (nbu.gov.sk) • Protezione dei dati: UOOU (dataprotection.gov.sk)

Standard internazionali e scuole

Le raccomandazioni pratiche contenute nella Parte 3 della presente politica si basano su una serie di standard di gestione riconosciuti a livello internazionale. Questa breve sezione spiega quali sono tali standard e perché sono importanti per le scuole. Non è necessario conoscere gli standard stessi per seguire le linee guida della Parte 3. Gli standard forniscono una base collaudata e ampiamente accettata che conferisce a questa politica la sua struttura e credibilità.

In questo contesto sono rilevanti cinque standard. Ciascuno di essi affronta un aspetto diverso di come le scuole possono proteggere i propri studenti, i loro dati e i propri sistemi.

La norma ISO/IEC 27001 è lo standard internazionale per la gestione della sicurezza delle informazioni. Fornisce un quadro di riferimento per identificare quali informazioni sono in possesso di una scuola, comprendere i rischi a cui tali informazioni sono esposte e mettere in atto le misure adeguate per proteggerle. Nel contesto scolastico, ciò comprende i dati degli studenti, i dati del personale, le piattaforme digitali e tutti i sistemi che supportano l'insegnamento e l'amministrazione. La norma ISO 27001 non prescrive soluzioni tecniche specifiche. Piuttosto, definisce un approccio sistematico alla sicurezza, assicurando che nulla di importante venga trascurato. Le azioni pratiche descritte nelle sezioni da 3.1 a 3.7 si basano tutte su questo quadro di riferimento.

La norma ISO/IEC 27002 affianca la norma ISO 27001 e fornisce i controlli dettagliati che consentono di mettere in pratica la sicurezza delle informazioni. Mentre la norma ISO 27001 descrive il quadro di riferimento gestionale, la norma ISO 27002 descrive le misure specifiche: come controllare l'accesso ai sistemi, come gestire le password, come gestire gli incidenti, come configurare i dispositivi in modo sicuro. Le sezioni 3.2 e 3.3 attingono in modo più diretto a questa norma.

La norma ISO/IEC 27701 estende il quadro di riferimento per la sicurezza delle informazioni per coprire specificamente la protezione dei dati personali. È direttamente collegata al GDPR e aiuta le scuole a dimostrare che gestiscono i dati degli studenti e del personale in modo responsabile. La sezione 3.1 si basa su questa norma.

La norma ISO 22301 riguarda la gestione della continuità operativa. Per le scuole, ciò significa essere preparate ad affrontare eventuali interruzioni: un attacco informatico, un guasto al sistema, un incidente causato da un ransomware che blocchi l'accesso alle cartelle degli studenti. La norma ISO 22301 incoraggia le organizzazioni a pianificare in anticipo tali situazioni, a predisporre procedure di backup e ripristino e a testarle regolarmente affinché funzionino quando necessario. Una scuola che adotta questo approccio è in grado di riprendersi rapidamente da un incidente, anziché dover affrontare settimane di interruzione delle attività. La sezione 3.2 e la procedura di risposta agli incidenti riportata nell'Appendice IV riflettono questo standard.

La norma ISO 31000 riguarda la gestione del rischio. Fornisce un modo di concepire il rischio applicabile a tutti gli ambiti della vita scolastica, non solo alla sicurezza informatica. Prima di adottare una nuova piattaforma digitale, prima di introdurre uno strumento di intelligenza artificiale, prima di modificare le modalità di trattamento dei dati degli studenti, una scuola dovrebbe chiedersi: cosa potrebbe andare storto, con quale probabilità e quali sarebbero le conseguenze? Questo è il ragionamento che sta alla base del processo DPIA descritto nell'Appendice V, dell'approccio di valutazione delle piattaforme illustrato nella Sezione 3.3 e dell'approccio più ampio orientato alla consapevolezza dei rischi presente in tutta la Parte 3.

Insieme, questi cinque standard costituiscono la spina dorsale della Parte 3. Sono la ragione per cui le raccomandazioni contenute in questa politica non sono arbitrarie. Rappresentano decenni di conoscenze accumulate su come le organizzazioni possano proteggere le proprie informazioni, gestire i propri rischi e continuare a operare quando le cose vanno male. Le linee guida che seguono traducono tali conoscenze in misure pratiche che qualsiasi scuola può adottare.

Parte 3: Cosa dovrebbe fare la vostra scuola

Questa parte è organizzata in sette aree. Ciascuna area inizia con una breve spiegazione della sua importanza, seguita da una tabella che illustra cosa deve fare la vostra scuola, perché ogni azione è importante e come attuarla.

Le raccomandazioni contenute in questa sezione sono più efficaci quando coinvolgono l'intera comunità scolastica. Dirigenti scolastici, insegnanti, personale amministrativo, studenti, genitori e organizzazioni di supporto esterne hanno tutti un ruolo da svolgere nella creazione di un ambiente digitale sicuro. Una comunicazione regolare, una formazione pratica e canali di segnalazione affidabili aiutano le scuole a costruire una cultura della resilienza informatica, anziché limitarsi a reagire agli incidenti.

3.1 Protezione dei dati personali

Le scuole detengono una grande quantità di informazioni personali relative a studenti, genitori e personale. Queste includono nomi, numeri di identificazione, registri delle presenze, voti, informazioni sanitarie e recapiti dei familiari. La protezione di questi dati è un obbligo di legge. È anche una questione di fiducia. Le famiglie condividono informazioni sensibili con le scuole perché sono costrette a farlo. Le scuole hanno la responsabilità di gestirle con attenzione.

Quando la protezione dei dati fallisce, le conseguenze possono essere gravi. Le informazioni sugli studenti potrebbero essere esposte a persone che non dovrebbero averne accesso. La scuola potrebbe essere sottoposta a un'indagine formale. E la fiducia degli studenti e delle famiglie può essere difficile da ricostruire. Mettere le basi giuste fin dall'inizio è molto più facile che affrontare le conseguenze di una violazione.

Cosa	Perché è importante	Come procedere
Nominare un responsabile della protezione dei dati (DPO)	Il DPO è la persona incaricata di garantire che la vostra scuola rispetti la normativa sulla protezione dei dati. Senza di lui, non vi è una chiara attribuzione di responsabilità quando qualcosa va storto. Il DPO è inoltre il referente principale per studenti, genitori e l'autorità di controllo nazionale.	Consultate la Parte 2 per verificare se la vostra scuola necessita di un proprio DPO o se tale ruolo è già ricoperto a livello di consorzio o di autorità. Il DPO deve essere facilmente raggiungibile da personale, studenti e genitori. È responsabile del monitoraggio della conformità, della consulenza in materia di protezione dei dati, della formazione del personale e dei rapporti con l'autorità di controllo.
Tenere un registro di tutte le attività di trattamento dei dati	Tale registro è richiesto dalla legge ai sensi dell'articolo 30 del GDPR. Esso indica quali dati personali la vostra scuola detiene, perché li detiene, chi può accedervi e per quanto tempo vengono conservati. Se l'autorità di controllo lo	Il registro deve coprire ogni categoria di dati personali trattati dalla vostra scuola: dati degli studenti, recapiti dei genitori, dati del personale, informazioni sanitarie e così via. Per ogni categoria, registrate la finalità, la base giuridica, chi ha accesso, per quanto tempo vengono conservati e cosa succede quando non sono più necessari. Il Responsabile della

Cosa	Perché è importante	Come procedere
	richiede, dovete essere in grado di presentarlo.	protezione dei dati (DPO) è responsabile di mantenerlo aggiornato.
Raccogli solo i dati di cui hai effettivamente bisogno	Ogni dato raccolto rappresenta un rischio. In caso di violazione, possono essere esposti solo i dati effettivamente in vostro possesso. Raccogliere più dati del necessario comporta anche un maggiore carico di lavoro nella gestione e un maggior rischio di non conformità.	Esamina tutti i moduli di raccolta dati, le procedure di iscrizione e le impostazioni delle piattaforme. Elimina tutti i campi che richiedono informazioni di cui la scuola non ha realmente bisogno. Se una piattaforma richiede più dati del necessario, fai pressione sul fornitore o scegli una piattaforma diversa. Stabilisci come regola che la raccolta dei dati facoltativi sia disattivata per impostazione predefinita.
Sottoscrivete accordi con ogni fornitore che tratta i dati degli studenti	Quando un'azienda tratta i dati degli studenti o del personale per vostro conto, ad esempio una piattaforma cloud, uno strumento di valutazione o un'app di comunicazione, la vostra scuola rimane legalmente responsabile del modo in cui tali dati vengono gestiti. Senza un accordo scritto, non potete dimostrare di aver adempiuto ai vostri obblighi.	Prima che qualsiasi fornitore attivi un servizio che coinvolga dati personali, deve firmare un Accordo sul trattamento dei dati. Questo deve specificare quali dati vengono trattati, per quale scopo, quali misure di sicurezza sono in atto e cosa succede ai dati al termine del contratto. Conservate copie di tutti gli accordi nei vostri archivi.
Limitate chi può accedere ai dati personali	Più persone hanno accesso ai dati, maggiore è il rischio che questi vengano utilizzati in modo improprio, divulgati accidentalmente o rubati. Ogni punto di accesso non necessario rappresenta una vulnerabilità.	Configurate l'accesso basato sui ruoli in modo che ogni membro del personale possa visualizzare solo i dati necessari per il proprio specifico incarico. Un insegnante dovrebbe poter visualizzare le cartelle dei propri studenti, non quelle dell'intera scuola. Il personale amministrativo dovrebbe accedere ai dati amministrativi, non alle cartelle cliniche o psicologiche. Verificate chi ha accesso almeno una volta all'anno e revocate immediatamente l'accesso quando qualcuno cambia ruolo o lascia l'incarico.
Informate gli studenti e i genitori su come vengono utilizzati i loro dati	Gli studenti e i genitori hanno il diritto legale di sapere quali dati vengono conservati su di loro e come vengono utilizzati. Fornire queste informazioni non è facoltativo. Le scuole che sono trasparenti sull'uso dei dati tendono anche ad	Redigete un'informativa sulla privacy in un linguaggio semplice, comprensibile a qualsiasi genitore o studente maggiorenne. Deve spiegare quali dati vengono raccolti, perché, chi può accedervi e per quanto tempo vengono conservati. Fornitela al momento dell'iscrizione degli studenti e ogni volta che si verificano cambiamenti significativi. Rendetela

Cosa	Perché è importante	Come procedere
	avere meno controversie e reclami.	disponibile in modo permanente, ad esempio sul sito web della scuola. Un modello di lettera è riportato nell'Appendice II.
Ottenere il consenso dei genitori per gli studenti al di sotto dell'età del consenso digitale	Per gli studenti al di sotto dell'età nazionale di consenso digitale, non è possibile iscriverli a una piattaforma digitale senza il consenso scritto di un genitore o tutore. Si tratta di un requisito legale. L'età varia tra i 13 e i 16 anni nei cinque paesi, il che significa che la stessa piattaforma potrebbe richiedere il consenso in un paese ma non in un altro.	Stabilite una procedura chiara per la raccolta, la registrazione e il rinnovo del consenso dei genitori. Il consenso deve essere specifico per ciascuna piattaforma, prestato liberamente e facilmente revocabile. Non date per scontato che la firma di un modulo di iscrizione generico copra tutte le piattaforme digitali. Verificate l'età minima per il consenso digitale nel vostro paese nella Parte 2.
Segnalare le violazioni dei dati entro 72 ore	Il termine di 72 ore è un requisito legale inderogabile. Se la vostra scuola rileva una violazione e non la segnala in tempo, oppure cerca di gestirla in modo discreto senza informare l'autorità di controllo, le conseguenze possono essere significativamente più gravi rispetto a quanto accadrebbe se la violazione fosse stata segnalata tempestivamente.	Predisponete una procedura scritta di risposta alle violazioni prima che si verifichi qualsiasi evento. Quando si verifica una violazione, il Responsabile della protezione dei dati (DPO) deve valutare immediatamente se essa comporti un rischio per le persone interessate. In caso affermativo, l'autorità di controllo nazionale deve essere informata entro 72 ore. Se il rischio è elevato, anche le persone interessate devono essere informate direttamente. Utilizzate il registro degli incidenti riportato nell'Appendice IV per documentare ogni fase.

Che cos'è una violazione dei dati?

Una violazione dei dati è qualsiasi incidente che comporti la perdita, la distruzione, la modifica, la divulgazione o l'accesso accidentale o illecito a dati personali da parte di qualcuno che non dovrebbe avervi accesso. Ciò include la perdita di una chiavetta USB contenente i dati degli studenti, un'e-mail inviata alla persona sbagliata, un attacco ransomware che blocca i dati della scuola o un'impostazione della piattaforma che rende accidentalmente visibili al pubblico i dati degli studenti. Molte delle violazioni più comuni nelle scuole sono causate da errori umani, non da attacchi esterni.

