CONSCIOUS YOUTH BEHAVIOURS
IN EMERGING REALITIES

R5. Document de recomandări de politici privind securitatea datelor și securitatea cibernetică, adaptat în mod specific pentru școli, în conformitate cu standardele ISO 27001, 27002, 27701, 22301 și 31000.

Comportamente conștiente ale tinerilor în realitățile emergente

Coordonator: SIGMA BUSINESS NETWORK, Greece

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.

Date despre document

Grant #	**2023-1-EL01-KA220-SCH-000156982**
Acronim	**C.Y.B.E.R.**
Titlu	**Comportamente conștiente ale tinerilor în realitățile emergente**
Data începerii:	16/11/2023
Rezultat:	Documentul R5 de recomandări de politici publice
Activități asociate:	A4.5 - Proiectarea și dezvoltarea R5
Coordonator de proiect:	SIGMA Tournis Symvouleftiki EE, Greece
Parteneri contributori:	• PRISM IMPRESA SOCIALE S.R.L. , Italy • County Centre for Educational Resources and Assistance Botoșani, Romania • CPM-Centrum Prevencie Mladeze, Slovakia • Casa Do Professor, Portugal • Vitale Tecnologie Comunicazione - VITECO SRL, Italy • EUROCERT Eyropaiki Etaireia Emeghon Kai Pistopoihseon Anonymos Etaireia, Greece
Nivel diseminare	Public
Declinarea responsabilității	Sprijinul acordat de Comisia Europeană pentru elaborarea acestei publicații nu constituie o aprobare a conținutului acesteia, care reflectă exclusiv opiniile autorilor. Comisia Europeană nu poate fi considerată responsabilă pentru nicio utilizare care ar putea fi făcută a informațiilor conținute în această publicație..

Istoricul versiunilor

Dată	Elaborat de	Verificat de	Versiune (Observații)
26/06/2026	SIGMA	Theodora Ntinou	1.0

Despre CYBER	
Tipul acțiunii	Erasmus+ KA220-SCH – Parteneriate de cooperare în educația școlară
Prioritate	ÎNVĂȚĂMÂNT ȘCOLAR: Dezvoltarea competențelor cheie ● Abordarea transformării digitale prin dezvoltarea pregătirii, rezilienței și capacității digitale ● Incluziune și diversitate în toate domeniile educației, formării, tineretului și sportului

Proiectul își propune să răspundă la o întrebare crucială: Cum influențează spațiul cibernetic comportamentul uman, în special în rândul tinerilor? În era digitală de astăzi, comportamentul online a devenit profund integrat în mediul psihologic al spațiului cibernetic. Acesta oferă oportunități unice pentru modelarea interacțiunii umane, dar ridică totodată preocupări din cauza naturii sale fără frontiere. Deși internetul aduce beneficii sociale și economice incontestabile, el a pus la încercare valori europene fundamentale precum egalitatea, drepturile omului și democrația. Pentru a construi un internet mai sigur, este esențial un efort colectiv. Schimbul de bune practici și educarea tinerelor generații, a cadrelor didactice și a părinților reprezintă pași cruciali spre promovarea unui mediu online mai sigur.

Proiectul CYBER își propune să dezvolte reziliența cibernetică a școlilor europene prin crearea unor proceduri de calitate adaptate la nivelul UE pentru sistemul de învățământ și prin echiparea cadrelor didactice și a elevilor cu instrumentele și cunoștințele necesare pentru a dezbate comportamentele online conștiente și inconștiente ale adolescenților, psihologia cibernetică (cyberpsychology) și dezavantajele utilizării excesive a internetului, cu scopul de a spori înțelegerea la nivelul clasei privind comportamentele periculoase emergente la care poate fi expus un tânăr utilizator.

Proiectul CYBER va elabora o metodologie structurată pentru integrarea problematicilor privind amenințările cibernetice și ciberpsihologia în cadrul procesului didactic și al sistemului de învățământ, încurajând dialogul între elevi referitor la noile comportamente de risc la adresa propriei persoane sau a colegilor. De asemenea, proiectul definește proceduri clare de securitate cibernetică și protecție a datelor în vederea obținerii de către unitățile de învățământ a certificării CYBER, stabilind cerințele necesare pentru instituirea, implementarea, menținerea și optimizarea managementului securității informației în mediul școlar.

Rezultatele proiectului sunt menite să vină în sprijinul fiecărui adolescent din toate țările europene, în special al celor născuți în era digitală. Contextul social al acestor probleme (spargerea profilurilor, știrile false, identitățile false, fraudele/înșelăciunile online, șantajul online, revenge porn, fenomenul hikikomori, cyberbullying-ul etc.) are o pondere mult mai mare, iar educarea și conștientizarea tinerilor cu privire la această problematică au un impact de departe mai puternic decât o simplă reglementare națională.

Conținut

Introducere

Acest document reprezintă Politica de Reziliență Cibernetică pentru Școli, elaborată în cadrul proiectului C.Y.B.E.R. (*Conscious Youth Behaviours in Emerging Realities*). Proiectul este cofinanțat de Uniunea Europeană prin Programul Erasmus+ și reunește organizații partenere din Grecia, Italia, Portugalia, România și Slovacia.

În prezent, școlile depind într-o mare măsură de tehnologia digitală. Elevii utilizează platforme online pentru a învăța, cadrele didactice comunică prin intermediul instrumentelor digitale, iar personalul administrează documentele în sisteme conectate. Aceasta este o evoluție pozitivă, însă înseamnă, totodată, că școlile se confruntă cu riscuri pe care nu le-au mai întâlnit în trecut: atacuri cibernetice, încălcări ale securității datelor, cyberbullying și impactul vieții digitale asupra sănătății mintale a elevilor.

Prezenta politică este concepută pentru a ajuta fiecare școală din cele cinci țări partenere să abordeze aceste provocări într-un mod practic. Aceasta reunește legislația europeană, reglementările naționale din fiecare țară, standardele de securitate recunoscute la nivel internațional și cele mai bune cercetări disponibile, toate într-un singur document, pe care orice școală îl poate consulta și utiliza.

Acesta nu este un manual tehnic, ci un ghid adresat tuturor celor care își desfășoară activitatea într-o școală: directorului, cadrelor didactice, personalului administrativ și coordonatorilor IT. Nu aveți nevoie de cunoștințe juridice sau tehnice pentru a-l folosi. Politica explică cerințele legale, bunele practici și măsurile pe care școala dumneavoastră trebuie să le adopte.

Modelele și instrumentele incluse în anexe au un caracter orientativ și adaptabil, unitățile de învățământ având posibilitatea de a le ajusta în funcție de legislația națională aplicabilă, procedurile interne și specificul propriu.

Cui i se adresează această politică?

Această politică se adresează tuturor celor implicați în conducerea și funcționarea unei școli: directorului, directorului adjunct, cadrelor didactice, coordonatorilor IT, personalului administrativ și consiliilor de administrație. Documentul este redactat într-un limbaj accesibil, pentru a fi înțeles de oricine, indiferent de pregătirea de specialitate.

Cum este structurat acest document

Secțiuni	Conținut
Partea 1: Cadrul juridic	Ce le impune legislația europeană școlilor, explicat pe înțelesul tuturor
Partea 2: Cadrul normativ și reglementările naționale	Normele naționale specifice care se aplică în fiecare dintre cele cinci țări
Standardele internaționale și unitățile de învățământ	Modelarea recomandărilor practice prevăzute de această politică, în conformitate cu standardele de management recunoscute la nivel internațional.

Secțiuni	Conținut
Partea 3: Ce ar trebui să facă școala ta	Pași practici organizați pe teme, bazați pe standardele internaționale și legislația UE
Partea 4: Ce ne arată datele și studiile	Ce ne spun cercetările științifice despre ce funcționează cu adevărat în școli
Anexe	Modele de documente și instrumente utile, pe care școala le poate descărca, modifica și folosi imediat
Bibliografie	Actele normative naționale și sursele oficiale utilizate pentru elaborarea Părții 2

Partea 1: Cadrul juridic

Școlile din toate cele cinci țări partenere trebuie să respecte legislația europeană privind prelucrarea datelor și protecția elevilor în mediul online. Această parte explică cerințele legislative într-un limbaj clar și accesibil. Există șase instrumente juridice principale pe care orice școală trebuie să le cunoască. Împreună, acestea acoperă protecția datelor, securitatea cibernetică, inteligența artificială, platformele online, comunicarea digitală și securitatea produselor digitale.

1.1 Regulamentul General privind Protecția Datelor (GDPR)

Regulamentul General privind Protecția Datelor (GDPR) constituie cadrul fundamental în materie de protecția datelor la nivel european. Prevederile sale sunt aplicabile tuturor entităților care prelucrează date cu caracter personal, inclusiv unităților de învățământ. În mediul școlar, datele cu caracter personal cuprind numele și datele de identificare ale elevilor, registrele de prezență, situația școlară, informațiile privind starea de sănătate, materialele foto/video și orice alte date referitoare la o persoană fizică identificată sau identificabilă.

GDPR încadrează minorii în categoria persoanelor vulnerabile. În consecință, instituțiile de învățământ au obligația de a aplica măsuri de protecție mai riguroase în gestionarea datelor privind elevii, comparativ cu standardele aplicabile datelor adulților

Cerințele GDPR aplicabile unităților de învățământ:

- **Școlile trebuie să aibă un temei legal clar pentru fiecare activitate de prelucrare a datelor.** În majoritatea cazurilor, acesta va fi o obligație prevăzută de legislația națională din domeniul educației, o sarcină de interes public necesară pentru funcționarea școlii sau, în anumite cazuri, consimțământul.
- **Școlile ar trebui să colecteze doar datele de care au într-adevăr nevoie.** Acestea nu trebuie să colecteze informații suplimentare doar pentru că s-ar putea să fie utile într-o bună zi.
- **Școlile ar trebui să desemneze un Responsabil cu Protecția Datelor (DPO).** În funcție de țară, această funcție poate fi gestionată la nivel de autoritate sau de grup de școli, și nu individual, pentru fiecare școală în parte.
- **Școlile ar trebui să efectueze o Evaluare a Impactului asupra Protecției Datelor (DPIA) înainte de a introduce orice sistem digital nou** care implică prelucrarea pe scară largă a datelor elevilor sau monitorizarea comportamentului acestora. Un model este inclus în Anexa V.

- **Școlile ar trebui să raporteze încălcările securității datelor cu caracter personal către autoritatea națională de supraveghere în termen de 72 de ore** de la data la care au luat cunoștință de acestea.
- **Școlile ar trebui să îi informeze pe elevi și pe părinți cu privire la modul în care le sunt utilizate datele,** într-un limbaj clar și simplu.
- **Elevii și părinții au dreptul de a accesa datele deținute despre ei, de a solicita rectificări** și, în anumite circumstanțe, de a solicita ștergerea acestora.

Vârsta consimțământului digital

GDPR permite fiecărei țări din UE să stabilească vârsta de la care un tânăr își poate da consimțământul privind utilizarea platformelor digitale, fără aprobarea părinților. Această vârstă variază între 13 și 16 ani, în cele cinci țări partenere. Pentru elevii care nu au atins pragul de vârstă stabilit de țara de apartenență pentru consimțământul digital, școlile trebuie să obțină consimțământul scris al părinților sau al tutorilor legali înainte de a-i înregistra pe platformele digitale. Vârsta specifică fiecărei țări este detaliată în Partea 2.

1.2 Directiva NIS2

Directiva NIS2 instituie un cadru normativ european unitar în domeniul securității cibernetice. Aceasta obligă entitățile să implementeze măsuri corespunzătoare de securitate cibernetică, să gestioneze riscurile asociate furnizorilor de servicii digitale și să semnalizeze incidentele cibernetice semnificative autorităților naționale competente.

Deși unitățile de învățământ nu sunt întotdeauna încadrate direct în categoria entităților esențiale sau importante conform NIS2, gradul ridicat de digitalizare a activității școlare face ca orice incident cibernetic să poată bloca procesul de învățământ și să compromită datele elevilor. Prin urmare, standardele promovate de Directiva NIS2 reprezintă un reper de bune practici pentru toate instituțiile de învățământ, indiferent de statutul lor juridic formal.

Ce înseamnă Directiva NIS2 pentru școli:

- **Școlile ar trebui să pună în aplicare măsuri de securitate cibernetică adaptate riscurilor la care sunt expuse.** La nivel minim, acest lucru presupune parole puternice, copii de rezervă (backup) realizate în mod regulat și rețele protejate.
- **Școlile ar trebui să verifice practicile de securitate cibernetică ale furnizorilor lor de servicii digitale.** O platformă utilizată pentru evidența elevilor trebuie să fie la fel de securizată ca școala însăși.
- **Școlile ar trebui să aibă o procedură pentru detectarea și gestionarea incidentelor de securitate cibernetică.** Personalul trebuie să știe pe cine să contacteze și ce pași trebuie să urmeze.
- **Școlile ar trebui să organizeze periodic sesiuni de instruire și conștientizare privind securitatea cibernetică** pentru întregul personal.
- **Incidentele semnificative ar trebui raportate autorității naționale pentru securitate cibernetică.** Termenele limită și autoritățile competente diferă în funcție de țară (a se vedea Partea 2).

1.3 Legea UE privind inteligența artificială

Legea privind inteligența artificială (AI Act) este prima lege europeană cuprinzătoare care reglementează utilizarea inteligenței artificiale. Aceasta a intrat în vigoare în august 2024 și se aplică treptat, până la punerea sa deplină în aplicare în august 2026. Școlile folosesc din ce în ce mai mult instrumente bazate pe IA: platforme de învățare adaptativă, sisteme de evaluare automată, roboți conversaționali și statistici educaționale (*learning analytics*). Legea privind IA stabilește reguli clare cu privire la modul în care aceste instrumente pot și nu pot fi utilizate.

Ce obligații impune școlilor Legea privind Inteligența Artificială:

- **Anumite utilizări ale IA în școli sunt complet interzise.** Printre acestea se numără sistemele de recunoaștere a emoțiilor utilizate pentru monitorizarea elevilor, clasificarea biometrică a elevilor și recunoașterea facială în timp real în mediile educaționale. Nu există excepții pentru școli.
- **Sistemele IA utilizate pentru evaluarea, admiterea sau monitorizarea elevilor sunt clasificate ca fiind de risc ridicat** și trebuie să îndeplinească cerințe stricte privind transparența, supravegherea umană și documentarea.
- **Elevii și părinții ar trebui să fie informați** atunci când sunt utilizate instrumente IA într-un mod care influențează deciziile educaționale.
- **Un cadru didactic ar trebui să verifice întotdeauna și să își asume responsabilitatea** pentru orice recomandare generată de IA care afectează un elev. IA nu poate lua decizii finale cu privire la elevi.
- **Școlile ar trebui să mențină o listă scrisă a tuturor instrumentelor IA utilizate,** care să includă rolul fiecărui instrument și datele pe care le prelucrează.

1.4 Legea privind Serviciile Digitale (DSA)

Legea privind Serviciile Digitale (DSA) reglementează platformele online și serviciile digitale. Acesta impune platformelor să fie mai transparente, să ofere modalități accesibile de raportare a conținutului dăunător și să consolideze protecția tinerilor. Școlile au un rol important în a-i ajuta pe elevi să înțeleagă modul în care funcționează platformele online și cum se pot proteja.

Ce înseamnă DSA pentru școli:

- **Școlile ar trebui să îi învețe pe elevi cum să recunoască și să raporteze conținutul dăunător** de pe platformele pe care le utilizează.
- **Școlile ar trebui să îi ajute pe elevi să înțeleagă modul în care funcționează algoritmii de recomandare** și cum le influențează aceștia conținutul pe care îl văd în mediul online.
- **Cadrele didactice ar trebui să cunoască obligațiile pe care DSA le impune marilor platforme** și să fie capabile să le discute cu elevii, ca parte a educației privind competențele digitale.

1.5 Directiva ePrivacy

Directiva ePrivacy protejează confidențialitatea comunicațiilor electronice. Aceasta se aplică sistemelor de poștă electronică (e-mail), platformelor de mesagerie, instrumentelor de videoconferință și oricărui alt serviciu de comunicare digitală utilizat în școli.

Ce înseamnă Directiva ePrivacy pentru școli:

- Comunicarea digitală dintre elevi, părinți, cadre didactice și personalul administrativ trebuie să fie sigură și confidențială.
- Instrumentele de videoconferință utilizate pentru învățarea la distanță trebuie configurate astfel încât să prevină accesul neautorizat. Sălile de clasă virtuale ar trebui să solicite autentificarea înainte ca cineva să se poată alătura.
- Lecțiile și ședințele nu trebuie înregistrate fără consimțământul explicit al tuturor participanților.
- Site-urile și platformele școlare care folosesc module cookie trebuie să afișeze o notificare privind cookie-urile conformă cu cerințele legale.

1.6 Legea privind securitatea cibernetică

Legea privind securitatea cibernetică consolidează rolul ENISA, Agenția Uniunii Europene pentru Securitate Cibernetică, și stabilește un cadru european pentru certificarea produselor și serviciilor digitale ca fiind sigure. Acesta susține adoptarea tehnologiilor de încredere în întreaga UE, inclusiv în școli.

Ce înseamnă Legea privind securitatea cibernetică pentru școli:

- Atunci când școlile aleg instrumente digitale, platforme sau echipamente, ar trebui să ia în considerare securitatea cibernetică și să prefere produsele certificate sau aprobate, acolo unde este posibil.
- Dispozitivele conectate din sălile de clasă, cum ar fi tablele interactive (smart), tabletele și camerele web, ar trebui să fie configurate în mod securizat și cu actualizările la zi.
- Școlile pot consulta ghidurile și instrumentele furnizate de ENISA pentru a le ajuta să își planifice strategia de securitate cibernetică.

1.7 Cum funcționează aceste legi împreună

Aceste șase instrumente juridice nu reprezintă obligații separate care trebuie abordate individual. Ele formează un cadru integrat. O școală care protejează datele elevilor în conformitate cu GDPR, gestionează securitatea cibernetică conform NIS2, utilizează inteligența artificială în mod responsabil în baza Legii privind IA, predă competențe digitale în acord cu DSA, securizează comunicațiile conform Directivei ePrivacy și selectează tehnologii de încredere în acord cu Legea privind securitatea cibernetică va acoperi întreaga gamă a obligațiilor sale legale.