3.2 Garantire la sicurezza dei sistemi scolastici

La sicurezza informatica consiste nel proteggere i computer, le reti e i dati della vostra scuola da attacchi e accessi non autorizzati. Le scuole rappresentano un bersaglio allettante per i criminali informatici perché conservano dati sensibili sui minori e spesso dispongono di risorse di sicurezza limitate. Un attacco riuscito

può mettere fuori uso i sistemi scolastici, rendere pubblici i dati degli studenti, interrompere l'attività didattica per settimane e causare danni duraturi alla reputazione della scuola.

La buona notizia è che la maggior parte degli attacchi informatici che vanno a buon fine sfrutta semplici punti deboli che possono essere risolti senza competenze specialistiche o budget ingenti. Password deboli, software non aggiornato, personale che non riconosce le e-mail di phishing e backup mancanti sono alla base della maggior parte degli incidenti. Risolvere questi aspetti fondamentali fa un'enorme differenza.

Altrettanto importante è essere preparati per il momento in cui qualcosa va storto. Disporre di un backup collaudato e di una procedura di ripristino chiara fa la differenza tra un'interruzione che dura poche ore e una che si protrae per settimane. Questo è il ragionamento alla base della pianificazione della continuità operativa: non solo prevenire gli incidenti, ma garantire che la scuola possa continuare a funzionare e riprendersi rapidamente quando questi si verificano.

Cosa	Perché è importante	Come procedere
Utilizzare password complesse e l'autenticazione a più fattori	Le password deboli sono il modo più comune con cui gli hacker riescono a penetrare nei sistemi scolastici. Una password facile da indovinare, o utilizzata su più account, significa che il furto di una sola password può consentire a un hacker di accedere a tutto. L'autenticazione a più fattori aggiunge un secondo livello di controllo che protegge gli account anche in caso di furto della password.	Tutti gli account del personale devono utilizzare password complesse di almeno 12 caratteri, che combinino lettere, numeri e simboli. Le password devono essere modificate se vi è motivo di ritenere che siano state compromesse. L'autenticazione a più fattori deve essere attivata su tutti i sistemi che contengono dati degli studenti. Dopo aver inserito la password, il membro del personale deve confermare la propria identità tramite un secondo metodo, come un codice inviato al proprio telefono.
Mantenere aggiornati tutti i software e i dispositivi	Gli aggiornamenti software spesso includono correzioni per le vulnerabilità di sicurezza che gli aggressori stanno attivamente sfruttando. Molti dei peggiori attacchi ransomware contro le scuole hanno preso di mira sistemi che utilizzavano software obsoleto e non aggiornato. Si tratta di una delle vulnerabilità più facilmente prevenibili che esistano.	Stabilite un programma regolare per l'applicazione degli aggiornamenti a tutti i dispositivi, i sistemi operativi, le applicazioni e i software di sicurezza della scuola. Applicate le patch di sicurezza critiche non appena sono disponibili. Se un dispositivo non è più in grado di ricevere aggiornamenti, rimuovetelo dalla rete o sostituitelo. Assegnate a un membro specifico del personale la responsabilità di assicurarsi che gli aggiornamenti vengano effettuati.
Eseguite regolarmente il	Gli attacchi ransomware funzionano crittografando i	Configurare backup giornalieri automatici per tutti i dati critici della scuola. Conservare almeno

Cosa	Perché è importante	Come procedere
backup di tutti i dati importanti	dati e richiedendo un pagamento per ripristinarne l'accesso. L'unico modo affidabile per recuperare i dati senza pagare è disporre di un backup effettuato prima dell'attacco. Senza un backup testato, una scuola può perdere settimane di lavoro e documenti permanenti.	una copia di ogni backup in una posizione non collegata alla rete principale della scuola, in modo che non possa essere crittografata durante lo stesso attacco. Testare il processo di ripristino almeno una volta all'anno per verificare che i backup funzionino effettivamente e che i dati possano essere ripristinati in un tempo ragionevole.
Utilizzate reti separate per l'amministrazione e gli studenti	Se la rete utilizzata dal personale amministrativo, dove vengono gestiti i dati e i voti degli studenti, è la stessa utilizzata dagli studenti e dai visitatori, un dispositivo di uno studente compromesso o un portatile infetto di un visitatore potrebbe potenzialmente raggiungere i sistemi amministrativi della scuola. Si tratta di un rischio fondamentale che la separazione delle reti elimina.	Configurare reti Wi-Fi separate: una per uso amministrativo e una per studenti e visitatori. Assicurarsi che la rete amministrativa non sia visibile né raggiungibile dalla rete degli studenti. Impostare controlli di accesso in modo che solo i dispositivi scolastici autorizzati possano connettersi alla rete amministrativa.
Proteggere tutti i dispositivi scolastici	I dispositivi che presentano password predefinite di fabbrica, che non sono mai stati aggiornati o che non dispongono di protezione antivirus installata sono bersagli facili. Molte scuole dispongono di dispositivi nelle aule o negli uffici che sono stati configurati anni fa e che da allora non sono stati sottoposti a revisione.	Installate software antivirus e antimalware su tutti i dispositivi scolastici e manteneteli aggiornati. Modificate tutte le password predefinite su router, telecamere, stampanti e qualsiasi altra apparecchiatura collegata non appena viene installata. Effettuate un controllo periodico di tutti i dispositivi collegati. Prima di smaltire i vecchi dispositivi, assicuratevi che tutti i dati siano stati cancellati in modo definitivo e sicuro.
Predisporre un piano scritto per la gestione degli incidenti	Senza un piano scritto, il personale che si trova a dover affrontare un attacco informatico non saprà cosa fare. Decisioni prese in preda al panico o ben intenzionate ma errate, come spegnere immediatamente un	Redigete una procedura di risposta agli incidenti informatici che definisca chi coordina la risposta, quali misure adottare e in quale ordine, quali autorità nazionali contattare e entro quali tempi, e come comunicare con gli studenti, i genitori e il personale durante e dopo un incidente. Assicuratevi che tutto il personale interessato conosca la procedura prima che si verifichi un

Cosa	Perché è importante	Come procedere
	dispositivo o tentare di pagare un riscatto, possono peggiorare notevolmente una situazione già grave.	incidente. Un modello è disponibile nell'Appendice IV.
Formare tutto il personale almeno una volta all'anno	Le e-mail di phishing sono all'origine della maggior parte degli attacchi informatici riusciti contro le scuole. Un membro del personale che non è in grado di riconoscere un'e-mail di phishing rappresenta una vulnerabilità contro la quale nessun sistema tecnico può garantire una protezione completa. Un solo clic su un link dannoso può consentire a un aggressore di ottenere pieno accesso ai sistemi scolastici.	Organizzate una formazione annuale obbligatoria sulla sicurezza informatica per tutto il personale. La formazione deve includere come individuare un'e-mail di phishing, come creare e gestire password sicure, cosa fare in caso di smarrimento o furto di un dispositivo e chi contattare se qualcosa sembra sospetto. Inserite promemoria periodici durante l'anno. Ove possibile, organizzate esercitazioni simulate di phishing: sono uno dei modi più efficaci per modificare il comportamento del personale.

Che cos'è un attacco di phishing?

Il phishing si verifica quando un malintenzionato invia un'e-mail, un messaggio o una notifica che sembra provenire da una fonte attendibile, come il Ministero dell'Istruzione, un fornitore di software o un collega. L'obiettivo è indurre il destinatario a cliccare su un link dannoso, a inserire le proprie credenziali di accesso su un sito web falso o ad aprire un file infetto. Il phishing è la forma più comune di attacco informatico contro le scuole. Qualsiasi messaggio inaspettato che richieda una password, inviti a cliccare urgentemente su un link o chieda di compiere un'azione insolita deve essere considerato con sospetto e verificato tramite un canale separato prima di rispondere.

3.3 Scegliere e utilizzare le piattaforme digitali in modo sicuro

Le scuole utilizzano un numero crescente di piattaforme digitali per l'insegnamento, la comunicazione e l'amministrazione. Ogni piattaforma che tratta i dati degli studenti rappresenta una potenziale fonte di rischio. Una piattaforma con misure di sicurezza inadeguate, che condivide i dati con gli inserzionisti o che archivia le informazioni degli studenti al di fuori dell'UE senza adeguate garanzie può causare danni concreti. Le scuole hanno l'obbligo legale di verificare le piattaforme prima di adottarle e di gestirle con attenzione una volta che sono in uso.

Lo stesso vale per gli strumenti di intelligenza artificiale. L'IA è sempre più presente nel settore dell'istruzione, ma non tutti gli strumenti sono sicuri da utilizzare con gli studenti. La legge dell'UE sull'IA traccia linee guida chiare e le scuole devono conoscere tali limiti prima di introdurre qualsiasi strumento di IA in classe o nei processi che riguardano gli studenti.

Cosa	Perché è importante	Come procedere
Verificare ogni piattaforma prima di utilizzarla	Una piattaforma adottata senza adeguati controlli potrebbe trattare i dati degli studenti in modi non concordati dalla scuola, archiviare i dati al di fuori dell'UE o presentare vulnerabilità di sicurezza. Una volta che i dati sono stati condivisi con il fornitore sbagliato, è molto difficile tornare indietro.	Prima di adottare qualsiasi nuova piattaforma, verificare che sia conforme al GDPR, che non utilizzi i dati degli studenti a fini pubblicitari né li condivida con terze parti senza consenso, e che conservi i dati all'interno dell'UE. Se la piattaforma comporta un trattamento su larga scala dei dati degli studenti, effettuare una valutazione d'impatto sulla protezione dei dati (DPIA) prima della messa in funzione (vedi Appendice V). Firmare un accordo sul trattamento dei dati con il fornitore prima di condividere qualsiasi dato.
Tenere un elenco delle piattaforme approvate	Senza un registro centralizzato, le scuole perdono traccia di quali piattaforme siano in uso, di quando sono state controllate l'ultima volta o di chi le abbia approvate. Il personale potrebbe iniziare a utilizzare le piattaforme in modo informale senza alcuna valutazione. Gli studenti potrebbero utilizzare account personali su strumenti non approvati per i compiti scolastici, portando i dati al di fuori del controllo della scuola.	Tenere un registro scritto di tutte le piattaforme e gli strumenti digitali approvati per l'uso nella propria scuola. Registrare il nome della piattaforma, a cosa serve, quando è stata valutata e quando è prevista la prossima revisione. Rivedere il registro almeno una volta all'anno. Il personale non deve introdurre nuove piattaforme per uso scolastico senza aver prima seguito il processo di approvazione.
Configurate le piattaforme in modo sicuro	Le impostazioni predefinite delle piattaforme sono solitamente progettate per facilitare l'uso, non per garantire la sicurezza. Un'aula virtuale a cui chiunque può accedere senza effettuare il login, una funzione di registrazione attiva di default o account degli studenti con autorizzazioni eccessive	Ogni piattaforma deve essere configurata in modo sicuro prima che gli studenti o il personale inizino a utilizzarla. Gli strumenti di videoconferenza devono richiedere un accesso prima che chiunque possa entrare in un'aula virtuale. La registrazione deve essere disattivata di default e attivata solo con il consenso esplicito di tutti i presenti. Gli account degli studenti dovrebbero avere solo le autorizzazioni necessarie per le loro attività didattiche. Controllare le impostazioni almeno una volta all'anno.

Cosa	Perché è importante	Come procedere
	rappresentano tutti rischi facilmente evitabili.	
Sapere quali utilizzi dell'IA sono vietati	Alcune pratiche relative all'IA in ambito educativo sono vietate dalla normativa dell'UE. Ciò vale indipendentemente da come lo strumento sia stato commercializzato o da quanto affermato dal fornitore. Il divieto è assoluto e si applica a tutte le scuole in tutti e cinque i paesi.	Non utilizzare alcuno strumento di intelligenza artificiale che comporti il riconoscimento delle emozioni degli studenti, la loro classificazione biometrica o la loro identificazione in tempo reale tramite il riconoscimento facciale. Tali utilizzi sono vietati ai sensi dell'articolo 5 della legge dell'UE sull'intelligenza artificiale. Se un fornitore offre queste funzionalità, la scuola non deve utilizzarle. Se la scuola sta già utilizzando uno strumento di questo tipo, deve interromperne l'uso.
Lasciare alle persone il controllo delle decisioni che riguardano gli studenti	Gli strumenti di IA possono fornire raccomandazioni errate, parziali o inique. Quando tali raccomandazioni influenzano le decisioni relative a uno studente, come un voto, un rinvio o una valutazione dei bisogni di apprendimento, le conseguenze possono essere gravi. La legge richiede che sia un essere umano ad avere l'ultima parola proprio per questo motivo.	Un insegnante o un adulto responsabile deve sempre esaminare e assumersi la responsabilità di qualsiasi risultato prodotto da uno strumento di IA che abbia ripercussioni su uno studente. Gli strumenti di IA possono fornire assistenza, ma non possono prendere decisioni definitive. Documentare in che modo viene esercitata la supervisione umana per ogni strumento di IA utilizzato nel processo decisionale in ambito educativo.
Informare gli studenti e i genitori quando si utilizza l'IA	Gli studenti e i genitori hanno il diritto di sapere quando gli strumenti di IA vengono utilizzati in modi che incidono sull'istruzione di uno studente. L'utilizzo di strumenti di IA senza informarli costituisce probabilmente una violazione sia della legge sull'IA (AI Act) che del GDPR.	Quando uno strumento di IA viene utilizzato in modo tale da influire sull'apprendimento o sulla valutazione di uno studente, informare gli studenti e i genitori in modo chiaro e con un linguaggio semplice: cosa fa lo strumento, quali dati utilizza, come vengono utilizzati i suoi risultati e come funziona la supervisione umana. Fornire queste informazioni prima che lo strumento venga utilizzato e mantenerle accessibili in modo permanente.
Tenere un registro di tutti gli	Le scuole che non sanno quali strumenti di IA	Tenete un registro degli strumenti di IA come parte del vostro elenco di piattaforme

Cosa	Perché è importante	Come procedere
strumenti di IA in uso	stanno utilizzando, quali dati tali strumenti trattano o quale valutazione sia stata effettuata prima della loro adozione non possono adempiere ai propri obblighi legali ai sensi della legge sull'IA o del GDPR.	approvate. Per ogni strumento di IA, registrate quali sono le sue funzioni, in quale categoria di rischio rientra ai sensi della legge sull'IA, quali dati tratta, quale valutazione è stata effettuata prima della sua adozione e chi è responsabile della supervisione. Rivedete questo registro almeno una volta all'anno.