Legea	Principalele obligații ale școlilor
GDPR	Protejează datele cu caracter personal, desemnează un DPO (Responsabil cu protecția datelor), obține consimțământul acolo unde este necesar și raportează încălcările securității datelor în termen de 72 de ore.
Directiva NIS2	Implementează măsuri de securitate cibernetică, verifică-ți furnizorii, raportează incidentele și instruiește-ți personalul.

EU AI Act	Nu utiliza sisteme AI interzise, menține deciziile sub control uman, informează elevii și părinții.
Legea privind serviciile digitale	Învață-i pe elevi să raporteze conținutul dăunător și să înțeleagă modul în care funcționează algoritmii.
Directiva ePrivacy	Securizează comunicațiile digitale, protejează clasele virtuale și respectă regulile privind modulele cookie.
Legea privind securitatea cibernetică	Ține cont de securitate atunci când achiziționezi tehnologie, securizează dispozitivele conectate și respectă ghidurile ENISA.

Partea 2: Ce se aplică în țara dumneavoastră

Legislația europeană stabilește cadrul comun, dar fiecare țară are propriile legi și ghiduri naționale pe care școlile trebuie să le respecte. Această parte rezumă cele mai importante reguli naționale pentru fiecare dintre cele cinci țări partenere. Găsiți-vă țara și verificați ce vi se aplică.

2.1 Grecia

Grecia aplică un model puternic centralizat pentru guvernanța digitală în școli. Securitatea cibernetică, protecția datelor și infrastructura digitală sunt gestionate în principal la nivel național de către Ministerul Educației și Ministerul Guvernării Digitale. Școlile individuale funcționează predominant ca utilizatori ai sistemelor gestionate centralizat, inclusiv ai sistemului de informații privind elevii MySchool, ai platformei de învățare e-Class și ai Rețelei Școlare Panelenice (PSN).

Domeniul	Ce înseamnă acest lucru pentru școli
Transpunerea Directivei NIS2 Legea 5160/2024 MD 1689/2025 MD 1899/2025	• Școlile trebuie să pună în aplicare măsuri de gestionare a riscurilor și să se asigure că platformele digitale ale terților (de exemplu, Webex) respectă standardele de securitate cibernetică. • Raportarea obligatorie a incidentelor: școlile trebuie să notifice EAKE cu privire la incidentele semnificative de securitate cibernetică. • Sunt necesare politici formale de securitate care să acopere controlul accesului la datele elevilor, procedurile de rezervă (backup), criptarea comunicațiilor și securitatea lanțului de aprovizionare pentru software-ul și hardware-ul utilizate în școli. • Instruirea personalului și igiena cibernetică sunt obligatorii: personalul școlar reprezintă o țintă frecventă a atacurilor de tip phishing și inginerie socială. • Școlile trebuie să mențină o documentație care să includă politici de securitate, evidențe ale instruirilor, diagrame de rețea și rezultate ale auditurilor periodice de securitate. • OM 1899/2025 impune desemnarea unui responsabil cu securitatea cibernetică, precum și proceduri formale de răspuns la incidente și de escaladare a acestora.

Domeniul	Ce înseamnă acest lucru pentru școli
Protecția datelor Legea 4624/2019	• Reglementează prelucrarea datelor cu caracter personal de către organismele din sectorul public, inclusiv școlile, în conformitate cu principiile GDPR. • Stabilește rolul și competențele de supraveghere ale Autorității Elene pentru Protecția Datelor (HDPA). • Responsabilitățile DPO (Responsabilul cu protecția datelor) sunt gestionate la nivel de autoritate, nu individual pentru fiecare școală în parte. • Școlile trebuie să notifice HDPA (Autoritatea Elenă pentru Protecția Datelor) în termen de 72 de ore de la orice încălcare a securității datelor cu caracter personal susceptibilă să genereze un risc pentru persoane. • Școlile trebuie să pună în aplicare măsuri de securitate adecvate pentru datele elevilor, părinților și personalului.
Vârsta consimțământului digital	• 15 ani. • Școlile trebuie să obțină consimțământul scris al părinților sau al tutorelui legal înainte de a înscrie elevii cu vârsta sub 15 ani pe orice platformă digitală care le prelucrează datele cu caracter personal.
Cyberbullying Legea 5029/2023	• Oferă un cadru juridic structurat pentru prevenirea și gestionarea hărțuirii cibernetice (cyberbullying) în școli. Introduce platforma națională de raportare stop-bullying.gov.gr pentru transmiterea și urmărirea formală a incidentelor. • Școlile trebuie să participe activ la identificarea, raportarea și gestionarea cazurilor de hărțuire cibernetică. • Școlile trebuie să aibă o procedură scrisă pentru gestionarea incidentelor de hărțuire cibernetică.
Telefoanele mobile	• Elevilor le este interzisă deținerea sau utilizarea telefoanelor mobile în incinta școlii. • Politică de toleranță zero în vigoare din anul 2024. • Abaterile atrag consecințe disciplinare imediate, inclusiv suspendarea.
IA in Educație	• Nu au fost emise ghiduri naționale specifice pentru utilizarea inteligenței artificiale în școli. • Legea UE privind IA (EU AI Act) se aplică direct. • Școlile ar trebui să manifeste precauție atunci când utilizează instrumente de IA care prelucrează datele elevilor.
Infrastructura digitală	• MySchool: sistemul național de informații privind elevii, gestionat centralizat. • e-Class: platforma națională de management al învățării (LMS).

Domeniul	Ce înseamnă acest lucru pentru școli
	• Panhellenic School Network (PSN): infrastructura națională securizată de conectivitate pentru toate școlile publice.
Contacte principale	• Securitate cibernetică: EAKE (cyber.gov.gr) • Protecția datelor: HDPA (dpa.gr) • Hărțuire cibernetică (Cyberbullying): stop-bullying.gov.gr

2.2 Italia

Italia aplică un model predominant centralizat, deși școlile păstrează un anumit grad de autonomie organizatorică. Agenția Națională de Securitate Cibernetică (ACN) joacă un rol central în coordonare și în gestionarea incidentelor. Școlile depind în mare măsură de recomandările ministeriale și de platformele gestionate centralizat, inclusiv platforma națională Unica. Autoritatea pentru Protecția Datelor (Garante) a emis ghiduri specifice și întrebări frecvente (FAQ) destinate școlilor, pe care acestea ar trebui să le consulte alături de GDPR.

Domeniul	Ce înseamnă acest lucru pentru școli
Transpunerea NIS2 Decretul Legislativ 138/2024 Legea 109/2021	• Decretul legislativ 138/2024 conturează cerințele privind evaluarea riscurilor, securitatea furnizorilor și raportarea incidentelor, chiar și pentru școlile care nu sunt clasificate direct ca entități NIS. • Școlile trebuie să gestioneze serviciile TIC furnizate de terți și să mențină canale structurate de raportare atunci când incidentele afectează activitățile educaționale sau datele elevilor. • Legea 109/2021 înființează Agenția Națională de Securitate Cibernetică (ACN), care joacă un rol central de coordonare a guvernanței securității cibernetice în instituțiile publice, inclusiv în școli.
Protecția datelor Decretul legislativ 196/2003 (modificat prin Decretul 101/2018)	• Reglementează prelucrarea datelor elevilor, părinților, cadrelor didactice și personalului în cadrul activităților școlare. • Autoritatea de supraveghere este Garante per la protezione dei dati personali. • Desemnarea DPO (Responsabilul cu protecția datelor) este obligatorie pentru școlile publice, dar poate fi organizată la nivel de școală sau prin acorduri comune între mai multe școli. • Autorizarea părinților este necesară pentru prelucrarea datelor copiilor atunci când serviciile digitale sunt oferite direct elevilor sub vârsta consimțământului digital. • Școlile trebuie să informeze elevii și părinții cu privire la drepturile lor privind datele și să gestioneze încălcările securității datelor în conformitate cu cerințele GDPR.

Domeniul	Ce înseamnă acest lucru pentru școli
Vârsta consimțământului digital	• 14 ani. • Consimțământul părinților este necesar pentru elevii cu vârsta sub 14 ani pentru înscrierea pe platformele de management al învățării (LMS), publicarea fotografiilor și orice prelucrare de date care implică minori într-un cadru educațional.
Hărțuirea cibernetică (Cyberbullying) Legea 71/2017	• Oferă un cadru juridic pentru combaterea hărțuirii cibernetice (cyberbullying) în școli. • Școlile trebuie să aibă proceduri scrise pentru gestionarea incidentelor și sprijinirea victimelor. • Școlile pot solicita eliminarea conținutului dăunător de pe platformele online.
Telefoane mobile Nota MIM 5274/2024 Circulara MIM 3392/2025	• Telefoanele inteligente sunt restricționate în timpul tuturor activităților școlare, la toate ciclurile de învățământ. • Restricțiile au ca scop protejarea mediului educațional și promovarea unei utilizări adecvate vârstei a instrumentelor digitale. • Excepții limitate se aplică doar pentru activități educaționale specifice sau pentru nevoi de accesibilitate.
Inteligența Artificială în Educație Decretul ministerial 166/2025	• Ghidurile naționale impun transparență cu privire la utilizarea inteligenței artificiale în școli. • Supravegherea umană asupra deciziilor educaționale susținute de IA este obligatorie. • Instrumentele de IA care prelucrează datele elevilor trebuie să respecte cerințele GDPR.
Platforme digitale	• Unica: platforma națională pentru funcții administrative și educaționale. • Microsoft 365 for Education: suită gestionată la nivel instituțional pentru predare și comunicare. • Cadrul de Predare Digitală Integrată (DDI) (MD 89/2020) impune școlilor să reglementeze utilizarea platformelor digitale, accesul elevilor și responsabilitățile cadrelor didactice în mediile educaționale online.
Contacte cheie	• Securitate cibernetică: ACN (acn.gov.it) • Protecția datelor: Garante (garanteprivacy.it)

2.3 Portugalia

Portugalia are unul dintre cele mai bine structurate cadre naționale de administrare digitală în școli din rândul celor cinci țări. Școlile beneficiază de planul obligatoriu PADDE (Planul de Acțiune pentru Dezvoltarea Digitală a Școlii), de programul de sprijin SeguraNet și de CERT.PT pentru gestionarea

incidentelor. Directiva NIS2 a fost transpusă prin Decretul-Lege 125/2025, care a intrat în vigoare la 3 aprilie 2026.

Domeniul	Ce înseamnă acest lucru pentru școli
Transpunerea NIS2 Decretul-Lege 125/2025 (în vigoare din 3 aprilie 2026) Legea 46/2018	• Școlile încadrate ca Entități Publice Relevante (Grupul A sau B) trebuie să pună în aplicare măsuri de gestionare a riscurilor de securitate cibernetică. • Desemnarea unui responsabil cu securitatea cibernetică este obligatorie. • Incidentele semnificative trebuie raportate către CNCS în termen de 24 de ore. • Școlile trebuie să identifice activele digitale critice, să stabilească proceduri de răspuns la incidente și să asigure continuitatea activității. • Legea 46/2018 rămâne cadrul fundamental care stabilește CNCS ca autoritate națională pentru securitate cibernetică.
Protecția datelor Legea 58/2019	• Desemnarea unui DPO (Responsabil cu protecția datelor) este obligatorie la nivelul fiecărui grup școlar (agrupamento de escolas), nu al fiecărei școli individuale. • DPO-ul trebuie să fie înregistrat la CNPD (Comisia Națională pentru Protecția Datelor) și este responsabil pentru monitorizarea respectării GDPR, consilierea personalului, desfășurarea formărilor și menținerea legăturii cu CNPD. • Școlile trebuie să notifice CNPD în termen de 72 de ore de la producerea unei încălcări a securității datelor cu caracter personal susceptibile să genereze un risc pentru persoane. • Școlile trebuie să țină un registru al activităților de prelucrare și să pună în aplicare măsuri de securitate adecvate.
Vârsta consimțământului digital	• 13 ani. Acesta este cel mai scăzut prag dintre cele cinci țări. • Este necesar consimțământul verificabil al părinților sau al tutorelui legal înainte de a înscrie elevii cu vârsta sub 13 ani pe orice platformă digitală sau instrument online care prelucrează date cu caracter personal. • Acest lucru se aplică platformelor de management al învățării (LMS), publicării fotografiilor și oricărei prelucrări de date care implică minori.
Hărțuirea cibernetică (Cyberbullying) Programul SeguraNet	• SeguraNet (gestionat de DGE în parteneriat cu CNCS) oferă îndrumări specifice privind prevenirea și gestionarea hărțuirii cibernetice (cyberbullying). • Școlile trebuie să integreze prevenirea hărțuirii cibernetice în planul lor PADDE și în regulamentele interne. • Modele pentru procedurile de răspuns la incidente și documente privind Politica de Utilizare Acceptabilă (AUP) sunt disponibile prin intermediul SeguraNet.

Domeniul	Ce înseamnă acest lucru pentru școli
Telefoane mobile Decretul-Lege 95/2025 (în vigoare din septembrie 2025)	• Smartphone-urile sunt interzise prin lege pentru toți elevii din clasele I-VI (ciclul primar și gimnazial) în toate școlile publice și private. • Pentru ciclul 3 și învățământul secundar, Ministerul a emis recomandări care încurajează restricțiile, școlile păstrându-și autonomia de a formaliza regulile în propriile regulamente interne. • Orice înregistrare a elevilor necesită consimțământul explicit în conformitate cu cerințele GDPR.
Planul digital al școlii (obligatoriu) Cadrul PADDE	• Fiecare grup școlar trebuie să elaboreze și să mențină un PADDE (Plan de Acțiune pentru Dezvoltarea Digitală a Școlii). • PADDE trebuie să includă în mod explicit măsuri de securitate cibernetică și acoperă trei dimensiuni: organizațională (leadership și guvernanță), pedagogică (cetățenie digitală și educație privind siguranța pe internet) și tehnologică (infrastructură și securitate). • Școlile trebuie să adopte o Politică de Utilizare Acceptabilă și să stabilească proceduri de răspuns la incidente cu trimitere la CERT.PT.
IA in educație	• Nu au fost emise încă ghiduri naționale specifice. • Legea UE privind IA (EU AI Act) se aplică direct. • DGE a recunoscut necesitatea unui cadru național și este de așteptat să emită recomandări. • Școlile ar trebui să manifeste precauție atunci când utilizează instrumente de IA care prelucrează datele elevilor.
Infrastructura digitală	• RCTS (gestionată de FCCN): rețeaua națională securizată de mare viteză pentru toate grupurile școlare publice. • Microsoft 365 for Education: suită gestionată la nivel național pentru predare și comunicare. • CERT.PT (operat de CNCS): CSIRT național și punct de contact pentru răspunsul la incidente în sectorul educațional.
Contacte cheie	• Securitate cibernetică: CNCS (cncs.gov.pt) • Răspuns la incidente: CERT.PT • Protecția datelor: CNPD (cnpd.pt) • Siguranță digitală: SeguraNet (seguranet.pt)

2.4 România

Cadrul național este coordonat de Ministerul Educației în colaborare cu Directoratul Național de Securitate Cibernetică (DNSC), în cadrul mai larg al politicii naționale și europene privind securitatea cibernetică. În multe școli, responsabilitățile legate de securitatea cibernetică sunt preluate de directorul școlii, coordonatorul TIC sau un cadru didactic desemnat, deoarece personalul dedicat securității cibernetice este rar. România se confruntă cu unele dintre cele mai mari decalaje de implementare dintre cele cinci țări partenere, dar există o dinamică în creștere pentru a le aborda.

Domeniul	Ce înseamnă acest lucru pentru școli
Transpunerea Directivei NIS2 OUG 155/2024 (aprobată prin Legea 124/2025) Legea 58/2023	• OUG 155/2024 se aplică direct învățământului superior. Pentru unitățile de învățământ preuniversitar, aplicabilitatea nu este pe deplin clară, însă școlile care interacționează cu rețele guvernamentale (de exemplu, SIIIR) au obligația de a respecta protocoalele NIS2. • Școlile trebuie să raporteze incidentele semnificative către DNSC în termen de 24 de ore prin intermediul platformei PNRISC. • Măsurile obligatorii includ: segmentarea rețelei (Wi-Fi separat pentru administrație și elevi), autentificarea cu mai mulți factori (MFA) pentru accesul la platformele oficiale, politici de analiză a riscurilor și instruirea obligatorie privind igiena cibernetică pentru întreg personalul. • Securitatea lanțului de aprovizionare: furnizorii privați de platforme de e-learning sau de programe informatice de contabilitate utilizate de școli trebuie să fie conformi cu cerințele NIS2. • Legea 58/2023 stabilește că responsabilitatea pentru securitatea cibernetică revine entității care deține sau administrează rețeaua, făcând conducerea școlii direct răspunzătoare.
Protecția datelor Legea 190/2018	• Școlile sunt clasificate ca operatori independenți de date și trebuie să asigure conformitatea deplină cu GDPR. • Este permisă desemnarea unui Responsabil cu Protecția Datelor (DPO) în regim comun la nivelul inspectoratului școlar județean sau la nivel central. • Școlile trebuie să implementeze proceduri obligatorii de obținere a acordului părintelui pentru utilizarea platformelor de învățare online și pentru folosirea imaginilor elevilor. • Supravegherea video este permisă exclusiv pentru protecția persoanelor și a bunurilor, fiind obligatorie informarea elevilor, cadrelor didactice și vizitatorilor. Înregistrările nu pot fi păstrate mai mult de 30 de zile, cu excepția situațiilor în care sunt parte a unor anchete în desfășurare. • Rezultatele examenelor trebuie publicate prin anonimizare sau pseudonimizare, în conformitate cu ghidurile ANSPDCP.
Vârsta consimțământului digital	• **16 ani.** Acesta este cel mai ridicat prag dintre cele cinci țări. • Este necesar acordul părintelui sau al tutorelui înainte de înregistrarea elevilor cu vârsta sub 16 ani pe orice platformă digitală. • În practică, această cerință se aplică aproape tuturor instrumentelor educaționale digitale utilizate în școlile din România.
Cyberbullying (Hărțuirea cibernetică) ROFUIP 2025/2026	• ROFUIP definește și sancționează cyberbullying-ul ca fiind un comportament interzis în mediul școlar. • Înregistrarea audio sau video neautorizată a activităților didactice este strict interzisă.