3.4 Gestione dei telefoni cellulari e dei dispositivi personali

Tutti e cinque i paesi partner hanno introdotto restrizioni legali sull'uso dei telefoni cellulari nelle scuole. Le norme specifiche variano da paese a paese (vedi Parte 2), ma le ragioni sono le stesse ovunque: i telefoni nelle aule distraggono gli studenti dall'apprendimento, creano rischi per la privacy e la protezione dei dati, facilitano il cyberbullismo e aumentano le pressioni digitali che incidono sulla salute mentale degli studenti.

Una politica sui telefoni cellulari è più di una semplice norma disciplinare. È una misura di protezione dei dati, una misura per il benessere e una dichiarazione dei valori della scuola. Una politica redatta in modo chiaro, realmente compresa da studenti, genitori e personale scolastico e applicata in modo coerente è di gran lunga più efficace di una che esiste solo sulla carta.

Cosa	Perché è importante	Come procedere
Disporre di una politica chiara e scritta sull'uso dei telefoni cellulari	Senza una politica scritta, le regole vengono applicate in modo diverso a seconda degli insegnanti. Non si può pretendere che studenti e genitori rispettino regole di cui non sono stati chiaramente informati. Un'applicazione incoerente crea conflitti e mina la fiducia nelle regole della scuola.	Redigete una politica sull'uso dei telefoni cellulari che specifichi quando è consentito e quando non è consentito utilizzarli, dove devono essere riposti durante gli orari in cui l'uso è limitato, quali eccezioni sono previste per esigenze mediche o attività didattiche specifiche e quali sono le conseguenze in caso di violazione delle regole. Comunicate la politica agli studenti e ai genitori all'inizio di ogni anno scolastico tramite la Politica di uso accettabile (Appendice III). Inseritela nel regolamento interno della scuola.
Limitare l'uso dei telefoni durante le lezioni	L'uso illimitato dei telefoni durante le lezioni disturba l'apprendimento, crea opportunità di cyberbullismo e registrazioni non autorizzate e aumenta le pressioni digitali che	Gli studenti non devono utilizzare i telefoni cellulari personali durante le lezioni, a meno che un insegnante non lo abbia espressamente autorizzato per una specifica attività didattica. Nei paesi in cui esiste un divieto legale, questo deve essere applicato. Specificare chiaramente dove devono essere riposti i telefoni durante gli orari in cui ne è

Cosa	Perché è importante	Come procedere
	incidono sul benessere degli studenti. Le ricerche dimostrano costantemente che gli studenti delle scuole con chiare restrizioni sull'uso dei telefoni ottengono risultati migliori a livello scolastico e riportano un maggiore benessere.	vietato l'uso. Le eccezioni per motivi medici devono essere documentate.
Vietare le registrazioni non autorizzate	Le registrazioni non autorizzate di studenti, insegnanti o altro personale costituiscono una grave violazione della privacy e possono costituire un reato penale ai sensi della legislazione nazionale. Le registrazioni condivise online possono causare danni duraturi alle persone coinvolte e alla scuola. La popolarità delle piattaforme di video brevi rende questo rischio sempre più elevato.	Chiarite in modo inequivocabile agli studenti e al personale che è vietato registrare chiunque all'interno della scuola senza il suo esplicito consenso, sia durante le lezioni, nei corridoi, durante le gite o in occasione di eventi. Indicate chiaramente le conseguenze. Trattate qualsiasi registrazione non autorizzata che coinvolga studenti o personale come una grave questione disciplinare e, se necessario, segnalatela alle autorità competenti.
Applicare standard di sicurezza ai dispositivi personali utilizzati per attività scolastiche	Quando un docente utilizza un dispositivo personale per accedere ai sistemi scolastici, la protezione dei dati della scuola è forte solo quanto l'anello più debole. Un dispositivo personale con una password debole, software obsoleto o dati degli studenti memorizzati localmente rappresenta una vera e propria vulnerabilità.	Il personale che utilizza dispositivi personali per attività scolastiche deve proteggerli con una password o un PIN forte, mantenere aggiornato il software, utilizzare una connessione sicura quando lavora da remoto e non memorizzare i dati degli studenti localmente sui dispositivi personali. Fornire indicazioni chiare al personale su ciò che ci si aspetta.

3.5 Prevenzione e risposta al cyberbullismo

Il cyberbullismo è una forma di bullismo che avviene tramite dispositivi e piattaforme digitali. Comprende l'invio di messaggi minacciosi o umilianti, la condivisione di immagini private senza consenso, la diffusione di informazioni false online e l'esclusione deliberata di qualcuno dai gruppi online. Il cyberbullismo può

causare danni gravi e duraturi alla salute mentale, al rendimento scolastico e alle relazioni sociali degli studenti.

Le scuole hanno sia l'obbligo legale che il dovere di diligenza di prevenire il cyberbullismo e di intervenire quando si verifica. Il cyberbullismo non si ferma al cancello della scuola. Ciò che accade online a casa la sera può influenzare l'esperienza scolastica di uno studente la mattina seguente, e viceversa. Le scuole devono considerare il cyberbullismo con la stessa serietà del bullismo fisico, anche quando si verifica al di fuori dell'orario scolastico.

Cosa	Perché è importante	Come agire
Includete esplicitamente il cyberbullismo nella vostra politica anti-bullismo	Una politica generale contro il bullismo che non menzioni il cyberbullismo lascia spazio a dubbi sul fatto che i comportamenti online siano contemplati. Gli studenti vittime di bullismo online potrebbero non segnalarlo perché pensano che la scuola dirà che non è un suo problema.	Aggiornate la vostra politica anti-bullismo per includere una sezione dedicata al cyberbullismo. Questa dovrebbe definire cosa sia il cyberbullismo, chiarire che viene trattato con la stessa serietà del bullismo fisico e confermare che la politica si applica ai comportamenti online al di fuori dell'orario scolastico quando questi incidono direttamente sulla comunità scolastica. Rivedete la politica almeno una volta all'anno.
Educate gli studenti sul cyberbullismo	Gli studenti che comprendono cos'è il cyberbullismo, perché provoca danni e cosa fare quando ne sono testimoni sono più propensi a segnalarlo e a sostenere un compagno che ne è vittima. Insegnare agli studenti a essere testimoni attivi e solidali è uno degli approcci più efficaci in assoluto.	Inserire l'educazione al cyberbullismo, adeguata all'età, come parte integrante del programma scolastico, non come evento isolato. Trattare le diverse forme di cyberbullismo sulle varie piattaforme, il danno che provoca, come sostenere chi ne è vittima e come segnalarlo. Coinvolgere gli studenti nella definizione dei contenuti: si sentono più coinvolti nei messaggi che hanno contribuito a creare.
Fornire agli studenti un modo chiaro e sicuro per segnalare gli episodi	Molti studenti vittime di cyberbullismo non lo segnalano. Temono di non essere creduti, che la segnalazione peggiori la situazione o che perdano l'accesso al proprio telefono. Senza un canale di segnalazione affidabile e accessibile, gli episodi	Offrite più di un modo per segnalare il cyberbullismo: un adulto di fiducia, un modulo o una cassetta anonima e, ove disponibile, la piattaforma nazionale di segnalazione (vedi Parte 2). Promuovete attivamente queste opzioni durante tutto l'anno scolastico, non solo a settembre. Quando uno studente effettua una segnalazione, rispondete rapidamente e chiarite che la prendete sul serio.

Cosa	Perché è importante	Come agire
	rimangono nascosti e peggiorano.	
Formate tutto il personale a riconoscere e reagire al cyberbullismo	Molti insegnanti non sanno bene come reagire al cyberbullismo, specialmente quando coinvolge piattaforme che non conoscono bene. L'incertezza porta a risposte incoerenti, che compromettono sia la capacità della vittima sia quella della scuola di gestire efficacemente gli episodi.	Fornite a tutto il personale una formazione che spieghi come individuare i segnali che indicano che uno studente potrebbe essere vittima di cyberbullismo, quali sono le procedure della scuola e qual è il ruolo di ciascuno al loro interno, come conservare le prove, inclusi gli screenshot, quando coinvolgere il consulente scolastico, i genitori o le autorità esterne e come sostenere uno studente senza peggiorare inavvertitamente la situazione.
Rispondete rapidamente e documentate tutto	Una risposta lenta o incoerente trasmette il messaggio che la scuola non prende sul serio il cyberbullismo. Inoltre, permette che gli incidenti si aggravino e che le prove vadano perse. Le scuole che non tengono registri adeguati hanno difficoltà a individuare schemi ricorrenti o a dimostrare di aver agito in modo appropriato nel caso in cui venga presentata una denuncia formale.	Quando viene segnalato un episodio di cyberbullismo, la priorità assoluta è la sicurezza e il benessere dello studente preso di mira. Annotate immediatamente i dettagli: data e ora, cosa è successo, quali piattaforme sono state coinvolte, chi è stato coinvolto, eventuali prove raccolte e ogni azione intrapresa. Applicate la procedura disciplinare in modo coerente. Tenetevi in contatto con lo studente preso di mira nei giorni e nelle settimane successivi all'episodio.
Coinvolgere i genitori come partner	I genitori che comprendono il cyberbullismo, sanno come parlarne con i propri figli e si sentono in sintonia con l'approccio della scuola sono di gran lunga più efficaci sia nel prevenire gli episodi che nel sostenere i propri figli quando questi si verificano.	All'inizio dell'anno scolastico informate i genitori sull'approccio della scuola al cyberbullismo, su cosa fare se il loro figlio ne è vittima e su come la scuola comunicherà con loro. Utilizzate il modello riportato nell'Appendice II. Quando si verificano episodi, coinvolgete i genitori di tutti gli studenti coinvolti, seguendo le procedure della scuola.

Le scuole non devono affrontare queste sfide da sole. La Giornata per un Internet più sicuro (febbraio) e il Mese europeo della sicurezza informatica (ottobre) forniscono alle scuole materiali di sensibilizzazione già pronti e convalidati a livello dell'UE. Il programma dell'UE «Better Internet for Kids» (BIK+) e la rete Insafe dei Centri per un Internet più sicuro gestiscono linee di assistenza, strumenti di segnalazione e risorse didattiche in tutti e cinque i paesi partner, a cui le scuole possono attingere direttamente.

3.6 Sostenere il benessere digitale degli studenti

Gli studenti affrontano online rischi che vanno oltre il cyberbullismo e le violazioni dei dati. Molti provano ansia, bassa autostima e pressioni sociali legate alla loro vita digitale. La paura di perdersi qualcosa (FOMO), la pressione di presentare online una versione idealizzata di sé stessi, il confronto costante con gli altri, il tempo eccessivo trascorso davanti allo schermo e la progettazione delle piattaforme dei social media che privilegiano il coinvolgimento a scapito del benessere contribuiscono tutti a problemi di salute mentale che colpiscono un numero significativo di giovani.

Limitare l'accesso da solo non risolve questi problemi. Gli studenti a cui viene semplicemente detto di usare meno la tecnologia, senza essere aiutati a capire il perché o senza ricevere strumenti per gestire il proprio comportamento, tendono a ricadere nelle vecchie abitudini non appena le restrizioni vengono revocate. Le scuole che ottengono cambiamenti positivi duraturi sono quelle che combinano limiti chiari con un'educazione onesta e basata su dati concreti e una cultura in cui gli studenti si sentono al sicuro nel parlare di ciò che vivono online.