Domeniul	Ce înseamnă acest lucru pentru școli
Statutul elevului (Ordinul 5707/2024)	• Personalul didactic trebuie să utilizeze exclusiv instrumente digitale aprobate oficial și să trateze datele elevilor cu o confidențialitate strictă. • Statutul Elevului interzice în mod explicit orice formă de agresiune în mediul virtual. • Nu există o platformă națională dedicată pentru raportare. Incidentele sunt gestionate la nivelul unității de învățământ și sunt redirecționate către ANSPDCP în cazul în care sunt implicate date cu caracter personal.
Telefoane mobile Legea 198/2023 ROFUIP	• Utilizarea telefoanelor mobile în timpul orelor de curs este interzisă la nivelul unităților de învățământ, cu excepția cazurilor în care este autorizată de cadrul didactic în scopuri educaționale. • Telefoanele trebuie să fie oprite sau trecute pe modul silențios pe durata orelor și depozitate într-un spațiu special amenajat, conform prevederilor ROFUIP. • Regulile privind utilizarea telefoanelor în timpul pauzelor sunt stabilite prin Regulamentul Intern al fiecărei unități de învățământ.
IA in educație	• Nu au fost emise ghiduri naționale specifice. Legea UE privind inteligența artificială(EU AI Act) se aplică direct. • Ministerul Educației nu a emis îndrumări cu privire la instrumentele de IA generativă (cum ar fi ChatGPT), creând un vid legislativ semnificativ. • Unitățile de învățământ trebuie să aplice cerințele Legii privind IA referitoare la transparență, supraveghere umană și protecția datelor atunci când utilizează orice instrument bazat pe IA în relație cu elevii.
Infrastructura digitală	• Nu există o rețea școlară națională unificată. Școlile depind de furnizori comerciali de servicii de internet, ceea ce duce la standarde de securitate cibernetică neuniforme. • SIIIR (gestionat centralizat de Minister) este principala bază de date națională pentru datele elevilor. • Școlile utilizează platforme comerciale (Google Workspace, Microsoft 365) pe baza unor contracte individuale.
Contacte principale	• Securitate cibernetică: DNSC (dnsc.ro) • Protecția datelor: ANSPDCP (dataprotection.ro)

2.5 Slovacia

Slovacia a demonstrat o dinamică legislativă puternică în privința guvernanței digitale în școli. Legea privind Securitatea Cibernetică 366/2024, restricțiile privind utilizarea telefoanelor mobile intrate în vigoare din ianuarie 2025, ghidul dedicat împotriva hărțuirii cibernetice (Ghidul 1/2025) și planul național privind introducerea IA în educație pentru perioada 2025–2027 reflectă o abordare cuprinzătoare și structurată. Directorul școlii poartă răspunderea juridică directă pentru securitatea cibernetică, conform legislației slovace. Programul de infrastructură DigiEDU/DigiNET asigură conexiune securizată și centralizată la internet pentru toate școlile din Slovacia.

Domeniul	Ce înseamnă acest lucru pentru școli
Transpunerea Directivei NIS2 Legea 366/2024 Legea 69/2018	• Legea 366/2024 definește direct obligațiile privind securitatea cibernetică ca responsabilitatea legală a directorului școlii, conform Legii 596/2003 privind învățământul. Directorul este răspunzător personal și juridic pentru protejarea sistemelor informatice ale școlii și a datelor cu caracter personal. • Unitățile de învățământ trebuie să implementeze măsuri fundamentale de securitate: parole complexe, software antivirus, actualizări periodice, copii de siguranță ale datelor (backup) și controlul accesului. • Școlile trebuie să aibă capacitatea de a răspunde la atacuri de tip phishing, ransomware, scurgeri de date și compromiteri ale sistemelor. • Trebuie urmate proceduri obligatorii de raportare în cazul incidentelor grave de securitate cibernetică. • Legea 69/2018 oferă cadrul fundamental pentru protecția sistemelor informatice și a rețelelor, asigurând securitatea datelor elevilor și utilizarea în siguranță a tehnologiilor digitale în școli.
Protecția datelor Legea 190/2018	• Un DPO (Responsabil cu Protecția Datelor) este obligatoriu pentru școlile publice, dar nu este necesar să existe unul desemnat per școală: este permisă desemnarea unui DPO comun pentru mai multe unități de învățământ. • Școlile trebuie să aplice minimizarea datelor: să colecteze și să utilizeze doar datele cu caracter personal ale elevilor care sunt strict necesare pentru activitatea educațională și administrativă. • Accesul la date trebuie limitat la persoanele autorizate (cadre didactice, conducere, personal administrativ), în funcție de necesitate. • Sistemele electronice, e-mailurile, documentele pe suport de hârtie și dispozitivele de stocare trebuie protejate împotriva pierderii sau accesului neautorizat. • Fotografiile, listele de elevi, rezultatele sau informațiile sensibile nu trebuie publicate fără un temei legal sau fără consimțământul explicit. • Orice încălcare a securității datelor cu caracter personal trebuie raportată autorității competente în termen de 72 de ore, dacă aceasta prezintă un risc pentru persoanele afectate.
Vârsta consimțământului digital	• 16 ani. • Este necesar consimțământul părinților sau al tutorelui legal înainte de a înscrie pe platforme digitale elevii cu vârsta sub 16 ani.
Hărțuirea cibernetică (Cyberbullying) Ghidul 1/2025	• Ghidul 1/2025 oferă reguli specifice privind prevenirea și soluționarea hărțuirii cibernetice în școli și unități de învățământ. • Definește semnele de bază, formele și manifestările hărțuirii cibernetice. • Stabilește proceduri de prevenire și metode de gestionare a incidentelor. • Include proceduri pentru sprijinirea victimelor.

Domeniul	Ce înseamnă acest lucru pentru școli
	• Școlile trebuie să implementeze procedurile prevăzute în acest ghid.
Telefoane mobile Legea 245/2008 (modificată din ianuarie 2025)	• Elevilor din clasele I-III le este complet interzisă utilizarea telefoanelor mobile sau a dispozitivelor similare pe durata programului școlar. • Elevii din clasele IV-IX le pot utiliza exclusiv în scopuri educaționale, doar atunci când cadrul didactic permite în mod specific acest lucru. • O excepție se aplică elevilor cu dizabilități, care folosesc dispozitivul în legătură cu starea lor de sănătate. • În cazul unei încălcări a regulilor, școala poate confisca temporar dispozitivul. • Condițiile detaliate sunt reglementate prin regulamentul intern al școlii.
IA în educație Planul privind IA 2025-2027	• Planul Ministerului Educației privind Utilizarea Responsabilă a IA în Educație 2025-2027 oferă îndrumări naționale practice pentru școli. • Școlile ar trebui să utilizeze acest plan împreună cu Legea UE privind IA(EU AI Act) pentru a evalua și guverna orice instrumente bazate pe IA pe care le introduc. • Se pune accent pe siguranță, utilizare etică și transparență.
Infrastructura digitală	• DigiEDU/DigiNET: Program de conectivitate la internet securizat și gestionat centralizat pentru toate școlile din Slovacia. • Securitatea cibernetică este supravegheată de Oficiul Național de Securitate (NBU), care operează SK-CERT pentru răspunsul la incidente. • NBU oferă îndrumare și sprijin pentru instituțiile publice, inclusiv pentru școli.
Contacte cheie	• Securitate Cibernetică: NBU/SK-CERT (nbu.gov.sk) • Protecția Datelor: UOOU (dataprotection.gov.sk)

Standardele internaționale aplicabile în unitățile de învățământ

Recomandările practice din Partea 3 a prezentei politici au la bază un set de standarde de management recunoscute la nivel internațional. Această scurtă secțiune explică ce reprezintă aceste standarde și de ce sunt importante pentru școli. Nu este necesar să cunoașteți în detaliu standardele respective pentru a putea aplica ghidul din Partea 3. Ceea ce oferă aceste standarde este o temelie verificată și larg acceptată, care conferă acestei politici structură și credibilitate.

Cinci standarde sunt relevante în acest context, fiecare dintre ele abordând o dimensiune diferită a modului în care școlile își pot proteja elevii, datele și sistemele.

ISO/IEC 27001 este regulamentul internațional pentru siguranța informațiilor. El ajută școala să știe ce date are, ce pericole pot apărea și ce măsuri trebuie luate. Este vorba despre cataloage, dosare ale elevilor și profesorilor, platforme de cursuri și toate sistemele din școală. Acest standard nu oferă soluții tehnice

fixe, ci te învață să te gândești organizat la securitate. Sfaturile din Secțiunile 3.1 - 3.7 pleacă de la această bază.

ISO/IEC 27002 vine în completarea primului standard și arată pașii concreți: cum se dă accesul în programe, cum se gestionează corect parolele, ce faci când apare o problemă IT și cum se configurează în siguranță tabletele sau calculatoarele. Secțiunile 3.2 și 3.3 sunt construite pe acest standard.

ISO/IEC 27701 adaugă reguli clare pentru protecția datelor personale. Este compatibil cu GDPR și ajută școala să arate că folosește datele elevilor și ale profesorilor în mod corect și legal. Secțiunea 3.1 se bazează pe el.

ISO 22301 constituie standardul internațional de referință pentru managementul continuității activității. În contextul unităților de învățământ, acesta presupune pregătirea proactivă pentru gestionarea situațiilor de criză sau perturbare: atacuri cibernetice, avarii majore ale sistemelor informatice sau incidente de tip ransomware care blochează accesul la bazele de date administrative și educaționale. Standardul ISO 22301 impune instituțiilor planificarea riguroasă a acestor scenarii, implementarea strategiilor de salvare a datelor (backup) și a procedurilor de restaurare, precum și testarea periodică a acestora pentru garantarea eficacității operaționale. O școală care adoptă acest model poate asigura reluarea rapidă a activității în urma unui incident, evitând perioadele prelungite de nefuncționare. Secțiunea 3.2 și protocolul de răspuns la incidente din Anexa IV sunt fundamentate pe prevederile acestui standard.

ISO 31000 reprezintă standardul internațional de referință privind managementul riscului. Acesta furnizează un cadru conceptual și metodologic aplicabil tuturor dimensiunilor activității dintr-o unitate de învățământ, depășind sfera strictă a securității cibernetice. Înaintea adoptării unei noi platforme digitale, integrării unui instrument de inteligență artificială sau modificării procedurilor de prelucrare a datelor cu caracter personal ale elevilor, conducerea școlii trebuie să evalueze: care sunt riscurile potențiale, care este probabilitatea de materializare a acestora și ce impact ar avea. Această viziune restructurează procesul de Evaluare a Impactului asupra Protecției Datelor (DPIA) din Anexa V, metodologia de evaluare a platformelor din Secțiunea 3.3 și întreaga abordare bazată pe risc din Partea 3.

Împreună, aceste cinci standarde constituie coloana vertebrală a Părții 3. Ele reprezintă motivul pentru care recomandările din această politică nu sunt arbitrare. Acestea reflectă decenii de cunoștințe acumulate despre modul în care organizațiile își pot proteja informațiile, își pot gestiona riscurile și pot continua să funcționeze atunci când lucrurile nu merg bine. Ghidul care urmează transpune aceste cunoștințe în pași practici pe care îi poate urma orice școală.

Partea 3: Ce ar trebui să facă școala dumneavoastră

Această parte este structurată în șapte domenii. Fiecare domeniu începe cu o scurtă explicație privind importanța sa, urmată de un tabel care arată ce trebuie să facă școala dumneavoastră, de ce este importantă fiecare acțiune și cum poate fi pusă în aplicare.

Recomandările din această secțiune sunt cel mai eficiente atunci când implică întreaga comunitate școlară. Conducerea școlii, cadrele didactice, personalul administrativ, elevii, părinții și organizațiile externe de sprijin au toate un rol de jucat în crearea unui mediu digital sigur. Comunicarea regulată, educația practică și canalele de raportare securizate ajută școlile să construiască o cultură a rezilienței cibernetice, în loc să reacționeze pur și simplu la incidente.

3.1 **Protecția datelor cu caracter personal**

Școlile dețin o cantitate mare de informații cu caracter personal despre elevi, părinți și personalul angajat. Acestea includ nume, coduri numerice personale (sau numere de identificare), evidențe ale prezenței, note, informații privind starea de sănătate și date de contact ale familiei. Protejarea acestor date reprezintă o obligație legală, dar este, în egală măsură, și o chestiune de încredere. Familiile furnizează informații sensibile școlilor din necesitate, iar școlile au responsabilitatea de a le gestiona cu maximă atenție.

Atunci când protecția datelor eșuează, consecințele pot fi grave. Informațiile despre elevi pot ajunge la persoane neautorizate, școala se poate confrunta cu investigații oficiale din partea autorităților, iar încrederea elevilor și a părinților este extrem de greu de recuperat. Este mult mai ușor să pui la punct regulile de bază de la bun început decât să gestionezi urmările unei breșe de securitate.

Ce presupune	De ce este important	Cum se procedează
Desemnarea unui Responsabil cu protecția datelor (DPO)	DPO-ul este persoana responsabilă pentru asigurarea conformității școlii dumneavoastră cu legislația privind protecția datelor. În lipsa acestei funcții, nu există o răspundere clară în cazul apariției unei probleme. De asemenea, DPO-ul este principalul punct de contact pentru elevi, părinți și autoritatea națională de supraveghere.	Verificați Partea a 2-a pentru a stabili dacă școala dumneavoastră are nevoie de propriul DPO sau dacă această funcție este asigurată la nivel de consorții ori de către autoritatea locală. DPO-ul trebuie să fie accesibil personalului, elevilor și părinților. Acesta are responsabilitatea de a monitoriza conformitatea, de a oferi consultanță privind protecția datelor, de a instrui personalul și de a menține legătura cu autoritatea de supraveghere.
Păstrați o evidență a tuturor activităților de prelucrare a datelor	Această evidență este obligatorie prin lege, conform Articolului 30 din GDPR. Aceasta indică ce date cu caracter personal deține școala dumneavoastră, motivul pentru care le deține, cine le poate accesa și pentru ce perioadă sunt păstrate. În cazul în care autoritatea de supraveghere o solicită, trebuie să puteți să o prezentați.	Registrul trebuie să acopere fiecare categorie de date cu caracter personal prelucrate de școală: dosarele elevilor, datele de contact ale părinților, datele personalului, informațiile medicale și alte categorii similare. Pentru fiecare categorie, înregistrați scopul, temeiul juridic, persoanele care au acces, durata de stocare și procedura aplicată atunci când datele nu mai sunt necesare. DPO-ul este responsabil pentru menținerea la zi a acestui registru.
Colectați doar datele de care aveți într-adevăr nevoie	Fiecare informație cu caracter personal pe care o colectați reprezintă un risc. În cazul unei încălcări a securității, doar datele pe care le dețineți efectiv pot fi expuse. De asemenea, colectarea mai multor date decât este necesar	Revizuiți toate formularele de colectare a datelor, procesele de înscriere și setările platformelor utilizate. Eliminați orice câmp care solicită informații de care școala nu are nevoie în mod real. În cazul în care o platformă cere mai multe date decât este necesar, solicitați ajustarea acesteia de către furnizor sau alegeți o altă soluție. Stabiliți ca regulă

Ce presupune	De ce este important	Cum se procedează
	implică mai mult efort de administrare și un potențial crescut de neconformitate.	generală dezactivarea implicită a colectării de date opționale.
Încheiați acorduri cu fiecare furnizor care prelucrează datele elevilor	Atunci când o societate prelucrează date ale elevilor sau ale personalului în numele dumneavoastră — de exemplu, o platformă cloud, un instrument de evaluare sau o aplicație de comunicare — școala dumneavoastră rămâne responsabilă din punct de vedere legal pentru modul în care sunt gestionate aceste date. În lipsa unui acord scris, nu puteți demonstra că v-ați îndeplinit obligațiile legale.	Înainte ca orice furnizor să pună în funcțiune un serviciu care implică date cu caracter personal, acesta trebuie să semneze un Acord de Prelucrare a Datelor (DPA). Acest document trebuie să precizeze clar ce date sunt prelucrate, în ce scop, ce măsuri de securitate sunt aplicate și ce se întâmplă cu datele la încetarea contractului. Păstrați copii ale tuturor acordurilor în arhiva instituției.
Restricționați accesul la datele cu caracter personal	Cu cât mai multe persoane au acces la date, cu atât este mai mare riscul ca acestea să fie utilizate necorespunzător, divulgate accidental sau furate. Fiecare punct de acces inutil reprezintă o vulnerabilitate.	Configurați accesul pe bază de roluri, astfel încât fiecare membru al personalului să poată vizualiza doar datele necesare îndeplinirii atribuțiilor sale specifice. Un cadru didactic trebuie să aibă acces doar la dosarele propriilor elevi, nu la cele ale întregii școli. Personalul administrativ trebuie să acceseze date administrative, fără a avea acces la fișele medicale sau psihologice. Reevaluați drepturile de acces cel puțin o dată pe an și revocați-le imediat în cazul schimbării funcției sau al încetării raporturilor de muncă.
Informați elevii și părinții cu privire la modul în care le sunt utilizate datele	Elevii și părinții au dreptul legal de a ști ce date sunt deținute despre ei și cum sunt utilizate acestea. Furnizarea acestor informații nu este opțională. De asemenea, școlile care sunt transparente în privința utilizării datelor au tendința de a înregistra mai puține dispute și plângeri.	Redactați o notă de informare privind confidențialitatea într-un limbaj clar, pe care orice părinte sau elev mai mare să o poată înțelege. Aceasta trebuie să explice ce date sunt colectate, scopul colectării, cine are acces la ele și durata stocării. Furnizați această notă la înscrierea elevilor și ori de câte ori intervin modificări semnificative. Asigurați-vă că este disponibilă permanent, de exemplu pe site-ul web al școlii. Un model de scrisoare este disponibil în Anexa II.

Ce presupune	De ce este important	Cum se procedează
Obțineți consimțământul părinților pentru elevii care nu au atins vârsta consimțământului digital	Pentru elevii care nu au atins vârsta consimțământului digital prevăzută de legislația națională, nu îi puteți înregistra pe o platformă digitală fără acordul scris al unui părinte sau tutore. Aceasta este o cerință legală. Vârsta variază între 13 și 16 ani în cele cinci țări, ceea ce înseamnă că aceeași platformă poate necesita consimțământ într-o țară, dar nu și în alta.	Stabiliți un proces clar pentru colectarea, înregistrarea și reînnoirea consimțământului parental. Consimțământul trebuie să fie specific pentru fiecare platformă, acordat în mod liber și ușor de retras. Nu presupuneți că semnarea unui formular general de înscriere acoperă toate platformele digitale. Verificați vârsta consimțământului digital specifică țării dumneavoastră în Partea a 2-a.
Raportați încălcările securității datelor în termen de cel mult 72 de ore	Termenul limită de 72 de ore este o cerință legală strictă. Dacă școala dumneavoastră descoperă o încălcare a securității datelor și nu o raportează la timp, sau încearcă să o gestioneze în discreție fără a informa autoritatea de supraveghere, consecințele pot fi semnificativ mai grave decât dacă încălcarea ar fi fost raportată prompt.	Stabilirea în scris a unei proceduri de răspuns la încălcările securității datelor este obligatorie înainte de producerea oricărui incident. În cazul apariției unei încălcări, Responsabilul cu Protecția Datelor (DPO) trebuie să evalueze imediat dacă aceasta generează un risc pentru persoanele fizice. În caz afirmativ, Autoritatea Națională de Supraveghere trebuie notificată în termen de cel mult 72 de ore. Dacă riscul este ridicat, persoanele afectate trebuie, de asemenea, informate direct. Utilizați registrul de incidente din Anexa IV pentru a înregistra fiecare etapă.

Ce este o breșă de securitate a datelor?

O breșă de securitate a datelor este orice incident care duce la pierderea, distrugerea, modificarea, divulgarea sau accesarea accidentală ori ilegală a datelor cu caracter personal de către o persoană neautorizată. Aceasta include pierderea unui stick USB care conține dosarele elevilor, trimiterea unui e-mail către o persoană greșită, un atac de tip ransomware care blochează datele școlii sau o configurare incorectă a unei platforme, care face ca datele elevilor să devină publice din greșeală. Multe dintre cele mai frecvente breșe din școli sunt cauzate de erori umane, nu de atacuri cibernetice externe.

3.2 Menținerea securității sistemelor școlare

Securitatea cibernetică înseamnă protejarea calculatoarelor, a rețelelor și a datelor școlii împotriva atacurilor și a accesului neautorizat. Școlile reprezintă o țintă atractivă pentru infractorii cibernetici, deoarece dețin date sensibile despre copii și au adesea resurse de securitate limitate. Un atac reușit poate bloca sistemele școlii, poate expune dosarele elevilor, poate întrerupe procesul de învățământ timp de săptămâni întregi și poate aduce daune durabile reputației școlii.

Vestea bună este că majoritatea atacurilor cibernetice reușite exploatează vulnerabilități simple, care pot fi remediate fără cunoștințe de specialitate sau bugete mari. Parolele slabe, software-ul neactualizat, personalul care nu recunoaște e-mailurile de phishing și lipsa copiilor de siguranță (backup) stau în spatele celor mai multe incidente. Remedierea acestor lucruri de bază face o diferență uriașă.

La fel de importantă este pregătirea pentru momentul în care ceva nu merge bine. Existența unui backup testat și a unei proceduri clare de recuperare face diferența între o întrerupere care durează câteva ore și una care durează săptămâni întregi. Aceasta este viziunea din spatele planificării continuității activității: nu doar prevenirea incidentelor, ci asigurarea faptului că școala poate continua să funcționeze și se poate recupera rapid atunci când acestea au loc.

Ce presupune	De ce este important	Cum se procedează
Utilizați parole puternice și autentificarea cu mai mulți factori.	Parolele slabe reprezintă cea mai frecventă cale prin care atacatorii obțin acces în sistemele școlare. O parolă ușor de ghicit sau una utilizată pentru mai multe conturi înseamnă că o singură parolă compromisă îi poate oferi unui atacator acces complet. Autentificarea cu factori multipli adaugă un nivel suplimentar de verificare, protejând conturile chiar și în cazul în care o parolă a fost furată.	Toate conturile personalului trebuie să utilizeze parole complexe de cel puțin 12 caractere, care combină litere, cifre și simboluri. Parolele trebuie schimbate imediat dacă există vreun motiv de a suspecta că au fost compromise. Autentificarea cu factori multipli (MFA) trebuie activată pentru toate sistemele care conțin date ale elevilor. După introducerea parolei, membrul personalului trebuie să își confirme identitatea printr-o a doua metodă, cum ar fi un cod trimis pe telefonul mobil.
Păstrați toate programele software și dispozitivele actualizate.	Actualizările software includ frecvent remedieri pentru vulnerabilitățile de securitate pe care atacatorii le exploatează în mod activ. Multe dintre cele mai grave atacuri de tip ransomware asupra instituțiilor de învățământ au vizat sisteme care rulau software învechit, neactualizat. Aceasta este una dintre vulnerabilitățile cel mai ușor de prevenit.	Configurați un program regulat pentru aplicarea actualizărilor pe toate dispozitivele, sistemele de operare, aplicațiile și programele de securitate ale școlii. Aplicați patch-urile critice de securitate de îndată ce sunt disponibile. Dacă un dispozitiv nu mai poate primi actualizări, deconectați-l din rețea sau înlocuiți-l. Desemnați un membru specific al personalului care să fie responsabil pentru efectuarea actualizărilor.
Efectuați în mod regulat copii de siguranță pentru toate datele importante.	Atacurile de tip ransomware funcționează prin criptarea datelor dumneavoastră și solicitarea unei plăți pentru restaurarea accesului. Singura modalitate sigură de recuperare fără a plăti este	Configurați copii de siguranță (backup) zilnice automate pentru toate datele critice ale școlii. Păstrați cel puțin o copie a fiecărei salvări într-o locație neconectată la rețeaua principală a școlii, astfel încât aceasta să nu poată fi criptată în cazul unui atac concomitent. Testați procesul de recuperare cel puțin o dată pe an pentru a

Ce presupune	De ce este important	Cum se procedează
	existența unei copii de siguranță create înainte de atac. Fără o copie de siguranță testată, o școală poate pierde săptămâni de muncă și înregistrări permanente.	confirma că salvările funcționează efectiv și că datele pot fi restaurate într-un timp rezonabil.
Utilizați rețele separate pentru administrație și elevi.	Dacă rețeaua utilizată de personalul administrativ, unde sunt gestionate dosarele și notele elevilor, este aceeași cu cea utilizată de elevi și vizitatori, un dispozitiv compromis al unui elev sau un laptop infectat al unui vizitator ar putea accesa sistemele administrative ale școlii. Aceasta este un risc de bază pe care separarea rețelelor îl elimină.	Configurați rețele Wi-Fi separate: una pentru uz administrativ și una pentru elevi și vizitatori. Asigurați-vă că rețeaua administrativă nu este vizibilă sau accesibilă din rețeaua elevilor. Configurați controale de acces, astfel încât doar dispozitivele școlare autorizate să se poată conecta la rețeaua administrativă.
Protejați toate dispozitivele școlii.	Dispozitivele care au parole implicite din fabrică, nu au fost actualizate niciodată sau nu au un soft antivirus instalat sunt ținte ușoare. Multe școli au în sălile de clasă sau în birouri dispozitive care au fost configurate cu ani în urmă și nu au mai fost reevaluate de atunci.	Instalați programe software antivirus și antimalware pe toate dispozitivele școlii și păstrați-le actualizate. Schimbați toate parolele implicite ale routerelor, camerelor, imprimantelor și ale oricărui alt echipament conectat imediat după instalare. Efectuați un audit regulat al tuturor dispozitivelor conectate. Înainte de a elimina echipamentele vechi, asigurați-vă că toate datele au fost șterse definitiv și în siguranță.
Pregătiți un plan scris pentru gestionarea incidentelor.	Fără un plan scris, personalul care se confruntă cu un atac cibernetic nu va ști ce măsuri să ia. Deciziile luate din panică sau bine intenționate, dar greșite — cum ar fi oprirea imediată a unui dispozitiv sau încercarea de a plăti o răscumpărare — pot agrava considerabil o situație deja critică.	Redactați o procedură de răspuns la incidentele de securitate cibernetică care să stabilească persoana/echipa care coordonează răspunsul, pașii de urmat și ordinea acestora, autoritățile naționale care trebuie contactate și termenul limită aferent, precum și modul de comunicare cu elevii, părinții și personalul în timpul și după producerea unui incident. Asigurați-vă că tot personalul relevant cunoaște procedura înainte de apariția unui incident. Un model este furnizat în Anexa IV.
Instruiți întregul personal cel puțin o dată pe an.	E-mail-urile de tip phishing stau la baza majorității atacurilor cibernetice de	Asigurați instruirea anuală obligatorie privind conștientizarea securității cibernetice pentru întregul personal. Instruirea trebuie să acopere

Ce presupune	De ce este important	Cum se procedează
	succes asupra școlilor. Un membru al personalului care nu poate identifica un email de phishing reprezintă o vulnerabilitate împotriva căreia niciun sistem tehnic nu poate oferi protecție deplină. Un singur clic pe un link malițios poate oferi unui atacator acces complet la sistemele școlii.	modul de identificare a unui e-mail de phishing, modul de creare și gestionare a parolelor puternice, acțiunile necesare în cazul pierderii sau furtului unui dispozitiv și persoana de contact în cazul în care ceva pare suspect. Adăugați mementouri periodice pe parcursul anului. Acolo unde este posibil, desfășurați exerciții de simulare a phishing-ului: acestea reprezintă una dintre cele mai eficiente metode de a schimba comportamentul personalului.

Ce este un atac de tip phishing?

Phishing-ul este o metodă prin care un atacator trimite un e-mail, un mesaj sau o notificare ce pare să vină din partea unei persoane sau instituții de încredere, cum ar fi Ministerul Educației, un furnizor de software sau un coleg. Scopul este de a convinge destinatarul să dea click pe un link dăunător, să-și introducă datele de autentificare pe un site fals sau să deschidă un fișier infectat. Phishing-ul este cea mai frecventă formă de atac cibernetic îndreptată împotriva școlilor. Orice mesaj neașteptat prin care se solicită o parolă, se cere accesarea urgentă a unui link sau se solicită o acțiune neobișnuită trebuie privit cu suspiciune și verificat printr-un canal separat înainte de a oferi un răspuns.

3.3 Alegerea și utilizarea în siguranță a platformelor digitale

Școlile folosesc un număr tot mai mare de platforme digitale pentru predare, comunicare și administrație. Fiecare platformă care prelucrează datele elevilor reprezintă o potențială sursă de risc. O platformă care are o securitate slabă, care distribuie date către companii de publicitate sau care stochează informațiile elevilor în afara UE fără garanții adecvate poate provoca daune reale. Școlile au obligația legală de a verifica platformele înainte de a le adopta și de a le gestiona cu atenție odată ce sunt puse în funcțiune.

Același lucru este valabil și pentru instrumentele bazate pe inteligență artificială. IA este din ce în ce mai prezentă în educație, însă nu toate instrumentele pot fi utilizate în siguranță cu elevii. Legea privind inteligența artificială adoptată la nivelul UE (EU AI Act) trasează limite clare, iar școlile trebuie să știe unde se află aceste limite înainte de a introduce orice instrument de IA în clasă sau în procesele care îi afectează pe elevi.

Ce presupune	De ce este important	Cum se procedează
Verificați fiecare platformă înainte de a o utiliza	O platformă adoptată fără verificări adecvate poate prelucra datele elevilor fără acordul școlii, le poate stoca în afara UE	Înainte de a adopta o nouă platformă, verificați dacă aceasta respectă GDPR, dacă nu utilizează datele elevilor în scopuri publicitare, nu le transmite terților fără consimțământ și le stochează în interiorul

Ce presupune	De ce este important	Cum se procedează
	sau poate avea vulnerabilități de securitate. Odată ce datele au fost transmise unui furnizor necorespunzător, situația este foarte greu de remediat.	UE. Dacă platforma implică prelucrarea pe scară largă a datelor elevilor, efectuați o evaluare a impactului asupra protecției datelor (DPIA) înainte de lansare (consultați Anexa V). Semnați un acord de prelucrare a datelor cu furnizorul înainte de partajarea oricăror date.
Mențineți o listă a platformelor aprobate	Fără o evidență centralizată, școlile pierd controlul asupra platformelor folosite, a datei ultimei verificări sau a persoanei care le-a aprobat. Personalul le poate utiliza neoficial, fără nicio evaluare, iar elevii pot folosi conturi personale pe instrumente neaprobate pentru teme, scăzând datele aflate în controlul școlii.	Păstrați un registru scris al tuturor platformelor și instrumentelor digitale aprobate pentru utilizare în școala dumneavoastră. Înregistrați numele platformei, scopul utilizării, data la care a fost evaluată și data următoarei revizuiri. Revizuiți registrul cel puțin o dată pe an. Personalul nu trebuie să introducă platforme noi pentru uz școlar fără a parcurge mai întâi procesul de aprobare.
Configurați platformele în mod securizat	Setările implicite ale platformelor sunt concepute de obicei pentru ușurința utilizării, nu pentru securitate. O clasă virtuală la care oricine se poate conecta fără autentificare, o funcție de înregistrare activată implicit sau conturi de elevi cu permisiuni excesive generează riscuri ușor de evitat.	Fiecare platformă trebuie configurată în siguranță înainte ca elevii sau personalul să înceapă să o utilizeze. Instrumentele de videoconferință trebuie să solicite autentificarea înainte ca cineva să se poată alătura unei clase virtuale. Înregistrarea trebuie să fie dezactivată în mod implicit și activată doar cu consimțământul explicit al tuturor celor prezenți. Conturile elevilor ar trebui să aibă doar permisiunile necesare activităților lor educaționale. Verificați setările cel puțin o dată pe an.
Cunoașteți utilizările interzise ale IA	Unele practici privind inteligența artificială în mediul educațional sunt interzise de legislația UE. Acest lucru este valabil indiferent de modul în care instrumentul a fost promovat sau de ceea ce susține furnizorul. Interdicția este absolută și	Nu utilizați niciun instrument de IA care implică recunoașterea emoțiilor elevilor, clasificarea biometrică a acestora sau identificarea lor în timp real prin recunoaștere facială. Aceste utilizări sunt interzise în temeiul articolului 5 din Legea privind inteligența artificială a UE. Dacă un furnizor oferă aceste funcționalități, școala nu trebuie să le utilizeze. Dacă școala

Ce presupune	De ce este important	Cum se procedează
	se aplică tuturor școlilor din toate cele cinci țări.	folosește deja un astfel de instrument, trebuie să înceteze utilizarea acestuia.
Păstrați factorul uman la comanda deciziilor privind elevii	Instrumentele de IA pot genera recomandări eronate, părtinitoare sau incorecte. Când aceste recomandări influențează parcursul unui elev — cum ar fi o notă, o evaluare disciplinară sau o evaluare a nevoilor de învățare — consecințele pot fi grave. Tocmai din acest motiv, legea impune ca decizia finală să aparțină întotdeauna unui om.	Un cadru didactic sau un adult responsabil trebuie să verifice întotdeauna și să își asume responsabilitatea pentru orice rezultat generat de un instrument de IA care afectează un elev. Instrumentele de IA pot oferi asistență, dar nu pot lua decizii finale. Documentați modul în care este aplicată supravegherea umană pentru fiecare instrument de IA utilizat în luarea deciziilor educaționale.
Informați elevii și părinții atunci când se utilizează IA	Elevii și părinții au dreptul de a ști când sunt utilizate instrumente de IA în moduri care le afectează parcursul educațional. Folosirea acestor instrumente fără a-i informa constituie, cel mai probabil, o încălcare atât a Actului privind IA, cât și a GDPR.	Atunci când un instrument de IA este utilizat într-un mod care afectează învățarea sau evaluarea unui elev, informați clar și într-un limbaj simplu elevii și părinții: ce face instrumentul, ce date utilizează, cum sunt folosite rezultatele sale și cum funcționează supravegherea umană. Furnizați aceste informații înainte de utilizarea instrumentului și păstrați-le permanent accesibile.
Păstrați o evidență a tuturor instrumentelor IA utilizate.	Școlile care nu cunosc instrumentele de IA pe care le folosesc, datele pe care acestea le prelucrează sau evaluările făcute înainte de adoptare nu-și pot îndeplini obligațiile legale prevăzute de Legea privind IA sau GDPR. .	Mențineți un registru al instrumentelor de IA ca parte a listei dumneavoastră de platforme aprobate. Pentru fiecare instrument de IA, înregistrați ce face, în ce categorie de risc se încadrează conform Legea privind IA, ce date prelucrează, ce evaluare a fost efectuată înainte de adoptare și cine este responsabil de supraveghere. Revizuiți această evidență cel puțin o dată pe an.

3.4 Gestionarea telefoanelor mobile și a dispozitivelor personale

Toate cele cinci țări partenere au introdus restricții legale privind utilizarea telefoanelor mobile în școli. Regulile specifice diferă de la o țară la alta (a se vedea Partea 2), însă motivele sunt aceleași peste tot: telefoanele din sălile de clasă le distrag elevilor atenția de la învățare, creează riscuri pentru confidențialitatea și protecția datelor, facilitează hărțuirea cibernetică (cyberbullying) și sporesc presiunea digitală care afectează sănătatea mintală a elevilor.

O politică privind utilizarea telefoanelor mobile reprezintă mai mult decât o simplă regulă disciplinară. Este o măsură de protecție a datelor, o măsură pentru starea de bine și o declarație privind valorile școlii. O politică redactată clar, înțeleasă cu adevărat de elevi, părinți și cadre didactice și aplicată în mod consecvent este mult mai eficientă decât una care există doar pe hârtie.