Cosa	Perché è importante	Come farlo
Integrare il benessere digitale nell'assistenza pastorale	Gli studenti che hanno difficoltà con la propria vita online hanno difficoltà anche con la loro salute mentale e la loro esperienza sociale in generale. Se il benessere digitale viene trattato come un argomento informatico a sé stante, gli studenti che hanno bisogno di sostegno rischiano di cadere nelle lacune tra i vari servizi.	Il benessere digitale dovrebbe essere una componente specifica del più ampio programma scolastico dedicato al benessere e all'assistenza pastorale. Il personale che sostiene gli studenti nelle altre difficoltà dovrebbe essere pronto a supportarli anche in quelle di natura digitale. I percorsi di riferimento dovrebbero essere chiari: qualsiasi insegnante che individui uno studente in difficoltà dovrebbe sapere esattamente a chi rivolgersi e quali saranno i passi successivi.
Insegnare agli studenti abitudini digitali sane	Gli studenti che comprendono come le piattaforme dei social media siano progettate per indurli a continuare a scorrere i contenuti, che sanno distinguere tra un'immagine online curata e la realtà e che hanno sviluppato le proprie strategie per gestire le proprie abitudini digitali	Includere l'educazione al benessere digitale come parte integrante del programma scolastico. Insegnare agli studenti come funzionano gli algoritmi di raccomandazione e perché spesso mostrano contenuti che suscitano forti emozioni. Discutere gli effetti dello scorrimento passivo dei social media sull'umore e sull'autostima. Aiutare gli studenti a sviluppare strategie pratiche per stabilire dei limiti al proprio uso della tecnologia.

Cosa	Perché è importante	Come farlo
	sono in una posizione migliore per navigare in sicurezza nel mondo online.	
Assicuratevi che gli studenti sappiano dove trovare aiuto	Molti studenti che stanno affrontando difficoltà online non chiedono aiuto perché non sanno che è disponibile, perché provano imbarazzo o perché temono che il loro telefono venga confiscato. Se il sostegno non viene promosso attivamente, rimane invisibile agli studenti che ne hanno più bisogno.	Ricordate regolarmente agli studenti a chi possono rivolgersi se qualcosa online li turba. Accennatene durante le assemblee, nelle lezioni e nelle interazioni quotidiane, non solo in un manuale. La persona a cui uno studente si rivolge non deve necessariamente essere un esperto di tecnologia. Deve semplicemente essere qualcuno di cui lo studente si fida, che lo ascolti senza giudicarlo e lo metta in contatto con l'aiuto giusto.
Non aumentare la pressione digitale attraverso le pratiche scolastiche	Le scuole possono inavvertitamente creare le stesse pressioni digitali che stanno cercando di ridurre. Le chat di gruppo scolastiche obbligatorie, l'aspettativa che gli studenti rispondano ai messaggi al di fuori dell'orario scolastico e i confronti pubblici tra studenti online possono tutti trasmettere messaggi controproducenti.	Rivedete il modo in cui la scuola comunica digitalmente e valutate se alcune delle sue pratiche contribuiscano alla pressione digitale. Evitate le chat di gruppo obbligatorie che confondono il confine tra tempo scolastico e tempo libero. Non aspettatevi che gli studenti o i genitori rispondano ai messaggi al di fuori dell'orario scolastico. Evitate di pubblicare classifiche o confronti online.
Riconoscere quando uno studente è in difficoltà	Gli studenti che stanno vivendo difficoltà nella loro vita digitale potrebbero non dirlo apertamente. I segnali sono spesso comportamentali e facili da trascurare, a meno che il personale non sappia cosa cercare.	Fornite al personale indicazioni sui segnali che indicano che uno studente potrebbe trovarsi in difficoltà nella propria vita digitale: ansia insolita per l'impossibilità di controllare il proprio telefono, sbalzi d'umore a seguito di interazioni online, allontanamento dalle attività sociali dopo un evento verificatosi online, disagio legato al proprio aspetto o al modo in cui gli altri li vedono online, riluttanza a venire a scuola dopo un incidente online, o qualsiasi segno che indichi che siano sottoposti a pressioni o presi di mira online. Quando compaiono questi segnali, il personale dovrebbe seguire la procedura di segnalazione di sostegno della scuola.

3.7 Diversità, inclusione ed equità digitale

Non tutti gli studenti affrontano gli stessi rischi digitali né hanno lo stesso accesso al sostegno. Il genere, l'orientamento sessuale, la disabilità, il reddito familiare e le preoccupazioni relative all'immagine corporea influenzano l'esperienza online di uno studente e la sua capacità di ottenere aiuto quando qualcosa va storto. Una politica che funziona bene per la maggior parte degli studenti ma trascura l'esperienza degli altri non è completa.

Sviluppare un approccio inclusivo alla sicurezza digitale significa riflettere attivamente su quali studenti siano maggiormente a rischio e assicurarsi che le politiche, l'educazione e i sistemi di supporto della scuola li raggiungano.

Cosa	Perché è importante	Come procedere
Affrontare esplicitamente i danni online legati al genere e all'identità	Le ragazze subiscono tassi sproporzionatamente elevati di molestie sessuali online, abusi basati sulle immagini e cyberbullismo legato all'aspetto fisico. Gli studenti LGBTQ+ sono significativamente più esposti al rischio di subire molestie online e, di conseguenza, di soffrire di disturbi di salute mentale. Le ricerche indicano che la prevalenza segnalata di cyberbullismo tra gli studenti LGBTQ+ varia notevolmente: da circa il 10% a oltre il 70% a seconda del contesto, e che gli studenti LGB riferiscono di essere vittime di cyberbullismo a un tasso circa doppio rispetto ai loro coetanei eterosessuali. Le ricerche dimostrano che il cyberbullismo media statisticamente gran parte dell'ansia, della depressione e della solitudine elevate segnalate dagli studenti appartenenti a minoranze sessuali, il che significa che una prevenzione inclusiva è un meccanismo centrale per proteggere la salute mentale di questo gruppo. Una politica che non menzioni queste forme specifiche di danno lascia gli studenti più vulnerabili senza una protezione adeguata.	Aggiornare la politica scolastica contro il cyberbullismo in modo da includere esplicitamente le molestie online basate sul genere, le molestie sessuali, la condivisione di immagini intime senza consenso e le molestie basate sull'orientamento sessuale o sull'identità di genere. Assicurarsi che la formazione del personale copra queste specifiche forme di danno e le modalità di risposta alle stesse. Creare un ambiente scolastico in cui ogni studente si senta ugualmente al sicuro nel segnalare ciò che gli sta accadendo.
Rendere accessibile l'educazione alla	Gli studenti con disabilità, comprese le difficoltà di apprendimento, possono essere più	Assicuratevi che tutta l'educazione alla sicurezza digitale sia erogata in modi adeguati agli studenti con diverse

Cosa	Perché è importante	Come procedere
sicurezza digitale agli studenti con disabilità	vulnerabili alla manipolazione e allo sfruttamento online. Potrebbero inoltre avere maggiori difficoltà ad accedere a un'educazione alla sicurezza digitale che non sia progettata tenendo conto delle loro esigenze. Se i meccanismi di segnalazione non sono accessibili a loro, di fatto non esistono.	esigenze di apprendimento. Verificate che le piattaforme digitali utilizzate a scuola rispettino gli standard di accessibilità. Assicuratevi che i meccanismi di segnalazione siano accessibili agli studenti che comunicano in modo diverso. Collaborate con il personale specializzato in bisogni educativi speciali per identificare gli studenti che potrebbero aver bisogno di ulteriore supporto nella comprensione e nella gestione dei rischi online.
Riconoscere e affrontare il divario digitale	Gli studenti provenienti da famiglie a basso reddito potrebbero avere un accesso a Internet limitato o inaffidabile a casa, dispositivi obsoleti o condivisi e un minore sostegno da parte degli adulti nella navigazione nel mondo online. Gli studenti che utilizzano dispositivi condivisi sono esposti a maggiori rischi per la privacy. Questi studenti potrebbero inoltre essere meno propensi a riconoscere o segnalare eventuali problemi.	Non progettare attività digitali o pratiche di comunicazione che presuppongano un livello di connettività domestica di cui non tutti gli studenti dispongono. Si tenga presente che gli studenti che utilizzano dispositivi condivisi sono esposti a particolari rischi per la privacy e forni loro indicazioni specifiche. Assicurarsi che l'educazione alla sicurezza digitale raggiunga tutti gli studenti. Identificare gli studenti che non dispongono di un'adeguata connettività domestica e affrontare la questione attraverso i programmi nazionali disponibili.
Aiutate gli studenti a sviluppare una consapevolezza critica dell'immagine corporea online	I social media espongono costantemente gli studenti a immagini modificate e filtrate che definiscono standard di aspetto non realistici. Ciò è associato a una minore autostima e ad ansia, in particolare nelle ragazze adolescenti, e in alcuni casi a disturbi alimentari.	Includete l'educazione sull'immagine corporea e sull'aspetto online come parte del programma didattico sul benessere digitale. Spiegate agli studenti come le immagini vengono modificate e filtrate prima di essere pubblicate e aiutateli a comprendere che ciò che vedono online è una rappresentazione piuttosto che la realtà. Discutete di come gli algoritmi delle piattaforme amplifichino i contenuti basati sull'aspetto fisico. Affrontate questo argomento con sensibilità. Alcuni studenti potrebbero già trovarsi in difficoltà. Assicuratevi che siano disponibili percorsi di riferimento verso un supporto specialistico.
Adottare una prospettiva inclusiva in tutta questa politica	Una politica elaborata senza tenere conto delle esperienze dei diversi gruppi di studenti rifletterà l'esperienza della maggioranza e	Esaminate ogni sezione di questa politica e chiedetevi: questo raggiunge gli studenti più a rischio? I nostri canali di segnalazione sono accessibili a tutti? La

Cosa	Perché è importante	Come procedere
	lascerà gli altri meno protetti. Gli studenti che affrontano i rischi online maggiori sono spesso quelli le cui esperienze sono state meno prese in considerazione.	formazione del nostro personale copre le vulnerabilità specifiche dei diversi gruppi? Coinvolgete gli studenti, compresi quelli appartenenti a gruppi sottorappresentati, nella revisione e nel miglioramento dell'approccio della scuola alla sicurezza digitale.

Parte 4: Cosa dimostrano i dati

Questa parte riassume ciò che la ricerca ci dice su ciò che funziona realmente quando le scuole affrontano i temi della sicurezza informatica, del cyberbullismo e del benessere digitale. Utilizzate questa sezione per compiere scelte informate sui programmi, gli approcci e gli interventi adottati dalla vostra scuola.

4.1 Sensibilizzazione e formazione sulla sicurezza informatica

La ricerca sulla sicurezza informatica nelle scuole identifica costantemente il comportamento umano come il fattore di rischio più importante. La maggior parte degli attacchi riusciti ha inizio con un'e-mail di phishing o una password debole. Le difese tecniche aiutano, ma non possono impedire un attacco quando il personale non è formato a riconoscere la minaccia. Ciò significa che investire nella formazione del personale è importante almeno quanto investire negli strumenti tecnici.

Gli studi sulla formazione del personale in materia di sicurezza informatica dimostrano che una formazione regolare e pratica funziona significativamente meglio di una singola sessione di sensibilizzazione. Il personale che riceve una formazione annuale e promemoria occasionali è sensibilmente meno propenso a cliccare su link di phishing o ad adottare pratiche non sicure con i sistemi scolastici. Anche il modo in cui viene erogata la formazione è importante: le sessioni interattive con esempi tratti dal mondo reale funzionano meglio della lettura passiva di informazioni o della visione di un video.

Le esercitazioni simulate di phishing, in cui il personale riceve un'e-mail di phishing fasulla accuratamente progettata per testare la propria reazione, sono tra i metodi di formazione più efficaci disponibili. Le scuole e le organizzazioni che conducono regolarmente queste esercitazioni registrano nel tempo chiari miglioramenti nel comportamento del personale. L'esercitazione è più efficace quando è seguita immediatamente da un feedback che spiega quali fossero i segnali di allarme e quale sarebbe stata la risposta corretta.

Per gli studenti, i dati dimostrano che l'educazione alla sicurezza informatica funziona meglio quando è integrata nel programma scolastico piuttosto che erogata come evento a sé stante. Gli studenti che apprendono la sicurezza online attraverso esempi reali, attività interattive e discussioni con i propri coetanei assimilano meglio le lezioni e le applicano in modo più coerente nella propria vita rispetto agli studenti che ricevono le stesse informazioni durante una lezione frontale.

4.2 Prevenzione del cyberbullismo

La ricerca sulla prevenzione del cyberbullismo dimostra costantemente che gli approcci che coinvolgono l'intera scuola funzionano meglio. Ciò significa programmi che riuniscono studenti, insegnanti, genitori e

dirigenti scolastici attorno a un obiettivo condiviso: creare un ambiente più sicuro. Le scuole che trattano il cyberbullismo esclusivamente come una questione disciplinare, da affrontare solo dopo che gli episodi si sono verificati, ottengono sistematicamente risultati peggiori rispetto alle scuole che adottano un approccio preventivo che coinvolge l'intera comunità.