Ce presupune	De ce este important	Cum se procedează
Adoptați o politică scrisă clară privind utilizarea telefoanelor mobile.	Fără o politică scrisă, profesorii aplică regulile în mod diferit. Nu le poți cere elevilor și părinților să respecte reguli care nu le-au fost aduse clar la cunoștință. Aplicarea inconsecventă creează conflicte și subminează încrederea în regulamentul școlii.	Adoptați o politică clară privind utilizarea telefoanelor mobile în spațiul școlar, bine structurată și transparentă. Specificați clar momentele și zonele în care utilizarea acestora este permisă sau interzisă, stabilind totodată spațiul exact pentru depozitarea lor pe durata orelor sau a perioadelor cu restricții (de exemplu: dulapuri individuale, cutii dedicate în clasă sau în ghiozdane, pe modul silențios ori oprit). De asemenea, definiți clar excepțiile permise — cum ar fi cerințele medicale specifice sau activitățile didactice ghidate de profesori — și clarificați consecințele disciplinare aplicate gradual în cazul nerespectării regulilor. .
Interziceți utilizarea telefoanelor mobile în timpul orelor de curs	Utilizarea nerestricționată a telefonului în timpul orelor perturbă procesul de învățare, creează oportunități pentru hărțuire cibernetică și înregistrări neautorizate și sporește presiunile digitale care afectează starea de bine a elevilor. Cercetările arată în mod constant că elevii din școlile cu restricții clare privind telefoanele au rezultate academice mai bune și raportează un nivel mai ridicat al stării de bine.	Elevii nu trebuie să folosească telefoanele mobile personale în timpul orelor, cu excepția cazului în care cadrul didactic a autorizat în mod specific utilizarea lor pentru o anumită activitate educațională. În țările în care există o interdicție legală, aceasta trebuie aplicată strict. Specificați clar unde trebuie depozitate telefoanele în perioadele cu restricții și asigurați-vă că excepțiile permise pentru nevoi medicale sunt documentate corespunzător.
Interziceți înregistrările neautorizate	Înregistrările neautorizate ale elevilor, cadrelor didactice sau altor membri ai personalului constituie o încălcare gravă a confidențialității și pot reprezenta o infracțiune conform legislației	Clarificați ferm pentru elevi și cadrele didactice faptul că înregistrarea oricărei persoane în spațiul școlar fără consimțământul explicit al acesteia este strict interzisă, fie că are loc în timpul orelor, pe coridoare, în excursii sau la evenimente. Specificați în mod clar consecințele aplicabile și tratați orice înregistrare neautorizată care implică elevi sau

Ce presupune	De ce este important	Cum se procedează
	naționale. Înregistrările distribuite în mediul online pot cauza daune de durată persoanelor implicate și școlii. Popularitatea platformelor de videoclipuri scurte face ca acesta să fie un risc tot mai mare.	personalul școlii ca pe o abatere disciplinară gravă, iar unde este necesar, direcționați cazul către autoritățile competente.
Aplicați cerințele de securitate pe dispozitivele personale folosite pentru activitățile școlare.	Când un profesor folosește un dispozitiv personal pentru a accesa sistemele școlii, protecția datelor depinde direct de cel mai slab element. Un dispozitiv personal cu o parolă slabă, un software neactualizat sau date ale elevilor stocate local reprezintă o vulnerabilitate reală.	Garantarea securității datelor este esențială: personalul care folosește dispozitive personale în scop didactic trebuie să le protejeze cu o parolă sau un cod PIN puternic, să mențină aplicațiile actualizate, să utilizeze o conexiune securizată când lucrează de la distanță și să nu stocheze datele elevilor local pe aceste echipamente. Oferiți instrucțiuni clare cadrelor didactice și personalului școlar cu privire la cerințele și așteptările pe care trebuie să le respecte.

3.5 Prevenirea și combaterea hărțuirii cibernetice (cyberbullying)

Hărțuirea cibernetică (*cyberbullying*) este o formă de hărțuire care are loc prin intermediul dispozitivelor și platformelor digitale. Aceasta include trimiterea de mesaje amenințătoare sau umilitoare, distribuirea de imagini private fără consimțământ, răspândirea de informații false în mediul online și excluderea deliberată a cuiva din grupuri virtuale. Cyberbullying-ul poate provoca daune grave și de lungă durată sănătății mintale a elevilor, rezultatelor școlare și relațiilor sociale ale acestora.

Școlile au atât o obligație legală, cât și o îndatorire morală de a preveni hărțuirea cibernetică și de a interveni atunci când aceasta se produce. Cyberbullying-ul nu se oprește la poarta școlii. Ceea ce se întâmplă online, acasă, în timpul serii, poate afecta starea elevului la școală a doua zi dimineață și invers. Școlile trebuie să trateze hărțuirea cibernetică cu aceeași seriozitate ca pe cea fizică, chiar și atunci când are loc în afara orelor de program.

Ce presupune	De ce este important	Cum se procedează
Includeți explicit hărțuirea cibernetică (*cyberbullying*) în politica anti-bullying a școlii	O politică generală de prevenire a violenței care nu menționează explicit hărțuirea cibernetică lasă loc de incertitudini cu privire la gestionarea comportamentului din	Actualizați politica anti-bullying prin introducerea unei secțiuni dedicate hărțuirii cibernetice (*cyberbullying*). În cadrul acesteia, definiți clar ce constituie o agresiune în mediul virtual și asigurați-vă că este tratată cu aceeași gravitate ca violența fizică. Extindeți aria de aplicabilitate a regulamentului astfel încât să acopere și

Ce presupune	De ce este important	Cum se procedează
	mediul online. Elevii agresați în spațiul virtual pot ezita să raporteze incidentele, considerând că școala va declina responsabilitatea pe motiv că problema nu intră în competența sa.	comportamentul online din afara orelor de curs, atunci când acesta are un impact direct asupra comunității școlare. Nu în ultimul rând, evaluați și revizuiți periodic acest cadru de reguli, cel puțin o dată pe an, pentru a-i menține eficiența.
Educați elevii cu privire la fenomenul hărțuirii cibernetice (*cyberbullying*).	Elevii care înțeleg ce este hărțuirea cibernetică, de ce provoacă suferință și cum trebuie să reacționeze atunci când asistă la un astfel de fenomen sunt mult mai dispuși să raporteze incidentele și să își sprijine colegii vizați. Formarea elevilor pentru a deveni martori activi și empatici reprezintă una dintre cele mai eficiente strategii de intervenție.	Integrați educația privind hărțuirea cibernetică direct în curriculum, oferind lecții regulate și adaptate vârstei elevilor, în locul unor evenimente izolate. Diversificați tematica abordată prin discutarea manifestărilor din mediul online, a efectelor nocive ale acesteia, dar și a modalităților concrete de sprijin și raportare. Totodată, implicați activ elevii în crearea materialelor educaționale; consultarea lor va crește semnificativ gradul de receptivitate și asumare față de mesajele transmise.
Oferiți elevilor un canal de raportare clar, accesibil și securizat pentru cazurile de hărțuire cibernetică.	Mulți elevi supuși hărțuirii cibernetice ezită să raporteze incidentele de teamă că nu vor fi crezuți, că situația se va agrava ori că le vor fi confiscate dispozitivele tehnologice. În lipsa unui canal de raportare accesibil și bazat pe încredere, aceste situații rămân invizibile și tind să se intensifice în timp.	Oferiți mai multe modalități de raportare a hărțuirii cibernetice: un adult de încredere, un formular sau o cutie anonimă și, unde este disponibilă, platforma națională de raportare (vezi Partea a 2-a). Promovați activ aceste opțiuni pe parcursul întregului an școlar, nu doar în luna septembrie. Când un elev raportează un incident, răspundeți rapid și lăsați să se înțeleagă clar că tratați situația cu toată seriozitatea.
Formați întregul personal pentru a recunoaște și a reacționa la hărțuirea cibernetică.	Mulți profesori nu sunt siguri cum să reacționeze la hărțuirea cibernetică, în special atunci când aceasta implică platforme cu care nu sunt familiarizați. Nesiguranța duce la răspunsuri inconsecvente, care subminează atât victima,	Oferiți întregului personal instruire care să acopere modul de identificare a semnelor că un elev ar putea fi victima hărțuirii cibernetice, care este procedura școlii și care este rolul lor în cadrul acesteia, cum să păstreze dovezile, inclusiv capturile de ecran, când să implice consilierul școlar, părinții sau autoritățile externe și cum să sprijine un elev fără a înrăutăți din greșeală lucrurile.

Ce presupune	De ce este important	Cum se procedează
	cât și capacitatea școlii de a gestiona eficient incidentele.	
Răspundeți rapid și documentați totul.	Un răspuns lent sau inconsecvent transmite mesajul că școala nu tratează hărțuirea cibernetică cu seriozitate. De asemenea, acesta permite escaladarea incidentelor și pierderea dovezilor. Școlile care nu păstrează dovezi adecvate consideră că este greu să identifice tipare sau să probeze faptul că au acționat corespunzător, în cazul în care se face o plângere formală.	Când este raportat un incident de hărțuire cibernetică, acordă prioritate absolută siguranței elevului vizat. Notează imediat detaliile: data și ora, ce s-a întâmplat, platformele implicate, persoanele implicate, dovezile colectate și fiecare măsură luată. Aplică procedura disciplinară în mod consecvent. Menține legătura cu elevul vizat în zilele și săptămânile de după incident, pentru a-i verifica starea.
Implicați părinții ca parteneri.	Părinții care înțeleg fenomenul de hărțuire online (cyberbullying), știu cum să discute cu copiii lor despre acest subiect și sunt la curent cu abordarea școlii sunt mult mai eficienți atât în prevenirea incidentelor, cât și în sprijinirea copiilor atunci când astfel de situații au loc.	Informați părinții la începutul anului școlar cu privire la strategia școlii privind hărțuirea online, pașii de urmat în cazul în care copilul lor este afectat și modul în care școala va comunica cu ei. Folosiți modelul din Anexa II. Când au loc incidente, implicați părinții tuturor elevilor afectați, respectând procedurile școlii.

Școlile nu trebuie să se confrunte singure cu aceste provocări. Ziua Siguranței pe Internet (*Safer Internet Day* - organizată în februarie) și Luna Europeană a Securității Cibernetice (*European Cybersecurity Month* - în octombrie) pun la dispoziția școlilor materiale de conștientizare gata de utilizare, validate la nivelul Uniunii Europene. Programul UE „Un internet mai bun pentru copii" (*Better Internet for Kids - BIK+*) și rețeaua *Insafe* a Centrelor pentru un Internet mai Sigur operează linii telefonice de asistență (*helplines*), instrumente de raportare și resurse educaționale în toate cele cinci țări partenere, pe care școlile le pot folosi în mod direct.

3.6 Sprijinirea stării de bine digitale a elevilor

Elevii se confruntă în mediul online cu riscuri care depășesc sfera hărțuirii cibernetice (*cyberbullying*) și a breșelor de date. Mulți dintre ei experimentează anxietate, o stimă de sine scăzută și o presiune socială puternică legate de viața lor digitală. Teama de a nu rata ceva (*Fear of Missing Out - FOMO*), presiunea de a prezenta o imagine idealizată a propriei persoane pe internet, compararea continuă cu ceilalți, timpul

excesiv petrecut în fața ecranelor și modul de proiectare a rețelelor sociale - care prioritizează fidelizarea în detrimentul stării de bine - contribuie la probleme de sănătate mentală ce afectează un număr semnificativ de tineri.

Simpla restricționare a accesului nu rezolvă aceste probleme. Elevii cărora li se cere doar să folosească mai puțin tehnologia, fără a fi ajutați să înțeleagă motivul sau fără a primi instrumente pentru a-și gestiona propriul comportament, tind să revină la vechile obiceiuri de îndată ce restricțiile sunt ridicate. Școlile care obțin schimbări pozitive de durată sunt cele care combină regulile clare cu o educație onestă, bazată pe dovezi, și cu o cultură în care elevii se simt în siguranță să vorbească deschis despre experiențele lor din mediul online.

Ce presupune	De ce este important	Cum se procedează
Consolidați siguranța online a elevilor prin intermediul serviciilor de consiliere și suport	Elevii care întâmpină dificultăți în mediul online se confruntă, de fapt, cu probleme privind sănătatea mintală și integrarea socială în ansamblu. Dacă bunăstarea digitală este tratată ca un subiect izolat de domeniul IT, elevii care au nevoie de sprijin pot fi scăpați din vedere din cauza lipsei de coordonare dintre servicii.	Bunăstarea digitală ar trebui să fie o parte distinctă a programului mai larg al școlii dedicat stării de bine și consilierii elevilor. Pregătiți personalul didactic care sprijină elevii în depășirea altor provocări să le ofere ajutor și în privința dificultăților din spațiul cibernetic. Stabilirea unor proceduri clare de îndrumare este esențială: asigurați-vă că orice cadru didactic care identifică un elev aflat în dificultate știe exact cui să se adreseze și care sunt pașii următori.
Formați elevilor deprinderi de utilizare responsabilă a tehnologiei	Elevii care înțeleg modul în care platformele de social media sunt concepute pentru a-i ține conectați în permanență, care pot face diferența între o imagine din mediul online atent selectată și realitate și care și-au dezvoltat propriile strategii de gestionare a obiceiurilor digitale sunt mai bine pregătiți să navigheze în siguranță în lumea online.	Includeți educația privind starea de bine în mediul digital ca parte integrantă a curriculumului. Învățați-i pe elevi cum funcționează algoritmii de recomandare și de ce aceștia afișează adesea conținut care declanșează emoții puternice. Discutați despre efectele pe care navigarea pasivă pe rețelele de socializare le are asupra stării de spirit și a stimei de sine. Ajutați-i pe elevi să își dezvolte strategii practice pentru a stabili limite clare în ceea ce privește propria utilizare a tehnologiei.
Asigurați-vă că elevii știu unde pot găsi ajutor	Mulți elevi care se confruntă cu dificultăți în mediul online nu cer ajutor deoarece nu știu că există sprijin disponibil, le este rușine sau se tem că li se va lua telefonul. Dacă opțiunile de sprijin nu sunt	Reamintiți-le în mod regulat elevilor la cine pot apela dacă ceva din mediul online îi deranjează. Menționați acest lucru în cadrul activităților școlare, la ore și în interacțiunile de zi cu zi, nu doar într-un ghid sau regulament. Persoana la care apelează un elev nu trebuie să fie un expert în tehnologie; trebuie doar să fie cineva în care

Ce presupune	De ce este important	Cum se procedează
	promovate în mod activ, ele rămân invizibile pentru elevii care au cea mai mare nevoie de ele.	elevul are încredere, cineva care îl va asculta fără să îl judece și îl va îndruma către sprijinul adecvat.
Nu amplificați presiunea digitală prin practicile adoptate de școală	Școlile pot crea, fără să își dea seama, exact aceleași presiuni digitale pe care încearcă să le reducă. Grupurile de chat obligatorii ale școlii, cerința ca elevii să răspundă la mesaje în afara orelor de curs și compararea publică a elevilor pe internet pot transmite mesaje dăunătoare.	Analizați modul în care școala comunică în mediul digital și dacă propriile practici contribuie la presiunea digitală. Evitați grupurile de chat obligatorii care estompează limita dintre timpul alocat școlii și cel personal. Nu aveți așteptarea ca elevii sau părinții să răspundă la mesaje în afara orelor normale de program. Evitați publicarea de clasamente sau comparații în mediul online.
Recunoașteți semnele când un elev se confruntă cu dificultăți	Elevii care întâmpină dificultăți în viața lor digitală s-ar putea să nu o spună în mod direct. Semnele sunt adesea comportamentale și ușor de trecut cu vederea, cu excepția cazului în care personalul școlar știe exact la ce să fie atent.	Oferiți cadrelor didactice instrucțiuni privind semnele care indică faptul că un elev s-ar putea confrunta cu dificultăți în viața sa digitală: anxietate neobișnuită atunci când nu își poate verifica telefonul, fluctuații de dispoziție în urma interacțiunilor online, retragere din activitățile sociale după un eveniment petrecut pe internet, stare de suferință legată de propriul aspect sau de modul în care este perceput online, ezitare în a veni la școală după un incident virtual sau orice alt semn că este presat ori vizat direct în mediul online. Când apar aceste semnalmente, personalul trebuie să urmeze procedura școlii privind consilierea și îndrumarea elevilor.

3.7 Diversitate, incluziune și echitate digitală

Nu toți elevii se confruntă cu aceleași riscuri digitale și nu toți au același acces la sprijin. Genul, orientarea sexuală, dizabilitățile, veniturile familiei și preocupările legate de imaginea corporală — toate influențează experiența online a unui elev și capacitatea acestuia de a primi ajutor atunci când ceva nu merge bine. O politică de securitate care funcționează bine pentru majoritatea elevilor, dar ignoră experiențele celorlalți, este o politică incompletă.

Construirea unei abordări incluzive a siguranței digitale înseamnă să analizăm activ care sunt elevii cei mai expuși riscurilor și să ne asigurăm că politicile școlii, programele educaționale și sistemele de sprijin ajung la ei.

Ce presupune	De ce este important	Cum se procedează
Abordați în mod explicit hărțuirea online bazată pe gen și pe identitate	Fetele se confruntă cu rate disproporționat de mari de hărțuire sexuală online, abuz bazat pe imagini și cyberbullying legat de aspectul fizic. Elevii LGBTQ+ au o probabilitate semnificativ mai mare de a suferi din cauza hărțuirii online și de a dezvolta, ca urmare, probleme de sănătate mintală. Cercetările arată că prevalența raportată a cyberbullying-ului în rândul elevilor LGBTQ+ variază considerabil: de la aproximativ 10% la peste 70%, în funcție de context, iar elevii LGBTQ+ raportează că sunt victime ale cyberbullying-ului la o rată de aproximativ două ori mai mare decât colegii lor heterosexuali. Studiile demonstrează că cyberbullying-ul explică din punct de vedere statistic o mare parte din nivelul ridicat de anxietate, depresie și singurătate raportat de elevii aparținând minorităților sexuale, ceea ce înseamnă că prevenția incluzivă reprezintă un mecanism central pentru protejarea sănătății mintale a acestui grup. O politică ce nu numește în mod explicit aceste forme specifice de abuz îi lasă pe cei mai vulnerabili elevi fără o protecție adecvată.	Actualizarea politicii anti-cyberbullying a școlii pentru a acoperi în mod explicit hărțuirea online bazată pe gen, hărțuirea sexuală, distribuirea de imagini intime fără consimțământ și hărțuirea pe criterii de orientare sexuală sau identitate de gen. Asigurarea că instruirea personalului acoperă aceste forme specifice de abuz și modul de reacție la acestea. Crearea unui mediu școlar în care fiecare elev se simte în egală măsură în siguranță să raporteze ceea ce i se întâmplă.
Asigurați accesibilitatea educației privind siguranța digitală pentru elevii cu dizabilități	Elevii cu dizabilități, inclusiv cei cu dificultăți de învățare, pot fi mai vulnerabili la manipulare și exploatare în mediul online. De asemenea, acestora le poate fi mai greu să acceseze resurse de educație privind siguranța digitală care nu sunt concepute având în vedere nevoile lor specifice. Dacă mecanismele de raportare nu le sunt accesibile, pentru acești elevi ele practic nu există.	Asigurați-vă că întreaga educație privind siguranța digitală este furnizată în modalități adecvate elevilor cu cerințe educaționale diferite. Verificați dacă platformele digitale utilizate în școală respectă standardele de accesibilitate. Asigurați-vă că mecanismele de raportare sunt accesibile elevilor care comunică în mod diferit. Colaborați cu personalul specializat în educație specială pentru a identifica elevii care ar putea avea nevoie de sprijin suplimentar în înțelegerea și gestionarea riscurilor din mediul online.

Ce presupune	De ce este important	Cum se procedează
Recunoașteți și abordați decalajul digital	Elevii din familii cu venituri reduse pot avea acces la internet limitat sau instabil acasă, dispozitive mai vechi ori folosite la comun și mai puțin sprijin din partea adulților în navigarea pe internet. Elevii care utilizează dispozitive partajate se confruntă cu riscuri mai mari privind confidențialitatea. De asemenea, este mai puțin probabil ca acești elevi să recunoască sau să raporteze problemele cu care se confruntă.	Nu proiectați activități digitale sau practici de comunicare care presupun un nivel de conectivitate la domiciliu de care nu toți elevii dispun. Țineți cont de faptul că elevii care folosesc dispozitive comune se confruntă cu riscuri specifice de confidențialitate și oferiți-le îndrumări clare. Asigurați-vă că educația privind siguranța digitală ajunge la toți elevii. Identificați elevii care nu au o conectivitate adecvată acasă și abordați această problemă prin intermediul programelor naționale disponibile.
Sprijiniți elevii să își dezvolte o gândire critică privind imaginea corporală în mediul online	Rețelele sociale îi expun în mod constant pe elevi la imagini editate și filtrate, care impun standarde de frumusețe nerealiste. Acest lucru este asociat cu o stimă de sine scăzută și anxietate, în special în rândul fetelor adolescente, iar în unele cazuri, cu tulburări de alimentație.	Includeți educația privind imaginea corporală și aspectul fizic în mediul online ca parte din curriculumul dedicat stării de bine digitale. Învățați-i pe elevi modul în care imaginile sunt editate și filtrate înainte de a fi postate și ajutați-i să înțeleagă că ceea ce văd pe internet este o reprezentare regizată, nu realitatea. Discutați despre modul în care algoritmii platformelor amplifică conținutul bazat pe aspectul fizic. Abordați acest subiect cu sensibilitate: unii elevi s-ar putea să se confrunte deja cu astfel de dificultăți. Asigurați-vă că există trasee clare de îndrumare către sprijin de specialitate.
Aplicarea unei perspective incluzive asupra întregii politici de siguranță digitală	O politică concepută fără a lua în considerare experiențele diferitelor grupuri de elevi va reflecta doar experiența majorității, lăsându-i pe ceilalți mai puțin protejați. Elevii care se confruntă cu cele mai mari riscuri online sunt adesea tocmai cei ale căror experiențe au fost cel mai puțin luate în calcul.	Parcurgeți fiecare secțiune a acestei politici și întrebați-vă: ajung aceste măsuri la elevii cei mai expuși riscurilor? Sunt canalele noastre de raportare accesibile tuturor? Acoperă instruirea personalului nostru vulnerabilitățile specifice ale diferitelor grupuri? Implicați elevii, inclusiv pe cei din grupuri subreprezentate, în revizuirea și îmbunătățirea abordării școlii cu privire la siguranța digitală.

Part 4: Ce spun studiile și cercetările

Această parte sintetizează ceea ce ne indică cercetările despre măsurile care funcționează cu adevărat atunci când școlile abordează securitatea cibernetică, hărțuirea pe internet (*cyberbullying*) și starea de bine digitală. Utilizați această secțiune pentru a lua decizii informate cu privire la programele, abordările și intervențiile pe care le adoptă școala dumneavoastră.

4.1 Conștientizarea și formarea în domeniul securității cibernetice

Cercetările privind securitatea cibernetică în școli identifică în mod consecvent comportamentul uman ca fiind cel mai important factor de risc. Majoritatea atacurilor de succes încep cu un e-mail de phishing sau o parolă slabă. Măsurile tehnice de protecție ajută, însă nu pot preveni un atac atunci când personalul nu este instruit să recunoască amenințarea. Acest lucru înseamnă că investiția în formarea personalului este cel puțin la fel de importantă ca investiția în instrumente tehnice.

Studiile privind instruirea personalului în domeniul securității cibernetice arată că sesiunile regulate și practice funcționează semnificativ mai bine decât o singură sesiune de conștientizare. Membrii personalului care beneficiază de formare anuală și de reamintiri periodice sunt măsurabil mai puțin dispuși să dea clic pe linkuri de phishing sau să folosească practici nesigure în sistemele școlare. De asemenea, modul de livrare a instruirii contează: sesiunile interactive cu exemple din viața reală funcționează mai bine decât citirea pasivă a informațiilor sau vizionarea unui videoclip.

Exercițiile de simulare a phishing-ului — în care personalul primește un e-mail fals creat cu atenție pentru a le testa reacția — se numără printre cele mai eficiente metode de formare disponibile. Școlile și organizațiile care derulează în mod regulat aceste exerciții observă îmbunătățiri clare în comportamentul personalului de-a lungul timpului. Exercițiul este cel mai eficient atunci când este urmat imediat de feedback, explicându-se care au fost indiciile și care ar fi trebuit să fie reacția corectă.

În ceea ce privește elevii, cercetările arată că educația privind securitatea cibernetică funcționează cel mai bine atunci când este integrată în curriculum, în loc să fie livrată ca un eveniment izolat. Elevii care învață despre siguranța online prin exemple reale, activități interactive și discuții cu colegii asimilează lecțiile mai bine și le aplică mai consecvent în propriile vieți decât cei care primesc aceleași informații sub forma unei prelegeri.

4.2 Prevenirea hărțuirii cibernetice

Cercetările privind prevenirea hărțuirii cibernetice (cyberbullying) arată în mod consecvent că cele mai bune rezultate le au abordările la nivelul întregii școli (whole-school approaches). Aceasta înseamnă programe care aduc împreună elevii, profesorii, părinții și conducerea școlii în jurul unui scop comun: crearea unui mediu mai sigur. Școlile care tratează cyberbullying-ul pur și simplu ca pe o problemă disciplinară, de rezolvat doar după ce au loc incidente, obțin în mod constant rezultate mai slabe decât cele care adoptă o abordare preventivă la nivelul întregii comunități.

Programele care se concentrează doar pe comportamentul celor care hărțuiesc sunt mai puțin eficiente decât cele care dezvoltă empatia și abilitățile martorilor (bystanders). Elevii care înțeleg răul pe care îl cauzează cyberbullying-ul și care au fost învățați cum să sprijine un coleg care devine țintă au șanse mai mari să raporteze incidentele și să intervină pentru a ajuta. Faptul că martorii intervin sau aleg să tacă este unul dintre cei mai puternici indicatori ai modului în care va evolua situația: dacă hărțuirea va escalada sau se va opri.

Sistemele de raportare anonimă duc în mod constant la semnalarea unui număr mai mare de incidente. Elevii care trec prin situații de cyberbullying adesea nu spun nimănui pentru că se tem că nu vor fi crezuți, că lucrurile se vor înrăutăți sau că vor exista consecințe sociale în grupul lor de prieteni. Școlile care oferă o cale de raportare cu adevărat confidențială și de încredere înregistrează rate mai mari de dezvăluire și posibilități de intervenție mai rapidă.

Formarea profesorilor este esențială și adesea subestimată. Cercetările arată că mulți profesori se simt nesiguri cu privire la modul în care ar trebui să reacționeze la cyberbullying, mai ales când sunt implicate aplicații sau funcționalități cu care nu sunt familiarizați. Școlile care investesc în cursuri de formare practice și structurate pentru profesori, axate pe recunoașterea și gestionarea cyberbullying-ului, obțin în mod constant rezultate mai bune pentru elevi.

Implicarea părinților face, de asemenea, o diferență constantă. Părinții care înțeleg ce înseamnă cyberbullying-ul, care știu cum funcționează platformele folosite de copiii lor și care se simt conectați la abordarea școlii sunt mai pregătiți atât să își sprijine copiii, cât și să consolideze acasă mesajele transmise la școală.

Cercetările oferă dovezi clare privind amploarea acestei probleme. Conform studiului OMS privind Comportamentele de Sănătate la Copiii de Vârstă Școlară (HBSC, 2024), aproximativ unul din șase adolescenți din Europa (în jur de 15%) raportează că a fost victimă a cyberbullying-ului, ratele fiind similare între băieți și fete și înregistrând o tendință de creștere față de anul 2018. Datele OECD au arătat variații între țări cuprinse între 7,5% și 27,1%. Datele colectate de liniile telefonice de asistență ale rețelei europene Insafe plasează constant cyberbullying-ul printre cele mai frecvente motive pentru care copiii și adolescenții contactează serviciile de suport, iar în trimestrul al patrulea din 2025 a fost din nou cea mai frecventă problemă semnalată.

În cadrul unei consultări organizate de Comisia Europeană în 2025, peste 6.000 de copii și adolescenți cu vârste între 12 și 17 ani din întreaga UE au exprimat așteptări clare din partea școlilor: o majoritate a solicitat reguli explicite și consecințe ferme pentru cyberbullying, ore dedicate predării acestui subiect și sprijin psihologic pentru cei afectați. Fetele au fost în mod constant mai predispuse decât băieții să solicite astfel de măsuri.

O meta-analiză realizată de Polanin et al. (2021), care a cuprins peste 45.000 de elevi, a arătat că programele dedicate prevenirii cyberbullying-ului au produs o reducere semnificativă din punct de vedere statistic atât a agresivității, cât și a victimizării, iar programele concepute specific pentru cyberbullying au depășit ca eficiență abordările generale anti-bullying.

4.3 Starea de bine digitală

Cercetările privind utilizarea tehnologiei și sănătatea mintală a elevilor nu susțin concluzii simple. Nu orice utilizare a tehnologiei este dăunătoare. Folosirea activă a tehnologiei pentru muncă creativă, comunicare sau învățare poate avea efecte pozitive. Problema constantă este utilizarea pasivă: derularea conținutului pe rețelele sociale (scrolling) fără un scop clar sau fără o interacțiune semnificativă. Acest tip de utilizare este cel mai puternic asociat cu anxietatea, singurătatea și o stimă de sine scăzută, efectele fiind deosebit de pronunțate în rândul fetelor adolescente.

Dovezile susțin ferm educația în defavoarea restricțiilor. Școlile care se concentrează exclusiv pe limitarea accesului la tehnologie, fără a-i ajuta pe elevi să înțeleagă de ce anumite tipare de utilizare sunt dăunătoare sau fără a le oferi instrumente pentru a-și gestiona propriul comportament, obțin schimbări mai puțin durabile. Elevii care înțeleg problema și și-au dezvoltat propriile strategii arată îmbunătățiri mult mai sustenabile ale stării de bine.

Programele care îi învață pe elevi să gândească critic cu privire la obiceiurile lor digitale, să înțeleagă modul în care platformele de socializare sunt concepute pentru a le capta atenția cât mai mult timp și să recunoască decalajul dintre imaginile ideale de pe internet și realitate au arătat rezultate pozitive în reducerea anxietății și îmbunătățirea stimei de sine în multiple studii. Aceste programe funcționează cel mai bine atunci când sunt desfășurate continuu, ca parte din curriculum, și nu ca un eveniment izolat.

Implicarea elevilor în crearea regulilor digitale ale școlii crește în mod constant atât nivelul de conformare, cât și sentimentul lor de responsabilitate față de aceste reguli. Elevii care simt că regulile sunt echitabile și că au avut un cuvânt de spus în formularea lor sunt mai înclinați să le respecte și să își încurajeze colegii să facă la fel.

O constatare deosebit de importantă privește teama de a nu rata ceva (Fear of Missing Out - FOMO). Cercetările încadrează tot mai mult FOMO nu ca pe o stare de spirit trecătoare, ci ca pe o trăsătură psihologică relativ stabilă — o anxietate persistentă legată de ratarea unor experiențe valoroase pe care ceilalți le trăiesc. Studiile asociază FOMO cu simptome depresive, tulburări de somn și comportamentul compulsiv de verificare a telefonului. O revizuire sistematică și o meta-analiză din 2025 au confirmat o asociere statistică constantă între dependența de rețelele sociale și niveluri mai ridicate de anxietate, depresie, singurătate și o stimă de sine scăzută, FOMO fiind identificat frecvent ca un factor mediator. Școlile ar trebui să abordeze explicit FOMO și tiparele de utilizare compulsivă în activitățile destinate elevilor, nu doar prin mesaje generice despre timpul petrecut în fața ecranului.

Cercetările arată, de asemenea, că rezultatele depind în mare măsură nu doar de cât de mult folosesc elevii platformele digitale, ci și de modul în care le folosesc. Rețelele sociale pot funcționa ca o sursă de sprijin pentru unii elevi, în special pentru cei care sunt izolați sau aparțin unor grupuri minoritare. Abordările bazate pe prevenție ar trebui să îi ajute pe elevi să dezvolte o relație mai conștientă și mai intenționată cu tehnologia.

Identificarea timpurie și îndrumarea către sprijin specializat sunt esențiale. Elevii care sunt conectați cu sprijinul potrivit înainte ca dificultățile lor să devină grave au rezultate semnificativ mai bune decât cei care sunt identificați abia când problemele devin deja vizibile prin scăderea notelor sau schimbări comportamentale serioase. Școlile care au trasee clare și bine cunoscute pentru identificarea și sprijinirea elevilor aflați în dificultate sunt într-o poziție mult mai bună pentru a-i ajuta.

Anexa I: Tabelul de referință la nivel național

Utilizați acest tabel pentru a identifica parametrii naționali principali specifici țării dumneavoastră. Atunci când prezenta politică face trimitere la normele naționale, aici trebuie să le căutați.

Parametri	Grecia	Italia	Portugalia	Romania	Slovacia
Vârsta pentru consimțământul digital	15 ani	14 ani	13 ani	16 ani	16 ani
Autoritatea de protecție a datelor	HDPA dpa.gr	Garante garantepriva cy. it	CNPD cnpd.pt	ANSPDCP dataprotection . ro	UOOU dataprotection . gov.sk
Autoritatea pentru securitate cibernetică	EAKE cyber. gov.gr	ACN acn.gov.it	CNCS cncs.gov. pt	DNSC dnsc.ro	NBU nbu.gov.sk
Raportarea incidentelor cibernetice	EAKE	ACN	CERT.PT (24h pentru NIS2)	DNSC/PNRISC (24h)	NBU/SK-CERT
Raportarea încălcărilor securității datelor	HDPA, 72 de ore	Garante, 72 de ore	CNPD, 72 de ore	ANSPDCP, 72 de ore	UOOU,72 de ore
Resurse împotriva cyberbullying-ului	stop-bullying. gov.gr	Raportare către școală sau poliție	seguranet.pt	Școală sau ANSPDCP	Ghidul 1/2025
Cadrul legislativ privind telefoanele mobile	Interdicție strictă 2018/2024	Toate ciclurile de învățământ 2024/25	Anii de studiu 1–6 începând cu septembrie 2025	În timpul orelor, Legea 198/2023	Toate clasele începând cu ianuarie 2025
Ghid privind utilizarea IA în școli	Doar Legea UE privind IA	OM 166/2025	Neadoptate până în prezent	Neadoptate până în prezent	Planul privind IA 2025–2027

Anexa II: Model de scrisoare către părinți

Școlile pot adapta această scrisoare pentru a-i informa pe părinți cu privire la modul în care instituția prelucrează datele elevilor și la măsurile adoptate pentru a le garanta siguranța în mediul online. Transmiteți această informare în momentul înscrierii și ori de câte ori au loc modificări semnificative ale sistemelor digitale sau ale politicilor școlii.

[Numele școlii și adresa]
[Data]

Stimate părinte / Tutore legal,
Protecția datelor copilului dumneavoastră și asigurarea siguranței în mediul digital

Vă scriem pentru a vă informa cu privire la modul în care școala noastră prelucrează datele cu caracter personal ale elevilor și la măsurile pe care le luăm pentru a asigura un mediu de învățare digital sigur pentru copilul dumneavoastră.

Ce date colectăm și în ce scop. Colectăm informațiile cu caracter personal necesare desfășurării procesului educațional și gestionării administrative. Acestea includ numele, codul numeric personal (sau alt număr de identificare), situația prezenței și notele/calificativele. În anumite cazuri, putem stoca și informații privind starea de sănătate, dacă acestea sunt relevante pentru parcursul educațional. Colectăm strict datele necesare și le păstrăm numai pe perioada prevăzută de lege.

Cine are acces la date. Accesul la datele cu caracter personal ale copilului dumneavoastră este restricționat, fiind permis exclusiv personalului autorizat care are nevoie de aceste informații pentru a-și îndeplini atribuțiile de serviciu. Nu transmitem date către terți, cu excepția cazurilor în care există o obligație legală sau în care ne-ați acordat consimțământul dumneavoastră explicit.

Platformele digitale. Școala noastră utilizează platforme digitale pentru desfășurarea procesului instructiv-educativ și pentru activitățile administrative. Înainte de adoptarea oricărei platforme, verificăm conformitatea acesteia cu Regulamentul general privind protecția datelor (GDPR). Copilul dumneavoastră va accesa aceste platforme printr-un cont creat de școală. Lista platformelor utilizate în prezent poate fi obținută de la secretariatul școlii.

Consimțământul dumneavoastră. În cazul elevilor care nu au împlinit vârsta de [introduceți vârsta națională pentru consimțământul digital, ex: 16 ani], este necesar consimțământul scris al părinților înainte de a-i putea înregistra pe o platformă digitală. Vi se va solicita acordul la momentul înscrierii și ori de câte ori este introdusă o nouă platformă.

Hărțuirea cibernetică (cyberbullying). Școala noastră aplică proceduri clare pentru prevenirea și combaterea hărțuirii cibernetice. În cazul în care copilul dumneavoastră este victima sau martorul unui act de cyberbullying, vă rugăm să îl încurajați să se adreseze unui adult de încredere din școală sau să ne contactați direct la [date de contact].

Drepturile dumneavoastră. Aveți dreptul de a solicita accesul la datele pe care le deținem despre copilul dumneavoastră, rectificarea acestora și, în anumite condiții, ștergerea lor. Pentru exercitarea acestor drepturi, vă rugăm să contactați responsabilul cu protecția datelor (DPO) la adresa: [date de contact DPO].

Susținerea stării de bine digitale acasă. Vă încurajăm să purtați discuții deschise și empatice cu copilul dumneavoastră despre experiențele din mediul online. Dacă observați că este afectat sau neobișnuit de anxios în legătură cu utilizarea telefonului ori cu interacțiunile din mediul virtual, vă rugăm să luați legătura cu [consilierul școlar / persoana de contact desemnată]. De asemenea, la nivel național sunt disponibile linii telefonice de asistență destinate copiilor și tinerilor.