I programmi che si concentrano esclusivamente sul comportamento di chi compie atti di bullismo sono meno efficaci di quelli che sviluppano anche l'empatia e le capacità di intervento dei testimoni. Gli studenti che comprendono il danno causato dal cyberbullismo e a cui è stato insegnato come sostenere un coetaneo vittima di bullismo sono più propensi a segnalare gli episodi e a intervenire per aiutare. Il fatto che i testimoni intervengano o restino in silenzio è uno dei fattori predittivi più significativi dell'escalation o dell'arresto del bullismo.

I sistemi di segnalazione anonima portano costantemente a un aumento del numero di episodi segnalati. Gli studenti vittime di cyberbullismo spesso non ne parlano con nessuno perché temono di non essere creduti, che la situazione peggiori o che ci siano ripercussioni sociali tra i loro coetanei. Le scuole che offrono un canale di segnalazione realmente riservato e affidabile registrano tassi più elevati di segnalazione e un intervento più tempestivo.

La formazione degli insegnanti è essenziale e spesso sottovalutata. Le ricerche dimostrano che molti insegnanti si sentono incerti su come reagire al cyberbullismo, in particolare quando questo coinvolge app o funzionalità che non conoscono bene. Le scuole che investono in una formazione pratica e strutturata degli insegnanti sul riconoscimento e la gestione del cyberbullismo ottengono costantemente risultati migliori per gli studenti.

Anche il coinvolgimento dei genitori fa una differenza significativa. I genitori che comprendono il cyberbullismo, che conoscono il funzionamento delle piattaforme utilizzate dai propri figli e che si sentono in sintonia con l'approccio della scuola sono più efficaci sia nel sostenere i propri figli sia nel rafforzare i messaggi della scuola a casa.

La ricerca fornisce prove evidenti della portata del problema. Secondo lo studio dell'OMS «Health Behaviour in School-aged Children» (2024), circa un adolescente su sei in Europa, pari a circa il 15%, riferisce di aver subito cyberbullismo, con percentuali sostanzialmente simili tra ragazzi e ragazze e una tendenza al rialzo rispetto al 2018. I dati dell'OCSE hanno rilevato variazioni tra i paesi che vanno dal 7,5% circa al 27,1%. I dati delle linee di assistenza della rete Insafe dell'UE collocano costantemente il cyberbullismo tra i motivi più comuni per cui bambini e adolescenti contattano i servizi di supporto e, nel quarto trimestre del 2025, è stato nuovamente il problema più frequente segnalato.

Intervistati dalla Commissione europea nel 2025, oltre 6.000 bambini e adolescenti di età compresa tra i 12 e i 17 anni in tutta l'UE hanno espresso chiare aspettative nei confronti delle scuole: la maggioranza desiderava regole esplicite e conseguenze per il cyberbullismo, un insegnamento diretto sull'argomento e un sostegno psicologico per le persone colpite. Le ragazze erano costantemente più propense dei ragazzi a richiedere queste misure.

Una meta-analisi condotta da Polanin et al. (2021), che ha coinvolto oltre 45.000 studenti, ha rilevato che i programmi dedicati alla prevenzione del cyberbullismo hanno prodotto una riduzione statisticamente significativa sia dei casi di bullismo che di vittimizzazione, e che i programmi progettati specificamente per il cyberbullismo hanno dato risultati migliori rispetto agli approcci generali contro il bullismo.

4.3 Benessere digitale

La ricerca sull'uso della tecnologia e sulla salute mentale degli studenti non permette di trarre conclusioni semplicistiche. Non tutto l'uso della tecnologia è dannoso. Utilizzare la tecnologia in modo attivo per il lavoro creativo, la comunicazione o l'apprendimento può avere effetti positivi. Il problema ricorrente è l'uso passivo: scorrere i social media senza uno scopo preciso o un'interazione significativa. Questo tipo di utilizzo è fortemente associato ad ansia, solitudine e bassa autostima, con effetti particolarmente marcati nelle ragazze adolescenti.

Le evidenze sostengono con forza l'educazione rispetto alla restrizione. Le scuole che si concentrano esclusivamente sulla limitazione dell'accesso alla tecnologia, senza aiutare gli studenti a comprendere perché determinati modelli di utilizzo siano dannosi né fornendo loro gli strumenti per gestire il proprio comportamento, registrano cambiamenti meno duraturi. Gli studenti che comprendono il problema e hanno sviluppato le proprie strategie mostrano miglioramenti più duraturi nel benessere.

I programmi che insegnano agli studenti a riflettere in modo critico sulle proprie abitudini digitali, a comprendere come le piattaforme dei social media siano progettate per massimizzare il coinvolgimento e a riconoscere il divario tra le immagini online curate e la realtà hanno dimostrato, in numerosi studi, risultati positivi nella riduzione dell'ansia e nel miglioramento dell'autostima. Questi programmi funzionano meglio quando vengono erogati nel corso del tempo come parte del programma scolastico, piuttosto che come evento isolato.

Coinvolgere gli studenti nella creazione delle regole digitali della scuola aumenta costantemente sia il loro grado di rispetto delle regole sia il loro senso di appartenenza nei confronti delle stesse. Gli studenti che ritengono che le regole siano eque e che abbiano avuto voce in capitolo nella loro definizione sono più propensi a seguirle e a incoraggiare i propri coetanei a fare lo stesso.

Un risultato particolarmente importante riguarda la «paura di perdersi qualcosa» (Fear of Missing Out, FOMO). La ricerca concettualizza sempre più spesso la FOMO non come uno stato d'animo passeggero, ma come una caratteristica psicologica relativamente stabile, un'ansia persistente di perdersi esperienze gratificanti che gli altri stanno vivendo. Gli studi associano la FOMO a sintomi depressivi, disturbi del sonno e comportamenti compulsivi di controllo. Una revisione sistematica e una meta-analisi del 2025 hanno confermato un'associazione statistica consistente tra la dipendenza dai social media e livelli più elevati di ansia, depressione, solitudine e bassa autostima, con la FOMO spesso identificata come fattore mediatore. Le scuole dovrebbero affrontare esplicitamente la FOMO e i modelli di utilizzo compulsivo nelle attività rivolte agli studenti, non solo attraverso messaggi generici sul tempo trascorso davanti allo schermo.

La ricerca rileva inoltre che gli esiti dipendono in larga misura non solo da quanto gli studenti utilizzano le piattaforme digitali, ma anche da come le utilizzano. I social media possono fungere da fonte di sostegno per alcuni studenti, in particolare per quelli che sono isolati o appartengono a gruppi minoritari. Gli approcci preventivi dovrebbero aiutare gli studenti a sviluppare un rapporto più consapevole e intenzionale con la tecnologia.

L'individuazione precoce e l'indirizzamento sono fondamentali. Gli studenti che vengono indirizzati verso il giusto sostegno prima che le loro difficoltà diventino gravi mostrano risultati significativamente migliori rispetto a quelli che vengono individuati solo quando i problemi sono già evidenti attraverso il calo dei voti o gravi cambiamenti comportamentali. Le scuole che dispongono di percorsi chiari e ben noti per individuare e sostenere gli studenti in difficoltà sono in una posizione molto migliore per aiutarli.

Appendice I: Tabella di riferimento nazionale

Utilizzate questa tabella per individuare i principali parametri nazionali relativi al vostro Paese. Laddove la presente politica richieda di verificare le norme nazionali, è qui che dovrete consultare.

Parametro	Grecia	Italia	Portogallo	Romania	Slovacchia
Età del consenso digitale	15 anni	14 anni	13 anni	16 anni	16 anni
Autorità per la protezione dei dati	HDPA dpa.gr	Garante garanteprivacy.it	CNPD cnpd.pt	ANSPDCP dataprotection.ro	UOOU dataprotection.gov.sk
Autorità per la sicurezza informatica	EAKE cyber.gov.gr	ACN acn.gov.it	CNCS cncs.gov.pt	DNSC dnsc.ro	NBU nbu.gov.sk
Segnalazione di incidenti informatici	EAKE	ACN	CERT.PT (24 ore su 24 per NIS2)	DNSC/PNRISC (24 ore)	NBU/SK-CERT
Segnalazione di violazioni dei dati	HDPA, 72 ore	Garante, 72 ore	CNPD, 72 ore	ANSPDCP, 72 ore	UOOU, 72 ore
Risorse sul cyberbullismo	stop-bullying.gov.gr	Segnalare alla scuola o alla polizia	seguranet.pt	Scuola o ANSPDCP	Linee guida 1/2025
Legge sui telefoni cellulari	Divieto assoluto 2018/2024	Tutti i cicli 2024/25	Anni 1-6 a partire da settembre 2025	Durante le lezioni, Legge 198/2023	Tutte le classi a partire da gennaio 2025
Linee guida sull'IA per le scuole	Solo legge UE sull'IA	Decreto Ministeriale n. 166/2025	Non ancora emanato	Non ancora emanato	Piano sull'IA 2025-2027

Appendice II: Modello di lettera ai genitori

Le scuole possono adattare questa lettera per informare i genitori su come la scuola gestisce i dati degli studenti e sulle misure adottate per garantire la sicurezza degli studenti online. Inviarla al momento dell'iscrizione e ogni volta che vengono apportate modifiche significative ai sistemi digitali o alle politiche della scuola.

[Nome e indirizzo della scuola]

[Data]

Gentile genitore/tutore,

Come proteggiamo i dati di vostro figlio e ne garantiamo la sicurezza digitale

Vi scriviamo per illustrarvi come la nostra scuola gestisce i dati personali degli studenti e quali misure adottiamo per garantire la sicurezza di vostro figlio nel suo ambiente di apprendimento digitale.

Quali dati raccogliamo e perché. Raccogliamo le informazioni personali relative a vostro figlio necessarie ai fini didattici e amministrativi. Queste includono il nome, il numero di identificazione, i registri delle presenze e i voti. In alcuni casi potremmo anche conservare informazioni relative alla salute, qualora fossero rilevanti per la sua istruzione. Raccogliamo solo ciò di cui abbiamo bisogno e conserviamo i dati per il periodo previsto dalla legge.

Chi può accedervi. L'accesso ai dati personali di vostro figlio è limitato ai membri del personale autorizzati che ne hanno bisogno per svolgere il proprio lavoro. Non condividiamo i dati con soggetti esterni a meno che non sia richiesto dalla legge o non abbiate fornito il vostro consenso esplicito.

Piattaforme digitali. La nostra scuola utilizza piattaforme digitali per l'insegnamento e l'amministrazione. Prima di adottare qualsiasi piattaforma, verifichiamo che sia conforme al GDPR. Vostro figlio accederà a queste piattaforme tramite un account fornito dalla scuola. Un elenco delle piattaforme che utilizziamo attualmente è disponibile presso la segreteria della scuola.

Il vostro consenso. Per gli studenti di età inferiore a [inserire l'età nazionale di consenso all'uso dei dati personali], abbiamo bisogno del consenso scritto dei genitori prima di poter iscrivere vostro figlio a una piattaforma digitale. Vi verrà chiesto di fornirlo al momento dell'iscrizione e ogni volta che verrà introdotta una nuova piattaforma.

Cyberbullismo. La nostra scuola dispone di procedure chiare per prevenire e contrastare il cyberbullismo. Se vostro figlio subisce o assiste a episodi di cyberbullismo, vi preghiamo di incoraggiarlo a parlarne con un adulto di fiducia a scuola o a contattarci direttamente all'indirizzo [recapiti].

I vostri diritti. Avete il diritto di visionare i dati in nostro possesso relativi a vostro figlio, di richiederne la correzione e, in alcune circostanze, di chiederne la cancellazione. A tal fine, vi preghiamo di contattare il nostro Responsabile della protezione dei dati all'indirizzo [recapiti del DPO].

Promuovere il benessere digitale a casa. Vi incoraggiamo a parlare regolarmente con vostro figlio delle sue esperienze online, senza giudicarlo. Se vostro figlio sembra turbato o insolitamente ansioso riguardo al proprio telefono o alle interazioni online, vi preghiamo di contattare [consulente scolastico / referente designato]. Nel vostro Paese sono disponibili anche linee di assistenza nazionali per bambini e giovani.

Se avete domande, non esitate a contattarci.

Cordiali saluti,

[Nome del Preside e scuola]

Appendice III: Modello di Politica di Utilizzo Accettabile

Adattate questo modello per creare la politica di utilizzo accettabile della vostra scuola. Dovrà essere firmata dagli studenti, dai genitori o dai tutori e dal personale all'inizio di ogni anno scolastico. Adattatela in modo che rifletta i sistemi della vostra scuola, le norme nazionali e il contesto.

Politica di utilizzo accettabile

[Nome della scuola] | Anno scolastico [XXXX-XXXX]

1. Finalità

La presente politica definisce le regole per l'utilizzo dei dispositivi digitali, di Internet e delle piattaforme digitali nella nostra scuola. Si applica a tutti gli studenti, al personale e ai visitatori che utilizzano i sistemi scolastici. Firmando la presente politica, confermi di aver letto e compreso queste regole e di accettare di rispettarle.