Dacă aveți întrebări, vă stăm cu plăcere la dispoziție.

Cu deosebită considerație,

[Numele directorului și Școala]

Anexa III: Model de regulament de utilizare a resurselor IT

Adaptați acest model pentru a elabora regulamentul de utilizare a resurselor digitale din cadrul școlii. Documentul trebuie semnat de către elevi, părinți sau tutori legali și cadrele didactice/personalul școlii la începutul fiecărui an școlar. Modificați-l pentru a reflecta sistemele folosite în școală, reglementările naționale și contextul specific.

Regulament de utilizare a resurselor IT

[Numele Școlii] | Anul școlar [XXXX–XXXX]

1. Scop

Prezenta politică stabilește regulile privind utilizarea dispozitivelor digitale, a internetului și a platformelor educaționale în cadrul școlii noastre. Prevederile se aplică tuturor elevilor, cadrelor didactice, personalului auxiliar și vizitatorilor care utilizează sistemele școlare. Prin semnarea acestui document, confirmați că ați citit, ați înțeles și sunteți de acord să respectați aceste reguli (în cazul elevilor minori, părinții/tutorii legali se obligă să le explice acestora conținutul prezentului document).

2. Destinația resurselor digitale ale școlii

Resursele digitale pot fi utilizate exclusiv pentru:

- Realizarea temelor, a proiectelor și a activităților didactice;
- Comunicarea cu cadrele didactice și colegii de clasă în scopuri strict educaționale;
- Utilizarea platformelor digitale aprobate oficial de către școală;
- Desfășurarea activităților educaționale autorizate în mod explicit de către un cadru didactic.

3. Interdicții (Ce NU este permis)

Este strict interzis:

- Accesarea, crearea sau distribuirea de conținut ilegal, dăunător, ofensator sau discriminatoriu;
- Hărțuirea, intimidarea, amenințarea sau umilirea altor elevi sau cadre didactice prin mijloace digitale (cyberbullying);
- Partajarea informațiilor cu caracter personal ale altor elevi sau ale personalului școlii fără consimțământul prealabil al acestora;
- Înregistrarea audio sau video a elevilor, profesorilor sau personalului școlii fără acordul lor explicit;
- Utilizarea contului unei alte persoane sau divulgarea propriilor date de autentificare;
- Instalarea de aplicații sau programe software pe dispozitivele școlii fără autorizație;
- Utilizarea conturilor personale pe platforme neaprobate pentru activități legate de școală.

4. Telefoanele mobile și dispozitivele personale

[Descrieți aici regulile școlii privind utilizarea telefoanelor mobile, în conformitate cu legislația națională (ex. Legea învățământului preuniversitar nr. 198/2023). Precizați unde trebuie depozitate telefoanele în timpul orelor, ce excepții se aplică și ce măsuri se iau în cazul nerespectării regulilor.]

5. Rețelele de socializare și comportamentul online

Elevii și personalul nu au voie să publice conținut referitor la școală, colegi sau cadre didactice care este dăunător, înșelător sau care ar putea prejudicia reputația unei persoane. Comportamentul online ce constituie hărțuire cibernetică (cyberbullying), indiferent dacă are loc în timpul sau în afara programului școlar, intră sub incidența prezentei politici și a procedurilor școlare privind prevenirea și combaterea bullyingului.

6. Raportarea incidentelor

Dacă întâlniți conținut care vă face pe dumneavoastră sau pe un alt elev să nu vă simțiți în siguranță, sau dacă observați o încălcare a acestei politici, raportați imediat situația unui adult de încredere din școală sau către:

7. Consecințe

Nerespectarea prezentei politici poate atrage suspendarea accesului la sistemele informatice ale școlii, aplicarea altor măsuri sau sancțiuni disciplinare prevăzute în regulamentul intern al școlii, iar în cazurile grave, sesizarea organelor de aplicare a legii.

Numele și prenumele elevului	
Semnătura elevului	
Numele și prenumele părintelui / tutorelui legal	
Semnătura părintelui / tutorelui legal	
Data	

Anexa IV: Procedură de răspuns la incidentele de securitate cibernetică

Urmați acești pași de fiecare dată când are loc un incident de securitate cibernetică în școala dumneavoastră. Un incident cibernetic reprezintă orice eveniment care compromite securitatea, disponibilitatea sau confidențialitatea datelor ori a sistemelor școlare. Aceasta include atacurile de tip ransomware, accesul neautorizat la sistemele școlii sau încălcarea securității datelor cu caracter personal.

Pasul 1: Identificarea și izolarea

De îndată ce observați un incident, anunțați imediat coordonatorul IT sau directorul școlii. Nu încercați să rezolvați problema pe cont propriu. Deconectați dispozitivul afectat de la rețea prin scoaterea cablului sau oprirea conexiunii Wi-Fi. Nu opriți dispozitivul decât dacă vi se cere în mod expres acest lucru, deoarece oprirea poate distruge probe importante. Notați ora și o descriere a ceea ce ați observat.

Pasul 2: Evaluarea

Coordonatorul IT și responsabilul cu protecția datelor (DPO) trebuie să evalueze incidentul împreună. Stabiliți ce sisteme, conturi sau date au fost afectate. Determinați dacă datele cu caracter personal au fost sau ar fi putut fi compromise. Verificați dacă incidentul este încă în desfășurare sau dacă a fost izolat.

Pasul 3: Notificarea

Datele cu caracter personal au fost sau ar fi putut fi compromise	Notificați autoritatea națională pentru protecția datelor în termen de 72 de ore. Consultați Partea 2 pentru autoritatea din țara dumneavoastră.
A avut loc un incident grav de securitate cibernetică	Notificați autoritatea națională de securitate cibernetică. În Portugalia, pentru entitățile vizate de directiva NIS2, acest lucru trebuie făcut în termen de 24 de ore. Consultați Partea 2 pentru autoritatea din țara dumneavoastră.
Sunt implicate activități infracționale	Contactați poliția.
Elevii sau personalul sunt în pericol imediat sau au fost afectați direct	Oferiți sprijin imediat și informați părinții sau tutorii legali, după caz.

Pasul 4: Recuperarea

Restaurați sistemele din copii de siguranță (backup), acolo unde acestea sunt disponibile. Resetați imediat toate parolele și datele de autentificare afectate. Aplicați toate actualizările de securitate relevante înainte de a reintroduce sistemele în uz. Verificați dacă sistemele restaurate funcționează corect înainte de a le pune din nou la dispoziția elevilor și a personalului.

Pasul 4a: Sprijinirea persoanelor afectate

Oferiți sprijin psihologic și practic imediat oricărui elev sau membru al personalului direct afectat de incident. Acest lucru trebuie să se desfășoare în paralel cu intervenția tehnică, nu după finalizarea acesteia. Contactați fără întârziere consilierul școlar sau echipa de asistență psihopedagogică. Respectați protocolul școlii privind starea de bine.

Pasul 5: Evaluarea

După ce incidentul a fost soluționat, efectuați o evaluare completă. Consemnați în scris ce s-a întâmplat, cum a apărut incidentul, ce măsuri au fost luate și care a fost rezultatul. Identificați modificările care ar reduce riscul ca un astfel de eveniment să se repete. Informați personalul vizat cu privire la concluziile trase, mai ales dacă incidentul a implicat un e-mail de phishing sau o eroare umană. Actualizați procedura de răspuns la incidente, dacă este necesar.

Registrul incidentelor

Data și ora incidentului	
Cum a fost descoperit și de către cine?	

Ce s-a întâmplat?	
Ce sisteme și date au fost afectate?	
Măsurile imediate luate	
Au fost compromise date cu caracter personal?	
A fost notificată autoritatea pentru protecția datelor? (Data)	
A fost notificată autoritatea de securitate cibernetică? (Data)	
A fost contactată poliția? (Data)	
Măsurile de recuperare luate	
Data la care sistemele au fost restaurate	
Evaluare finalizată? (Data)	
Modificări efectuate în urma evaluării	

Anexa V: Șablon de evaluare a impactului asupra protecției datelor (DPIA)

O evaluare a impactului asupra protecției datelor (DPIA) este necesară înainte ca școala dumneavoastră să introducă un nou sistem sau o nouă platformă digitală care implică prelucrarea unor cantități mari de date despre elevi, monitorizarea sistematică a elevilor, luarea de decizii automatizate care îi afectează pe elevi sau categorii speciale (sensibile) de date. Dacă nu sunteți sigur dacă este necesară o evaluare DPIA, adresați-vă DPO-ului dumneavoastră.

Partea A: Ce date vor fi prelucrate

Denumirea sistemului sau a platformei	
Furnizorul sau vânzătorul	
Ce date cu caracter personal vor fi prelucrate?	
Cine sunt persoanele vizate? (elevi, personal, părinți)	
Care este scopul prelucrării?	

Care este temeiul juridic al prelucrării?	
Unde vor fi stocate datele? (țara, în cadrul SEE?)	
Cine va avea acces?	
Cât timp vor fi păstrate datele?	
Vor fi furnizate datele unor terți?	

Partea B: Evaluarea riscurilor

Risc	Nivel (Scăzut / Mediu / Ridicat) și modul în care va fi abordat
Acces neautorizat la datele elevilor	
Date pierdute sau șterse accidental	
Date utilizate în alte scopuri decât cele inițiale	
Elevi monitorizați sau profilați fără transparență	
Date transferate în afara SEE fără garanții adecvate	
Date păstrate mai mult timp decât este necesar	

Partea C: Decizie

Nivelul general de risc (Scăzut / Mediu / Ridicat)	
Poate fi inițiată prelucrarea? (Da / Da, cu măsuri de atenuare / Nu)	
Ce măsuri trebuie luate înainte de începerea prelucrării?	
A fost consultat DPO-ul? (Da / Nu / Data)	

Evaluare completată de	
Data evaluării	
Data următoarei reevaluări	

Anexa VI: Registrul de riscuri al școlii

Registrul de riscuri al școlii ajută instituția dumneavoastră să identifice, să evalueze și să gestioneze principalele riscuri de securitate cibernetică și de protecție a datelor cu care se confruntă. Completarea acestui registru reprezintă un pas practic în aplicarea abordării de gestionare a riscurilor descrise în Partea a 3-a a prezentei politici.

Exemplele din tabelul de mai jos au caracter orientativ. Acestea sunt oferite pentru a ajuta școala să demareze procesul și pentru a ilustra tipurile de riscuri cel mai des întâlnite într-un mediu școlar. Școala dumneavoastră ar trebui să adauge, să elimine sau să adapteze înregistrările pentru a reflecta propriile circumstanțe, sisteme și contextul specific. Registrul trebuie reevaluat cel puțin o dată pe an și actualizat ori de câte ori are loc o schimbare semnificativă, cum ar fi introducerea unei noi platforme digitale sau un incident de securitate cibernetică.

Cum se evaluează riscurile

Pentru fiecare risc, acordați un punctaj de la 1 la 5 pentru Probabilitate și Impact (1 = foarte scăzut, 5 = foarte ridicat). Înmulțiți cele două punctaje pentru a obține Scorul de risc.

Risc ridicat (15–25): trebuie abordat imediat.

Risc mediu-ridicat (8–14): trebuie abordat; se vor prioritiza riscurile cu impact ridicat.

Risc mediu-scăzut (4–7): ar trebui abordat acolo unde impactul este semnificativ.

Risc scăzut (1–3): acceptabil; se monitorizează cu regularitate. .

Tabelul orientativ privind Registrul de riscuri se află pe pagina următoare (orientare landscape/vedere).

ID	Risc	Ce s-ar putea întâmpla	Cum îl reducem	Probabilitate (1-5)	Impact (1-5)	Scor de risc	Responsabil	Dacă se întâmplă
1	Phishing prin e-mail direcționat către personal	Personalul accesează un link malițios, oferind unui atacator acces la sistemele școlare și la datele elevilor	Instruire anuală a personalului, exerciții de simulare a phishing-ului, autentificare cu mai mulți factori (MFA) pe toate conturile	4	4	16	Director / Coordonator IT	Izolarea dispozitivului afectat, notificarea autorității naționale de securitate cibernetică, restaurarea datelor din copia de rezervă (backup)
2	Atac de tip ransomware	Sistemele școlii sunt blocate, iar fișele și notele elevilor devin inaccesibile	Copii de rezervă (backup) periodice și testate, stocate offline, software antivirus actualizat la zi, instruirea personalului	3	5	15	Coordonator IT	Restaurare din copia de rezervă, raportare către autoritatea națională de securitate cibernetică, Notificarea Autorității Naționale de Supraveghere a Prelucrării Datelor cu Caracter Personal (ANSPDCP) dacă sunt afectate datele elevilor
3	Date ale elevilor trimise din greșeală unei persoane neautorizate	Datele cu caracter personal ale unui elev sunt distribuite accidental unei persoane neautorizate	Instruire a personalului privind manipularea datelor, utilizarea exclusivă a canalelor oficiale de comunicare ale școlii	4	3	12	DPO (Responsabilul pentru protecția datelor)	Contactarea destinatarului și solicitarea ștergerii datelor, raportarea către autoritatea națională de protecție a datelor în termen de 72 de ore (dacă este

ID	Risc	Ce s-ar putea întâmpla	Cum îl reducem	Probabilitate (1-5)	Impact (1-5)	Scor de risc	Responsabil	Dacă se întâmplă
								cazul), documentarea incidentului
4	Hărțuire cibernetică (cyberbullying) prin intermediul platformei școlare	Un elev folosește un instrument de comunicare al școlii pentru a hărțui un alt elev	Regulament de utilizare a resurselor IT semnat de toți elevii și părinții, educație privind combaterea hărțuirii cibernetice, procedură clară de raportare	4	3	12	Director / Diriginte	Respectarea procedurii școlare anti-bullying, oferirea de sprijin elevului afectat, implicarea părinților, documentarea incidentului

Anexa VII: Registrul de evidență a prelucrărilor de date

Registrul de evidență a prelucrărilor de date ajută unitatea dumneavoastră de învățământ să țină o evidență clară a tuturor datelor cu caracter personal pe care le prelucrează. Păstrarea acestui registru reprezintă o obligație legală în conformitate cu articolul 30 din RGPD. Acesta trebuie pus la dispoziția autorității naționale de supraveghere a prelucrării datelor cu caracter personal, la cererea acesteia.

Exemplele de mai jos includ cele mai frecvente categorii de date cu caracter personal prelucrate în unitățile de învățământ. Lista are un caracter orientativ: unitatea dumneavoastră de învățământ trebuie să adauge categoriile specifice propriului context și să le elimine pe cele care nu se aplică. Revizuiți și actualizați registrul cel puțin o dată pe an, precum și ori de câte ori introduceți un sistem sau o platformă nouă.

Ce este un temei juridic?

De fiecare dată când școala dumneavoastră prelucrează date cu caracter personal, trebuie să dispună de un motiv legal. Cele mai frecvente temeiuri juridice aplicabile instituțiilor de învățământ sunt:
Obligația legală: prelucrarea este impusă de legislația națională din domeniul educației (de exemplu, evidența prezenței).
Îndeplinirea unei sarcini de interes public: prelucrarea este necesară pentru ca școala să își exercite atribuțiile și funcțiile publice.
Consimțământul: persoana vizată și-a exprimat acordul cu privire la prelucrare (necesar, de exemplu, pentru publicarea fotografiilor sau utilizarea unor platforme opționale/neesențiale).

Un registru orientativ de cartografiere a datelor este prezentat pe pagina următoare (format landscape / vedere) .

Tipul de date	De ce le prelucrăm	Temei legal	Unde sunt stocate	Cine are acces	Cât timp le păstrăm	Există copii de siguranță?	Transmise către
Date cu caracter personal ale elevilor (nume, prenume, cod numeric personal, adresă, dată de naștere)	Necesare pentru administrarea unității de învățământ și pentru asigurarea conformității cu legislația națională din domeniul educației	Obligație legală	Sistemul informatic național al școlii (de ex. MySchool, SIIIR, Unica	Exclusiv directorul și personalul administrativ	Conform perioadei prevăzute de legislația națională	Da	Ministerul Educației, prin intermediul platformei naționale
Situația școlară a elevilor (note, prezență, evaluări)	Necesare pentru monitorizarea progresului școlar al elevilor și pentru informarea părinților	Obligație legală / Îndeplinire a unei sarcini de interes public	Sistemul informatic al unității de învățământ și catalogul profesoral	Profesorii diriginți/cadrele didactice, directorul, personalul administrativ	Conform perioadei prevăzute de legislația națională	Da	Părinții (prin intermediul unui canal securizat), Ministerul Educației
Informații privind starea de sănătate a elevilor (alergii, dizabilități, cerințe medicale speciale)	Necesare pentru protejarea sănătății și siguranței elevilor pe durata programului școlar	Obligație legală / Interese vitale	Dosar fizic securizat sau înregistrare digitală criptată	Exclusiv directorul, asistentul medical/ medicul școlar și cadrele didactice vizate	Pe durata școlarizării, la care se adaugă perioada prevăzută de lege	Da (criptat)	Furnizorii de servicii medicale, exclusiv în caz de necesitate

Tipul de date	De ce le prelucrăm	Temei legal	Unde sunt stocate	Cine are acces	Cât timp le păstrăm	Există copii de siguranță?	Transmise către
Fotografii și imagini ale elevilor	Legitimație de elev, publicații, documentarea evenimentelor	Consimță-mântul părinților	Serverul unității de învățământ sau platformă aprobată	Personalul administrativ, cadre didactice autorizate	Pe durata școlarizării; șterse la cerere	Da	Fără transmitere către terți în lipsa unui consimțământ suplimentar

Anexa VIII: Registrul politicilor și procedurilor unității de învățământ

Acest registru ajută unitatea dumneavoastră de învățământ să evidențieze principalele politici de securitate și de protecție a datelor puse în aplicare. Existența unor politici documentate în fiecare dintre aceste domenii constituie o dovadă importantă a faptului că școala își gestionează responsabilitățile privind securitatea cibernetică și protecția datelor într-un mod structurat.

Politicile enumerate mai jos sunt cele mai relevante în raport cu recomandările din prezenta Politică de reziliență cibernetică. Lista are caracter orientativ: școala dumneavoastră poate avea politici suplimentare care ar trebui, de asemenea, incluse în această secțiune. Pentru fiecare politică, menționați persoana responsabilă, data ultimei actualizări și data următoarei revizuiri. În cazul în care o politică nu a fost încă elaborată, consemnați acest fapt ca acțiune prioritară.