2. Per quali scopi è possibile utilizzare le risorse digitali della scuola

- Svolgere i compiti scolastici e le attività didattiche
- Comunicare con insegnanti e compagni di classe per motivi scolastici
- Utilizzo delle piattaforme approvate dalla scuola
- Attività didattiche specificatamente autorizzate da un insegnante

3. Cosa non devi fare

- Accedere, creare o condividere contenuti illegali, dannosi, offensivi o discriminatori
- Molestare, minacciare o umiliare altri studenti o il personale tramite mezzi digitali
- Condividere informazioni personali su altri studenti o membri del personale senza il loro consenso
- Registrare video o audio di studenti, insegnanti o membri del personale senza il loro esplicito consenso
- Utilizzare l'account di un'altra persona o condividere le proprie credenziali di accesso
- Installare software o applicazioni sui dispositivi della scuola senza autorizzazione
- Utilizzare account personali su piattaforme non approvate per attività scolastiche

4. Telefoni cellulari

[Descrivere qui le regole della propria scuola relative ai telefoni cellulari, in linea con la legislazione nazionale del proprio paese come descritto nella Parte 2 della presente politica. Specificare dove devono essere riposti i telefoni, quali eccezioni si applicano e cosa succede in caso di violazione delle regole.]

5. Social media

Gli studenti non devono pubblicare contenuti relativi alla scuola, ad altri studenti o al personale che siano dannosi, fuorvianti o che possano danneggiare la reputazione di qualcuno. I comportamenti online che costituiscono cyberbullismo, sia durante che al di fuori dell'orario scolastico, sono disciplinati dalla presente politica e dalle procedure anti-bullismo della scuola.

6. Segnalazioni

Se vi imbattete in contenuti che fanno sentire voi o un altro studente in pericolo, o se notate una violazione del presente regolamento, segnalatelo a un adulto di fiducia a scuola o a [referente per le segnalazioni].

7. Conseguenze

La violazione della presente politica può comportare la sospensione dell'accesso ai sistemi scolastici, altre misure disciplinari previste dal regolamento scolastico e, nei casi più gravi, la segnalazione alle forze dell'ordine.

Nome e cognome dello studente	
Firma dello studente	
Nome del genitore o tutore	
Firma del genitore o tutore	
Data	

Appendice IV: Procedura di risposta agli incidenti informatici

Seguire questi passaggi ogni volta che si verifica un incidente informatico nella propria scuola. Per incidente informatico si intende qualsiasi evento che comprometta la sicurezza, la disponibilità o la riservatezza dei dati o dei sistemi scolastici. Ciò include un attacco ransomware, l'accesso non autorizzato ai sistemi scolastici o una violazione dei dati personali.

Fase 1: Identificazione e contenimento

Non appena qualcuno rileva un incidente, deve informare immediatamente il coordinatore IT della scuola o il preside. Non cercare di risolvere il problema da solo. Scollega il dispositivo interessato dalla rete staccando il cavo o disattivando il Wi-Fi. Non spegnere il dispositivo a meno che non ti venga espressamente richiesto di farlo, poiché ciò potrebbe distruggere le prove. Annota l'ora e una descrizione di ciò che hai osservato.

Fase 2: Valutare

Il coordinatore IT e il responsabile della protezione dei dati (DPO) devono valutare l'incidente insieme. Individuare quali sistemi, account o dati sono stati interessati. Determinare se i dati personali sono stati o potrebbero essere stati compromessi. Verificare se l'incidente è ancora in corso o è stato contenuto.

Fase 3: Notifica

Se si è verificata questa situazione...	Dovreste...
I dati personali sono stati o potrebbero essere stati compromessi	Notificarlo all'autorità nazionale per la protezione dei dati entro 72 ore. Consultare la Parte 2 per conoscere l'autorità competente nel proprio paese.
Si è verificato un incidente di sicurezza informatica di rilievo	Segnalare l'accaduto all'autorità nazionale per la sicurezza informatica. In Portogallo, per i soggetti soggetti alla normativa NIS2, ciò deve avvenire entro 24 ore. Consultare la Parte 2 per conoscere l'autorità competente nel proprio paese.
È coinvolta un'attività criminale	Contattare la polizia.
Gli studenti o il personale sono esposti a un rischio immediato o hanno subito un danno diretto	Fornire immediatamente assistenza e informare i genitori o i tutori, a seconda dei casi.

Fase 4: Ripristino

Ripristinare i sistemi dai backup, se disponibili. Reimpostare immediatamente tutte le password e le credenziali di accesso interessate. Applicare eventuali aggiornamenti di sicurezza rilevanti prima di rimettere in funzione i sistemi. Verificare che i sistemi ripristinati funzionino correttamente prima di renderli nuovamente disponibili a studenti e personale.

Fase 4a: Supportare le persone coinvolte

Fornire immediatamente supporto psicologico e pratico a qualsiasi studente o membro del personale direttamente coinvolto nell'incidente. Ciò dovrebbe avvenire parallelamente alla risposta tecnica, non dopo di essa. Contattare senza indugio il consulente scolastico o il team di assistenza pastorale. Seguire il protocollo di benessere della scuola.

Fase 5: Analisi

Una volta risolto l'incidente, effettuare una revisione completa. Annotare cosa è successo, come si è verificato, cosa è stato fatto e qual è stato il risultato. Individuare quali cambiamenti potrebbero ridurre il rischio che si ripeta. Informare il personale interessato dei risultati, specialmente se l'incidente ha coinvolto un'e-mail di phishing o un errore umano. Aggiornare la procedura di risposta agli incidenti, se necessario.

Registro degli incidenti

Data e ora dell'incidente	
Come è stato scoperto e da chi?	
Cosa è successo?	
Quali sistemi e dati sono stati interessati?	
Misure immediate adottate	
I dati personali sono stati compromessi?	
È stata informata l'autorità garante della protezione dei dati? (Data)	
È stata informata l'autorità per la sicurezza informatica? (Data)	
È stata contattata la polizia? (Data)	
Misure di ripristino adottate	
Data di ripristino dei sistemi	
Revisione completata? (Data)	
Modifiche apportate a seguito della revisione	

Appendice V: Modello di valutazione d'impatto sulla protezione dei dati (DPIA)

È necessario effettuare una DPIA prima che la vostra scuola introduca un nuovo sistema o una nuova piattaforma digitale che comporti il trattamento di grandi quantità di dati degli studenti, il monitoraggio sistematico degli studenti, processi decisionali automatizzati che incidono sugli studenti o categorie di dati sensibili. Se non siete sicuri della necessità di una DPIA, rivolgetevi al vostro responsabile della protezione dei dati (DPO).

Parte A: Cosa verrà trattato

Nome del sistema o della piattaforma	
Fornitore o venditore	
Quali dati personali saranno trattati?	
Chi sono gli interessati? (studenti, personale, genitori)	
Qual è la finalità del trattamento?	
Qual è la base giuridica del trattamento?	
Dove saranno conservati i dati? (paese, all'interno del SEE?)	
Chi avrà accesso ai dati?	
Per quanto tempo saranno conservati i dati?	
I dati saranno condivisi con terze parti?	

Parte B: Valutazione dei rischi

Rischio	(Basso / Medio / Alto) e modalità di gestione
Accesso non autorizzato ai dati degli studenti	
Perdita o cancellazione accidentale dei dati	
Dati utilizzati per scopi diversi da quelli originari	

Rischio	(Basso / Medio / Alto) e modalità di gestione
Monitoraggio o profilazione degli studenti senza trasparenza	
Trasferimento di dati al di fuori del SEE senza garanzie	
Conservazione dei dati per un periodo più lungo del necessario	

Parte C: Decisione

Livello di rischio complessivo (Basso / Medio / Alto)	
Il trattamento può procedere? (Sì / Sì con misure di mitigazione / No)	
Cosa occorre fare prima di poter avviare il trattamento?	
È stato consultato il responsabile della protezione dei dati? (Sì / No / Data)	
Valutazione completata da	
Data della valutazione	
Data della prossima revisione	

Appendice VI: Registro dei rischi della scuola

Il Registro dei rischi scolastici aiuta la vostra scuola a identificare, valutare e gestire i principali rischi in materia di sicurezza informatica e protezione dei dati a cui è esposta. La compilazione di questo registro costituisce un passo concreto nell'attuazione dell'approccio alla gestione dei rischi descritto nella Parte 3 della presente politica.

Gli esempi riportati nella tabella sottostante sono indicativi. Sono forniti per aiutare la vostra scuola a muovere i primi passi e per illustrare il tipo di rischi più comuni in un ambiente scolastico. La vostra scuola dovrebbe aggiungere, rimuovere o adattare le voci per riflettere le proprie circostanze, i propri sistemi e il proprio contesto specifici. Il registro dovrebbe essere rivisto almeno una volta all'anno e aggiornato ogni volta che si verifica un cambiamento significativo, come l'introduzione di una nuova piattaforma digitale o un incidente di sicurezza informatica.

Come valutare i rischi

Per ciascun rischio, assegnare un punteggio alla Probabilità e all'Impatto su una scala da 1 a 5 (1 = molto basso, 5 = molto alto). Moltiplicare i due punteggi per ottenere il Punteggio di rischio.

Rischio elevato (15-25): deve essere affrontato immediatamente.

Rischio medio-alto (8-14): deve essere affrontato, dando priorità a quelli con impatto elevato.

Rischio medio-basso (4-7): va affrontato se l'impatto è significativo.

Rischio basso (1-3): accettabile, monitorare regolarmente.

Nella pagina seguente (in formato orizzontale) è riportata una tabella indicativa del Registro dei rischi.

ID	Rischio	Cosa potrebbe accadere	Come ridurlo	Probabilità (1-5)	Impatto (1-5)	Punteggio di rischio	Responsabile	Se dovesse verificarsi
1	E-mail di phishing rivolta al personale	Il personale clicca su un link dannoso, consentendo a un malintenzionato di accedere ai sistemi scolastici e ai dati degli studenti	Formazione annuale del personale, esercitazioni simulate di phishing, autenticazione a più fattori su tutti gli account	4	4	16	Preside / Coordinatore IT	Isolare il dispositivo interessato, informare l'autorità nazionale per la sicurezza informatica, ripristinare dai backup
2	Attacco ransomware	I sistemi scolastici vengono bloccati, i dati degli studenti e i voti diventano inaccessibili	Backup regolari e testati archiviati offline, software antivirus aggiornato, formazione del personale	3	5	15	Coordinatore IT	Ripristino dal backup, segnalazione all'autorità nazionale per la sicurezza informatica, notifica all'autorità garante della protezione dei dati qualora siano interessati i dati degli studenti
3	Dati degli studenti inviati per errore alla	I dati personali di uno studente vengono accidentalmente	Formazione del personale sulla gestione dei dati, utilizzo esclusivo dei	4	3	12	DPO	Contattare il destinatario e richiedere la cancellazione;

ID	Rischio	Cosa potrebbe accadere	Come ridurlo	Probabilità (1-5)	Impatto (1-5)	Punteggio di rischio	Responsabile	Se dovesse verificarsi
	persona sbagliata	condivisi con una persona non autorizzata	canali di comunicazione ufficiali della scuola					segnalare l'incidente all'autorità nazionale per la protezione dei dati entro 72 ore, se richiesto; documentare l'incidente
4	Cyberbullismo tramite la piattaforma scolastica	Uno studente utilizza uno strumento di comunicazione scolastico per molestare un altro studente	Politica di utilizzo accettabile firmata da tutti gli studenti e dai genitori, formazione sul cyberbullismo, procedure chiare per la segnalazione	4	3	12	Preside / Insegnante di classe	Seguire la procedura scolastica contro il bullismo, sostenere lo studente coinvolto, coinvolgere i genitori, documentare l'incidente

Appendice VII: Registro di mappatura dei dati

Il Registro di mappatura dei dati aiuta la vostra scuola a registrare tutti i dati personali che tratta. La tenuta di questo registro è un obbligo di legge ai sensi dell'articolo 30 del GDPR. Deve essere messo a disposizione dell'autorità nazionale per la protezione dei dati su richiesta.

Gli esempi riportati di seguito coprono le categorie più comuni di dati personali trattati dalle scuole. Sono indicativi: la vostra scuola dovrebbe aggiungere eventuali categorie aggiuntive applicabili alla propria situazione ed eliminare quelle non pertinenti. Esaminate e aggiornate il registro almeno una volta all'anno e ogni volta che viene introdotto un nuovo sistema o una nuova piattaforma.

Che cos'è una base giuridica?

Ogni volta che la vostra scuola tratta dati personali, deve avere un motivo legittimo. I motivi più comuni per le scuole sono:

Obbligo di legge: trattamento richiesto dalla normativa nazionale in materia di istruzione (ad esempio, la tenuta dei registri delle presenze).

Funzione pubblica: trattamento necessario affinché la scuola possa svolgere le proprie funzioni pubbliche.

Consenso: la persona ha acconsentito al trattamento (richiesto per le foto e le piattaforme non essenziali).

Nella pagina seguente (in formato orizzontale) è riportata una tabella indicativa del Registro di mappatura dei dati.

Tipo di dati	Motivo del trattamento	Base giuridica	Dove vengono conservati	Chi vi ha accesso	Per quanto tempo li conserviamo	Viene eseguito il backup?	Con chi vengono condivisi
Dati personali degli studenti (nome, codice identificativo, indirizzo, data di nascita)	Necessari per l'amministrazione scolastica e il rispetto della normativa nazionale in materia di istruzione	Obbligo di legge	Sistema informativo scolastico nazionale (ad es. MySchool, SIIIR, Unica)	Solo il preside e il personale amministrativo	Come previsto dalla normativa nazionale	Sì	Ministero dell'Istruzione tramite piattaforma nazionale
Documenti scolastici degli studenti (voti, frequenza, valutazioni)	Necessari per monitorare i progressi degli studenti e riferire ai genitori	Obbligo di legge / Funzione pubblica	Sistema informativo scolastico e registro delle valutazioni degli insegnanti	Insegnanti di classe, preside, personale amministrativo	Come previsto dalla normativa nazionale	Sì	Genitori (tramite canale sicuro), Ministero dell'Istruzione
Informazioni sulla salute degli studenti (allergie, disabilità, esigenze mediche)	Necessario per tutelare la salute e la sicurezza degli studenti durante l'orario scolastico	Obbligo di legge / Interessi vitali	Archivio cartaceo protetto o registro digitale crittografato	Solo il preside, l'infermiera scolastica e gli insegnanti interessati	Durata dell'iscrizione più quanto previsto dalla legge	Sì (crittografati)	Operatori sanitari solo se necessario
Foto e immagini degli studenti	Tesserino scolastico, pubblicazioni, documentazione relativa agli eventi	Consenso dei genitori	Server scolastico o piattaforma approvata	Personale amministrativo, docenti autorizzati	Durata dell'iscrizione; cancellazione su richiesta	Sì	Nessuna condivisione con terzi senza

Tipo di dati	Motivo del trattamento	Base giuridica	Dove vengono conservati	Chi vi ha accesso	Per quanto tempo li conserviamo	Viene eseguito il backup?	Con chi vengono condivisi
							ulteriore consenso

Appendice VIII: Registro delle politiche e delle procedure scolastiche

Questo registro aiuta la vostra scuola a tenere traccia delle principali politiche di sicurezza e protezione dei dati in vigore. Disporre di politiche documentate in ciascuna di queste aree è un segnale importante del fatto che la scuola sta gestendo le proprie responsabilità in materia di sicurezza informatica e protezione dei dati in modo strutturato.

Le politiche elencate di seguito sono quelle più rilevanti per le raccomandazioni contenute nella presente Politica di resilienza informatica. L'elenco è indicativo: la vostra scuola potrebbe disporre di ulteriori politiche che dovrebbero essere registrate in questa sede. Per ciascuna politica, indicate chi ne è responsabile, quando è stata aggiornata l'ultima volta e quando è prevista la prossima revisione. Qualora una politica non esista ancora, registratela come azione prioritaria.

Modelli disponibili

Le appendici della presente politica contengono modelli per diverse delle politiche elencate di seguito:

- Politica sull'uso accettabile: Appendice III.
- Procedura di risposta agli incidenti: Appendice IV.
- Valutazione d'impatto sulla protezione dei dati (DPIA): Appendice V.
- Registro dei rischi: Appendice VI.
- Registro di mappatura dei dati: Appendice VII.
- Autovalutazione della resilienza informatica della scuola: Appendice IX

ID	Nome della politica	Aree chiave trattate	Titolare della politica	Ultimo aggiornamento	Prossima revisione
1	Politica di utilizzo accettabile (AUP)	Utilizzo dei sistemi e dei dispositivi scolastici. Regole relative ai telefoni cellulari. Segnalazioni.	Preside / Coordinatore IT		
2	Politica di controllo degli accessi	Chi può accedere a quali sistemi e dati. Regole relative alle password. Revoca dell'accesso in caso di cessazione del rapporto di lavoro di un membro del personale.	Coordinatore IT / Responsabile della protezione dei dati		

ID	Nome della politica	Aree chiave trattate	Titolare della politica	Ultimo aggiornamento	Prossima revisione
3	Politica sulla protezione dei dati	Conformità al GDPR. Responsabilità del Responsabile della protezione dei dati (DPO). Consenso dei genitori. Informative sulla privacy. Gestione delle violazioni dei dati.	Responsabile della protezione dei dati (DPO) / Direttore		
4	Politica di backup	Cosa viene sottoposto a backup, con quale frequenza, dove viene archiviato e come viene testato il ripristino.	Coordinatore IT		
5	Politica di risposta agli incidenti	Come la scuola risponde agli incidenti di sicurezza informatica e alle violazioni dei dati. Chi ne è responsabile. Come informare le autorità.	Preside / Responsabile della protezione dei dati (DPO) / Coordinatore IT		
6	Politica contro il bullismo (compreso il cyberbullismo)	Definizione di cyberbullismo. Procedura di segnalazione. Come interviene la scuola. Formazione del personale. Coinvolgimento dei genitori.	Preside		
7	Regolamento sui dispositivi mobili	Regole relative all'uso dei telefoni cellulari da parte	Preside		

ID	Nome della politica	Aree chiave trattate	Titolare della politica	Ultimo aggiornamento	Prossima revisione
		degli studenti in linea con la normativa nazionale. Divieto di registrazioni non autorizzate.			

Appendice IX: Autovalutazione della resilienza informatica della scuola

Le scuole possono utilizzare questa checklist per acquisire una comprensione di base della propria attuale resilienza informatica e individuare le lacune prioritarie. Contrassegnare ciascuna voce con Sì, Parzialmente o No. Lo scopo non è quello di superare o fallire la valutazione, ma di individuare su quali aspetti concentrare gli sforzi.

Le scuole sono incoraggiate a ripetere questa autovalutazione almeno una volta all'anno. Il monitoraggio dei punteggi nel tempo aiuta a tenere traccia dei progressi e favorisce una cultura del miglioramento continuo.

Le voci elencate sono indicative. Adattatele in modo che riflettano il contesto specifico della vostra scuola, i requisiti nazionali e le circostanze particolari.

Ambito	Cosa verificare	Sì / Parzialmente / No
Governance	La scuola dispone di un coordinatore designato per la sicurezza informatica o la sicurezza digitale.	
Governance	La scuola dispone di una Politica di Utilizzo Accettabile (AUP) scritta, rivista negli ultimi 2 anni.	
Governance	La scuola dispone di una procedura documentata di risposta agli incidenti, nota al personale.	
Sensibilizzazione e formazione	Il personale riceve una formazione almeno una volta all'anno in materia di sicurezza informatica e sicurezza online.	

Ambito	Cosa verificare	Sì / Parzialmente / No
Sensibilizzazione e formazione	Gli studenti ricevono un'educazione alla cittadinanza digitale e alla sicurezza online adeguata alla loro età.	
Sensibilizzazione e formazione	I genitori e i tutori ricevono informazioni sui rischi digitali almeno una volta per anno scolastico.	
Benessere e prevenzione	La scuola dispone di un protocollo specifico e ben definito per la gestione del cyberbullismo.	
Benessere e prevenzione	Gli studenti sanno come e a chi segnalare in modo riservato gli incidenti online.	
Benessere e prevenzione	Le attività di prevenzione si rivolgono esplicitamente a gruppi diversi e vulnerabili.	
Dati e privacy	La scuola tiene un registro delle piattaforme e degli strumenti che trattano i dati degli studenti.	
Dati e privacy	Il consenso dei genitori viene ottenuto prima di iscrivere gli studenti alle piattaforme digitali, laddove richiesto dalla legge.	
Misure tecniche	I dispositivi e le reti della scuola utilizzano software di protezione aggiornati e controlli di accesso.	
Misure tecniche	Vengono effettuati regolarmente backup dei dati scolastici critici, che vengono sottoposti a test.	

Come interpretare il punteggio

Conta le risposte "Sì" (1 punto) e quelle "In parte" (0,5 punti). Dividi per 13 e moltiplica per 100 per ottenere una percentuale. Incrocia il risultato con i livelli di maturità riportati di seguito.

Livello	Punteggio	Descrizione
1 - Iniziale	Da 0 a 20%	Esistono poche o nessuna governance formale, formazione o procedure per la gestione degli incidenti.
2 - In fase di sviluppo	Dal 21 al 45%	Esistono politiche di base, ma non vengono applicate, riviste o comunicate in modo coerente.

3 - Consolidato	Dal 46 al 70%	Gli elementi fondamentali relativi alla governance, alla formazione e alla risposta agli incidenti sono in atto e noti al personale.
4 - Livello avanzato	Dal 71 al 90%	Le politiche e la formazione, complete e regolarmente riviste, raggiungono il personale, gli studenti e i genitori.
5 - Resiliente	Dal 91 al 100%	La resilienza informatica è integrata nella cultura scolastica grazie a una formazione continua e a misure di prevenzione inclusive.

Questi livelli costituiscono esclusivamente uno strumento di autovalutazione e non rappresentano una certificazione formale né una valutazione di conformità.

Riferimenti

Legislazione dell'Unione europea

I seguenti strumenti giuridici dell'Unione europea costituiscono il quadro giuridico comune su cui si fonda la presente politica. Essi stabiliscono i requisiti principali in materia di protezione dei dati, sicurezza informatica, intelligenza artificiale, servizi digitali, comunicazioni elettroniche e istruzione digitale in tutti gli Stati membri dell'UE.

- Unione europea, Regolamento (UE) 2016/679 (Regolamento generale sulla protezione dei dati – GDPR), Gazzetta ufficiale dell'Unione europea. Disponibile all'indirizzo: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679
- Unione europea, Direttiva (UE) 2022/2555 (Direttiva NIS 2), Gazzetta ufficiale dell'Unione europea. Disponibile all'indirizzo: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022L2555
- Unione europea, Regolamento (UE) 2024/1689 (Legge sull'intelligenza artificiale), Gazzetta ufficiale dell'Unione europea. Disponibile all'indirizzo: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L_202401689
- Unione europea, Regolamento (UE) 2022/2065 (Legge sui servizi digitali), Gazzetta ufficiale dell'Unione europea. Disponibile all'indirizzo: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022R2065
- Unione europea, Direttiva 2002/58/CE (Direttiva sulla privacy elettronica), Gazzetta ufficiale delle Comunità europee. Disponibile all'indirizzo: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32002L0058
- Unione europea, Regolamento (UE) 2019/881 (Legge sulla sicurezza informatica), Gazzetta ufficiale dell'Unione europea. Disponibile all'indirizzo: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019R0881

Strumenti legislativi nazionali

Per la stesura della Parte 2 della presente politica sono stati utilizzati i seguenti strumenti legislativi nazionali e fonti ufficiali. Essi sono elencati per paese in conformità con la prassi standard di riferimento per i progetti finanziati dall'Unione europea.

Grecia

- Repubblica Ellenica (2018). Legge n. 4577/2018 sulla sicurezza delle reti e dei sistemi informativi. Gazzetta Ufficiale A' 199 del 03.12.2018. Disponibile all'indirizzo: https://www.mindigital.gr/wp-content/uploads/2019/09/N.4577_2018.pdf
- Repubblica Ellenica (2019). Legge n. 4624/2019 sulla protezione delle persone fisiche con riguardo al trattamento dei dati personali (attuazione del GDPR). Gazzetta Ufficiale A' 137/29.08.2019. Disponibile all'indirizzo: https://www.dpa.gr/sites/default/files/2020-08/LAW%204624_2019_EN_TRANSLATED%20BY%20THE%20HDPA.PDF
- Repubblica Ellenica (2020). Legge n. 4727/2020 sulla governance digitale e le comunicazioni elettroniche. Gazzetta Ufficiale A' 184/23.09.2020. Disponibile all'indirizzo: https://adae.gov.gr/images/nomothetiko-plaisio/Nomos_4727_2020_01.pdf
- Repubblica Ellenica (2022). Legge n. 4961/2022 sulle tecnologie emergenti e la governance digitale. Gazzetta Ufficiale A' 146/27.07.2022. Disponibile all'indirizzo: https://www.mindigital.gr/wp-content/uploads/2024/02/N-4961.pdf

- Repubblica Ellenica (2023). Legge n. 5029/2023 sulla prevenzione e la gestione della violenza scolastica e del cyberbullismo. Gazzetta Ufficiale A' n. 55 del 10.03.2023. Disponibile all'indirizzo: https://www.iep.edu.gr/wp-content/uploads/2025/01/2024-08-02_N_5029-2023.pdf
- Repubblica Ellenica (2024). Legge n. 5160/2024 sulla sicurezza informatica (recepimento della direttiva NIS2). Gazzetta Ufficiale A' 195/27.11.2024. Disponibile all'indirizzo: https://search.et.gr/el/fek/?fekId=774154
- Ministero della Governance Digitale, Repubblica Ellenica (2025). Decisione ministeriale n. 1689/2025 sui requisiti di sicurezza informatica per gli enti del settore pubblico. Gazzetta Ufficiale B' n. 2186 del 06.05.2025. Disponibile all'indirizzo: https://cyber.gov.gr/wp-content/uploads/2025/05/20250202186.pdf
- Ministero della Governance Digitale, Repubblica Ellenica (2025). Decisione ministeriale n. 1899/2025 sulla governance della sicurezza delle informazioni per gli enti pubblici. Gazzetta Ufficiale B' n. 4250 del 05.08.2025. Disponibile all'indirizzo: https://cyber.gov.gr/wp-content/uploads/2025/03/KYA_APOFASI_10-Feb-2025_FEK-463_DEFTERO-TEFHOS.pdf

Italia

- Repubblica Italiana (2003). Decreto legislativo n. 196/2003 — Codice in materia di protezione dei dati personali, modificato dal decreto legislativo n. 101/2018. Disponibile all'indirizzo: https://www.garanteprivacy.it/documents/10160/0/Codice+in+materia+di+protezione+dei+dati+personali.pdf
- Repubblica Italiana (2021). Legge n. 109/2021 che converte il decreto-legge n. 82/2021 — Istituzione dell'Agenzia nazionale per la sicurezza informatica (ACN). Gazzetta Ufficiale, 04.08.2021. Disponibile all'indirizzo: https://www.gazzettaufficiale.it/atto/serie_generale/caricaDettaglioAtto/originario?atto.codiceRedazionale=21A04841
- Repubblica Italiana (2024). Decreto legislativo n. 138/2024 — Recepimento della direttiva NIS2. Gazzetta Ufficiale, 01.10.2024. Disponibile all'indirizzo: https://www.gazzettaufficiale.it/eli/id/2024/10/01/24G00155/SG
- Ministero dell'Istruzione, Repubblica Italiana (2020). Decreto ministeriale n. 89/2020 — Linee guida per la didattica digitale integrata (DDI). Disponibile all'indirizzo: https://www.mim.gov.it/documents/20182/0/Decreto.pdf
- Ministero dell'Istruzione della Repubblica Italiana (2024). Nota MIM n. 5274/2024 — Limitazioni all'uso degli smartphone nelle scuole. Disponibile all'indirizzo: https://www.mim.gov.it/-/nota-n-5274-dell-11-luglio-2024
- Ministero dell'Istruzione della Repubblica Italiana (2025). Circolare MIM n. 3392/2025 — Restrizioni relative ai telefoni cellulari nelle scuole. Disponibile all'indirizzo: https://www.mim.gov.it/-/circolare-n-3392-del-16-giugno-2025
- Ministero dell'Istruzione, Repubblica Italiana (2025). Decreto ministeriale n. 166/2025 — Linee guida per l'uso responsabile dell'intelligenza artificiale nelle scuole. Disponibile all'indirizzo: https://www.mim.gov.it/-/decreto-ministeriale-n-166-del-9-agosto-2025

Portogallo

- Repubblica Portoghese (2018). Legge n. 46/2018 — Quadro giuridico per la sicurezza del cyberspazio (RFSC). Diário da República, 13.08.2018. Disponibile all'indirizzo: https://diariodarepublica.pt/dr/detalhe/lei/46-2018-116029384
- Repubblica Portoghese (2019). Legge n. 58/2019 — Legge portoghese sulla protezione dei dati (attuazione del GDPR). Diário da República, 08.08.2019. Disponibile all'indirizzo: https://diariodarepublica.pt/dr/detalhe/lei/58-2019-123815982

- Consiglio dei Ministri, Repubblica Portoghese (2020). Risoluzione n. 30/2020 — Piano d'azione per la transizione digitale (PATD). Diário da República, 2020. Disponibile all'indirizzo: https://diariodarepublica.pt/dr/detalhe/resolucao-conselho-ministros/30-2020-132133788
- Repubblica Portoghese (2025). Decreto-legge n. 95/2025 — Divieto di utilizzo degli smartphone nelle scuole (classi 1-6). Diário da República, 03.07.2025.
- Repubblica Portoghese (2025). Decreto-legge n. 125/2025 — Recepimento della direttiva NIS2 (in vigore dal 3 aprile 2026). Diário da República, 04.12.2025. Disponibile all'indirizzo: Decreto-Lei n.º 125/2025, de 4 de dezembro | DR
- Direzione Generale dell'Istruzione (DGE), Portogallo. PADDE — Quadro del Piano d'Azione per lo Sviluppo Digitale delle Scuole. Disponibile all'indirizzo: https://www.dge.mec.pt
- Centro Nazionale per la Sicurezza Informatica (CNCS) / DGE, Portogallo. SeguraNet — Risorse sulla sicurezza digitale e la sicurezza informatica per le scuole. Disponibile all'indirizzo: https://www.seguranet.pt
- Centro Nazionale per la Sicurezza Informatica (CNCS), Portogallo. CERT.PT — Squadra nazionale di risposta alle emergenze informatiche. Disponibile all'indirizzo: https://www.cncs.gov.pt/pt/certpt/

Romania

- Repubblica di Romania (2018). Legge n. 190/2018 — Protezione dei dati personali (attuazione del GDPR). Gazzetta Ufficiale della Romania n. 651 del 26.07.2018. Disponibile all'indirizzo: https://portal.just.ro/101/Documents/LEGE__190_2018_date_cu_caracter_personal.pdf
- Repubblica di Romania (2023). Legge n. 58/2023 sugli obblighi in materia di sicurezza informatica per gli operatori di reti e sistemi informativi. Gazzetta Ufficiale della Romania n. 214/15.03.2023. Disponibile all'indirizzo: https://legislatie.just.ro/Public/DetaliiDocument/265677
- Repubblica di Romania (2023). Legge n. 198/2023 — Legge sull'istruzione preuniversitaria. Gazzetta Ufficiale della Romania n. 613 del 5 luglio 2023. Disponibile all'indirizzo: https://edu.ro/sites/default/files/_fisiere/Minister/2023/Legi_educatie_Romania_educata/legi_monitor/Legea_invatamantului_preuniversitar_nr_198.pdf
- Governo della Romania (2024). Ordinanza d'urgenza (OUG) n. 155/2024 — Recepimento della NIS2 (approvata con la Legge n. 124/2025). Gazzetta Ufficiale della Romania n. 1332 del 31.12.2024. Disponibile all'indirizzo: https://legislatie.just.ro/Public/DetaliiDocumentAfis/293121
- Ministero dell'Istruzione, Romania (2024). Ordinanza n. 5707/2024 — Statuto degli studenti. Gazzetta Ufficiale della Romania n. 795/12.08.2024. Disponibile all'indirizzo: https://www.edu.ro/sites/default/files/_fisiere/Legislatie/2024/OM_5707_2024_Statut_elev.pdf
- Ministero dell'Istruzione, Romania (2025). OMEC 6055-6058 — ROFUIP 2025-2026: Regolamento quadro per l'organizzazione e il funzionamento delle unità didattiche preuniversitarie. Gazzetta Ufficiale della Romania n. 819/04.09.2025. Disponibile all'indirizzo: https://www.edu.ro/ROFUIP

Slovacchia

- Repubblica Slovacca (2003). Legge n. 596/2003 Coll. sull'amministrazione statale nell'istruzione e sull'autogoverno scolastico (Legge sulle scuole e sulle strutture scolastiche), e successive modifiche. Disponibile all'indirizzo: https://www.slov-lex.sk
- Repubblica Slovacca (2008). Legge n. 245/2008 Racc. sull'istruzione e la formazione (Legge scolastica), modificata dalla legge n. 323/2025 Racc. con effetto dal 1° gennaio 2025 (restrizioni relative ai telefoni cellulari). Disponibile all'indirizzo: https://www.slov-lex.sk/ezbierky/pravne-predpisy/SK/ZZ/2008/245/

- Repubblica Slovacca (2018). Legge n. 18/2018 Coll. sulla protezione dei dati personali (attuazione del GDPR). Disponibile all'indirizzo: https://www.slov-lex.sk/ezbierky/pravne-predpisy/SK/ZZ/2018/18/
- Repubblica Slovacca (2018). Legge n. 69/2018 Coll. sulla sicurezza informatica. Disponibile all'indirizzo: https://www.zakonypreludi.sk/zz/2018-69
- Repubblica Slovacca (2024). Legge n. 366/2024 Coll. sulla sicurezza informatica (recepimento della direttiva NIS2), in vigore dal 1° gennaio 2025. Disponibile all'indirizzo: https://www.slov-lex.sk/ezbierky/pravne-predpisy/SK/ZZ/2024/366/20250101.html
- Ministero dell'Istruzione, Repubblica Slovacca (2025). Linee guida n. 1/2025 sulla prevenzione e la risoluzione del cyberbullismo nelle scuole e nelle strutture educative. Disponibile all'indirizzo: https://www.minedu.sk/data/att/d76/32441.fb1a83.pdf
- Ministero dell'Istruzione, Repubblica Slovacca (2025). Piano per l'uso responsabile dell'intelligenza artificiale nell'istruzione 2025-2027. Disponibile all'indirizzo: https://ai.iedu.sk/

Norme ISO

Le seguenti norme riconosciute a livello internazionale hanno ispirato l'elaborazione delle raccomandazioni pratiche e delle misure di governance presentate nella presente Politica.

- Organizzazione internazionale per la normazione (ISO), ISO/IEC 27001:2022, Sicurezza delle informazioni, sicurezza informatica e protezione della privacy - Sistemi di gestione della sicurezza delle informazioni - Requisiti. Disponibile all'indirizzo: https://www.iso.org/standard/27001
- Organizzazione internazionale per la normazione (ISO), ISO/IEC 27002:2022, Sicurezza delle informazioni, sicurezza informatica e protezione della privacy – Controlli di sicurezza delle informazioni. Disponibile all'indirizzo: https://www.iso.org/standard/75652.html
- Organizzazione internazionale per la normazione (ISO), ISO/IEC 27701:2025, Tecniche di sicurezza - Estensione alle norme ISO/IEC 27001 e ISO/IEC 27002 per la gestione delle informazioni relative alla privacy - Requisiti e linee guida. Disponibile all'indirizzo: https://www.iso.org/standard/27701
- Organizzazione internazionale per la normazione (ISO), ISO 22301:2019, Sicurezza e resilienza - Sistemi di gestione della continuità operativa - Requisiti. Disponibile all'indirizzo: https://www.iso.org/standard/75106.html
- Organizzazione internazionale per la normazione (ISO), ISO 31000:2018, Gestione del rischio - Linee guida. Disponibile all'indirizzo: https://www.iso.org/standard/65694.html

Ricerca e dati di riferimento

Nella stesura della Parte 4 della presente politica sono state utilizzate le seguenti fonti di ricerca e pubblicazioni.

- Commissione europea (2025). Le opinioni dei bambini sul cyberbullismo: consultazione con bambini di età compresa tra i 12 e i 17 anni. Disponibile all'indirizzo: https://eu-for-children.europa.eu/cyberbullying_en
- Commissione europea (2025). Linee guida sulle misure volte a garantire un elevato livello di privacy, sicurezza e protezione per i minori online. Disponibile all'indirizzo: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:C_202505519
- Commissione europea / Better Internet for Kids (BIK+) / rete Insafe (2025-2026). BIK Policy Monitor e statistiche sulla linea di assistenza. Disponibile all'indirizzo: https://better-internet-for-kids.europa.eu/en
- Agenzia dell'Unione europea per la sicurezza informatica (ENISA) (2022). Iniziative di educazione alla sicurezza informatica negli Stati membri dell'UE. Disponibile all'indirizzo: https://www.enisa.europa.eu/publications/cybersecurity-education-initiatives-in-the-eu-member-states

- OCSE (2025). Com'è la vita dei bambini nell'era digitale? Disponibile all'indirizzo: 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). Una revisione sistematica e una meta-analisi degli interventi volti a ridurre la perpetrazione e la vittimizzazione nel cyberbullismo. Prevention Science. Disponibile all'indirizzo: https://link.springer.com/article/10.1007/s11121-021-01259-y
- Torgal, C. e Aksoy, C. (2022). Una meta-analisi dell'impatto dei programmi scolastici di prevenzione del cyberbullismo sul comportamento dei cyber-spettatori. School Psychology Review, 52(2). Disponibile all'indirizzo: https://www.tandfonline.com/doi/full/10.1080/2372966X.2021.1913037
- Ufficio regionale per l'Europa dell'Organizzazione mondiale della sanità (2024). Comportamenti salutari nei bambini in età scolare (HBSC): risultati sul bullismo e sul cyberbullismo. Disponibile all'indirizzo: https://www.who.int/europe/initiatives/health-behaviour-in-school-aged-children-(hbsc)-study
- Cyberbullismo e giovani LGBTQ: una revisione sistematica della letteratura e raccomandazioni per la prevenzione e l'intervento (2018). Disponibile all'indirizzo: https://pmc.ncbi.nlm.nih.gov/articles/PMC7163911/
- Correlazioni tra dipendenza dai social media e ansia, depressione, FoMO, solitudine e autostima tra gli studenti: una revisione sistematica e una meta-analisi (2025). PLOS ONE. Disponibile all'indirizzo: https://journals.plos.org/plosone/article?id=10.1371/journal.pone.0329466