Modele disponibile

Modelele pentru câteva dintre politicile enumerate mai jos sunt incluse în anexele prezentei politici:

- Regulament de utilizare a resurselor IT : Anexa III.
- Procedura de răspuns la incidente: Anexa IV.
- Evaluarea impactului asupra protecției datelor (DPIA): Anexa V.
- Registrul de riscuri: Anexa VI.
- Registrul de evidență a prelucrărilor de date: Anexa VII.
- Autoevaluarea rezilienței cibernetice a unității de învățământ: Anexa IX.

ID	Denumirea politicii	Domenii cheie vizate	Responsabil de politică	Data ultimei actualizări	Data următoarei revizuiri
1	Regulamentul de utilizare a resurselor IT	Utilizarea sistemelor și a echipamentelor unității de învățământ. Reguli privind utilizarea telefoanelor mobile. Raportare.	Director / Coordinator IT		
2	Politica de control al accesului	Drepturile de acces la sisteme și date. Reguli privind parolele. Revocarea accesului la încetarea	Coordonator IT / DPO (Responsabil cu protecția datelor)		

ID	Denumirea politicii	Domenii cheie vizate	Responsabil de politică	Data ultimei actualizări	Data următoarei revizuiri
		raporturilor de muncă.			
3	Politica privind protecția datelor	Conformitatea GDPR. Responsabilitățile DPO. Consimțământul părinților. Note de informare privind confidențialitatea. Răspunsul la încălcările securității datelor.	DPO / Director		
4	Politica privind salvarea de siguranță (Backup)	Seturile de date salvate, frecvența, locul de stocare și procedura de testare a recuperării datelor.	Coordonator IT		
5	Politica privind răspunsul la incidente	Modul în care unitatea de învățământ reacționează la incidentele de securitate cibernetică și la încălcările securității datelor. Persoanele responsabile. Procedura de notificare a autorităților.	Director / DPO / Coordonator IT		
6	Politica anti-bullying (inclusiv hărțuirea online / cyberbullying)	Definirea hărțuirii online. Fluxul de raportare. Modul de reacție al unității de învățământ. Formarea personalului.	Director		

ID	Denumirea politicii	Domenii cheie vizate	Responsabil de politică	Data ultimei actualizări	Data următoarei revizuiri
		Implicarea părinților.			
7	Politica privind utilizarea dispozitivelor mobile	Regulile privind utilizarea telefoanelor mobile de către elevi, în conformitate cu legislația națională. Interzicerea înregistrărilor neautorizate.	Director		

Anexa IX: Autoevaluarea rezilienței cibernetice a unității de învățământ

Unitățile de învățământ pot utiliza această listă de verificare pentru a stabili un nivel de referință privind reziliența lor cibernetică actuală și pentru a identifica lacunele prioritare. Marcați fiecare element cu Da, Parțial sau Nu. Scopul nu este de a obține o calificare de tip „promovat”/„respins”, ci de a identifica domeniile care necesită atenție sporită.

Se recomandă ca unitățile de învățământ să repete această autoevaluare cel puțin o dată pe an. Evoluția punctajelor în timp reflectă progresul obținut și susține o cultură a îmbunătățirii continue.

Elementele enumerate au caracter orientativ. Adaptați-le pentru a reflecta contextul propriu al unității de învățământ, cerințele naționale și circumstanțele specifice.

Domeniu	Ce trebuie verificat	Da / Parțial / Nu
Management și organizare	Unitatea de învățământ are desemnat un coordonator pentru securitate cibernetică sau siguranță digitală.	
Management și organizare	Unitatea de învățământ deține o Politică de utilizare acceptabilă redactată în scris, revizuită în ultimii 2 ani.	
Management și organizare	Unitatea de învățământ dispune de o procedură documentată de răspuns la incidente, adusă la cunoștința personalului.	
Conștientizare și formare	Personalul beneficiază cel puțin o dată pe an de instruire privind securitatea cibernetică și siguranța online.	

Domeniu	Ce trebuie verificat	Da / Parțial / Nu
Conștientizare și formare	Elevii beneficiază de educație privind cetățenia digitală și siguranța online, adaptată vârstei lor.	
Conștientizare și formare	Părinții și tutorii legali primesc informații privind riscurile digitale cel puțin o dată pe an școlar.	
Siguranță digitală și prevenție	Unitatea de învățământ dispune de un protocol specific, menționat ca atare, pentru răspunsul la cazurile de cyberbullying.	
Siguranță digitală și prevenție	Elevii știu cum și cui să raporteze confidențial incidentele din mediul online.	
Siguranță digitală și prevenție	Activitățile de prevenție se adresează în mod explicit grupurilor diverse și vulnerabile	
Protecția datelor și confidențialitate	Unitatea de învățământ ține un registru al platformelor și instrumentelor care prelucrează datele elevilor.	
Protecția datelor și confidențialitate	Acordul părinților este obținut înainte de înscrierea elevilor pe platformele digitale, atunci când legea o impune.	
Măsuri tehnice	Dispozitivele și rețelele unității de învățământ utilizează software de protecție actualizat și controale de acces corespunzătoare	
Măsuri tehnice	Dispozitivele și rețelele unității de învățământ utilizează software de protecție actualizat și controale de acces corespunzătoare	

Interpretarea punctajului

Calculați răspunsurile Da (1 punct) și răspunsurile Parțial (0,5 puncte). Împărțiți suma la 13 și înmulțiți cu 100 pentru a obține procentul. Încadrați rezultatul în nivelurile de maturitate de mai jos.

Nivel	Punctaj	Descriere

1 - Inițial	0 – 20%	Există un cadru de conducere, sesiuni de formare sau proceduri de răspuns la incidente foarte reduse ori inexistente.
2 - În dezvoltare	21 – 45%	Există politici de bază, dar acestea nu sunt aplicate, revizuite sau comunicate în mod consecvent.
3 - Stabilit	46 – 70%	Elementele fundamentale de guvernanță, formare și răspuns la incidente sunt implementate și cunoscute de personal.
4 - Avansat	71 – 90%	Politicile cuprinzătoare și revizuite periodic, precum și sesiunile de formare, ajung la personal, elevi și părinți.
5 - Rezilient	91 – 100%	Reziliența cibernetică este integrată în cultura unității de învățământ, prin formare continuă și măsuri inclusive de prevenție.

Aceste niveluri reprezintă exclusiv un instrument de autoevaluare și nu constituie o certificare formală sau o evaluare oficială a conformității.

Referințe

Legislația Uniunii Europene

Următoarele acte juridice ale Uniunii Europene constituie cadrul legal comun care stă la baza prezentei Politici. Acestea stabilesc cerințele principale privind protecția datelor, securitatea cibernetică, inteligența artificială, serviciile digitale, comunicațiile electronice și educația digitală în toate statele membre ale UE.

- Uniunea Europeană, Regulamentul (UE) 2016/679 (Regulamentul General privind Protecția Datelor – GDPR), Jurnalul Oficial al Uniunii Europene. Disponibil la: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679
- Uniunea Europeană, Directiva (UE) 2022/2555 (Directiva NIS 2), Jurnalul Oficial al Uniunii Europene. Disponibilă la: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022L2555
- Uniunea Europeană, Regulamentul (UE) 2024/1689 (Actul privind Inteligența Artificială – AI Act), Jurnalul Oficial al Uniunii Europene. Disponibil la: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L_202401689
- Uniunea Europeană, Regulamentul (UE) 2022/2065 (Actul privind Serviciile Digitale – DSA), Jurnalul Oficial al Uniunii Europene. Disponibil la https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022R2065
- Uniunea Europeană, Directiva 2002/58/CE (Directiva asupra confidențialității și comunicațiilor electronice – Directiva ePrivacy), Jurnalul Oficial al Comunităților Europene. Disponibilă la: : https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32002L0058
- Uniunea Europeană, Regulamentul (UE) 2019/881 (Actul privind Securitatea Cibernetică – Cybersecurity Act), Jurnalul Oficial al Uniunii Europene. Disponibil la: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019R0881

Instrumente legislative naționale

Următoarele instrumente legislative naționale și surse oficiale au fost utilizate la elaborarea Părții a 2-a a prezentei politici. Acestea sunt enumerate pe țări, în conformitate cu practica standard de citare pentru proiectele finanțate de Uniunea Europeană.

Grecia

- Republica Elenă (2018). Legea nr. 4577/2018 privind securitatea rețelelor și a sistemelor informatice. Monitorul Oficial A' 199/03.12.2018. Disponibil la: https://www.mindigital.gr/wp-content/uploads/2019/09/N.4577_2018.pdf
- Republica Elenă (2019). Legea nr. 4624/2019 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal (Măsuri de aplicare a RGPD). Monitorul Oficial A' 137/29.08.2019. Traducere în limba engleză disponibilă la: https://www.dpa.gr/sites/default/files/2020-08/LAW%204624_2019_EN_TRANSLATED%20BY%20THE%20HDPA.PDF

- Republica Elenă (2020). Legea nr. 4727/2020 privind serviciile digitale și comunicațiile electronice. Monitorul Oficial A' 184/23.09.2020. Disponibil la: https://adae.gov.gr/images/nomothetiko-plaisio/Nomos_4727_2020_01.pdf
- Republica Elenă (2022). Legea nr. 4961/2022 privind tehnologiile emergente și guvernanța digitală. Monitorul Oficial A' 146/27.07.2022. Disponibil la: https://www.mindigital.gr/wp-content/uploads/2024/02/N-4961.pdf
- Republica Elenă (2023). Legea nr. 5029/2023 privind prevenirea și gestionarea violenței școlare și a hărțuirii cibernetice (cyberbullying). Monitorul Oficial A' 55/10.03.2023. Disponibil la: https://www.iep.edu.gr/wp-content/uploads/2025/01/2024-08-02_N_5029-2023.pdf
- Republica Elenă (2024). Legea nr. 5160/2024 privind securitatea cibernetică (Transpunerea Directivei NIS2). Monitorul Oficial A' 195/27.11.2024. Disponibil la: https://search.et.gr/el/fek/?fekId=774154
- Ministerul Transformării Digitale, Republica Elenă (2025). Decizia ministerială nr. 1689/2025 privind cerințele de securitate cibernetică pentru entitățile din sectorul public. Monitorul Oficial B' 2186/06.05.2025. Disponibil la: ttps://cyber.gov.gr/wp-content/uploads/2025/05/20250202186.pdf
- Ministerul Transformării Digitale, Republica Elenă (2025). Decizia ministerială nr. 1899/2025 privind managementul securității informației în entitățile publice. Monitorul Oficial B' 4250/05.08.2025. Disponibil la: https://cyber.gov.gr/wp-content/uploads/2025/03/KYA_APOFASI_10-Feb-2025_FEK-463_DEFTERO-TEFHOS.pdf

Italia

- Republica Italiană (2003). Decretul legislativ nr. 196/2003 — Codul privind protecția datelor cu caracter personal, modificat prin Decretul legislativ nr. 101/2018. Disponibil la: https://www.garanteprivacy.it/documents/10160/0/Codice+in+materia+di+protezione+dei+dati+personali.pdf
- Republica Italiană (2021). Legea nr. 109/2021 de aprobare a Decretului-lege nr. 82/2021 — Înființarea Agenției Naționale de Securitate Cibernetică (ACN). Monitorul Oficial, 04.08.2021. Disponibil la: https://www.gazzettaufficiale.it/atto/serie_generale/caricaDettaglioAtto/originario?atto.codiceRedazionale=21A04841
- Republica Italiană (2024). Decretul legislativ nr. 138/2024 — Transpunerea Directivei NIS2. Monitorul Oficial, 01.10.2024. Disponibil la: https://www.gazzettaufficiale.it/eli/id/2024/10/01/24G00155/SG
- Ministerul Educației, Republica Italiană (2020). Decretul ministerial nr. 89/2020 — Ghidul privind predarea digitală integrată (DDI). Disponibil la: https://www.mim.gov.it/documents/20182/0/Decreto.pdf
- Ministerul Educației, Republica Italiană (2024). Nota MIM nr. 5274/2024 — Restricții privind utilizarea telefoanelor inteligente în școli. Disponibilă la: https://www.mim.gov.it/-/nota-n-5274-dell-11-luglio-2024
- Ministerul Educației, Republica Italiană (2025). Circulara MIM nr. 3392/2025 — Restricții privind utilizarea telefoanelor mobile în școli. Disponibilă la: https://www.mim.gov.it/-/circolare-n-3392-del-16-giugno-2025
- Ministerul Educației, Republica Italiană (2025). Decretul ministerial nr. 166/2025 — Ghidul privind utilizarea responsabilă a inteligenței artificiale în școli. Disponibil la: https://www.mim.gov.it/-/decreto-ministeriale-n-166-del-9-agosto-2025

Portugalia

- Republica Portugheză (2018). Legea nr. 46/2018 — Cadrul juridic privind securitatea spațiului cibernetic (RFSC). Monitorul Oficial, 13.08.2018. Disponibil la: https://diariodarepublica.pt/dr/detalhe/lei/46-2018-116029384
- Republica Portugheză (2019). Legea nr. 58/2019 — Legea portugheză privind protecția datelor (Măsuri de aplicare a RGPD). Monitorul Oficial, 08.08.2019. Disponibil la: https://diariodarepublica.pt/dr/detalhe/lei/58-2019-123815982
- Consiliul de Miniștri, Republica Portugheză (2020). Hotărârea nr. 30/2020 — Planul de acțiune pentru tranziția digitală (PATD). Monitorul Oficial, 2020. Disponibil la: https://diariodarepublica.pt/dr/detalhe/resolucao-conselho-ministros/30-2020-132133788
- Republica Portugheză (2025). Decretul-lege nr. 95/2025 — Interzicerea utilizării telefoanelor inteligente în școli (clasele I-VI). Monitorul Oficial, 03.07.2025.
- Republica Portugheză (2025). Decretul-lege nr. 125/2025 — Transpunerea Directivei NIS2 (în vigoare din 3 aprilie 2026). Monitorul Oficial, 04.12.2025. Disponibil la: Decreto-Lei n.º 125/2025, de 4 de dezembro | DR
- Direcția Generală pentru Educație (DGE), Portugalia. Cadrul referențial pentru Planul de acțiune privind dezvoltarea digitală a școlii (PADDE). Disponibil la: https://www.dge.mec.pt
- Centrul Național de Securitate Cibernetică (CNCS) / DGE, Portugalia. SeguraNet — Resurse de siguranță digitală și securitate cibernetică pentru școli. Disponibil la: https://www.seguranet.pt
- Centrul Național de Securitate Cibernetică (CNCS), Portugalia. CERT.PT — Echipa națională de răspuns la incidente de securitate cibernetică. Disponibil la: https://www.cncs.gov.pt/pt/certpt/

România

- România (2018). Legea nr. 190/2018 privind măsuri de punere în aplicare a Regulamentului (UE) 2016/679 (RGPD). Monitorul Oficial al României, Partea I, nr. 651/26.07.2018. Disponibilă la: https://portal.just.ro/101/Documents/LEGE__190_2018_date_cu_caracter_personal.pdf
- România (2023). Legea nr. 58/2023 privind securitatea și apărarea cibernetică a României, precum și pentru modificarea și completarea unor acte normative. Monitorul Oficial al României, Partea I, nr. 214/15.03.2023. Disponibilă la: https://legislatie.just.ro/Public/DetaliiDocument/265677
- România (2023). Legea învățământului preuniversitar nr. 198/2023. Monitorul Oficial al României, Partea I, nr. 613/05.07.2023. Disponibilă la: https://edu.ro/sites/default/files/_fisiere/Minister/2023/Legi_educatie_Romania_educata/legi_monitor/Legea_invatamantului_preuniversitar_nr_198.pdf
- Guvernul României (2024). Ordonanța de urgență a Guvernului nr. 155/2024 privind măsuri pentru un nivel comun ridicat de securitate cibernetică în Uniunea Europeană (Transpunerea Directivei NIS2), aprobată prin Legea nr. 124/2025. Monitorul Oficial al României, Partea I, nr. 1332/31.12.2024. Disponibilă la: https://legislatie.just.ro/Public/DetaliiDocumentAfis/293121
- Ministerul Educației (2024). Ordinul ministrului educației nr. 5707/2024 privind aprobarea Statutului elevului. Monitorul Oficial al României, Partea I, nr. 795/12.08.2024. Disponibil la: https://www.edu.ro/sites/default/files/_fisiere/Legislatie/2024/OM_5707_2024_Statut_elev.pdf
- Ministerul Educației (2025). Ordinele ministrului educației nr. 6055-6058/2025 privind Regulamentul-cadru de organizare și funcționare a unităților de învățământ preuniversitar

(ROFUIP 2025-2026). Monitorul Oficial al României, Partea I, nr. 819/04.09.2025. Disponibile la: https://www.edu.ro/ROFUIP

Slovacia

- Republica Slovacă (2003). Legea nr. 596/2003 privind administrația de stat în învățământ și autoguvernarea școlară, cu modificările și completările ulterioare. Disponibilă la: https://www.slov-lex.sk
- Republica Slovacă (2008). Legea nr. 245/2008 privind educația și formarea profesională (Legea învățământului), modificată prin Legea nr. 323/2025 (restricții privind utilizarea telefoanelor mobile). Disponibilă la: https://www.slov-lex.sk/ezbierky/pravne-predpisy/SK/ZZ/2008/245/
- Republica Slovacă (2018). Legea nr. 18/2018 privind protecția datelor cu caracter personal (Măsuri de aplicare a RGPD). Disponibilă la: https://www.slov-lex.sk/ezbierky/pravne-predpisy/SK/ZZ/2018/18/
- Republica Slovacă (2018). Legea nr. 69/2018 privind securitatea cibernetică. Disponibilă la: https://www.zakonypreludi.sk/zz/2018-69
- Republica Slovacă (2024). Legea nr. 366/2024 privind securitatea cibernetică (Transpunerea Directivei NIS2). Disponibilă la: https://www.slov-lex.sk/ezbierky/pravne-predpisy/SK/ZZ/2024/366/20250101.html
- Ministerul Educației, Republica Slovacă (2025). Ghidul metodologic nr. 1/2025 privind prevenirea și gestionarea hărțuirii cibernetice (cyberbullying) în școli și unități de învățământ. Disponibilă la: https://www.minedu.sk/data/att/d76/32441.fb1a83.pdf
- Ministerul Educației, Republica Slovacă (2025). Planul pentru utilizarea responsabilă a inteligenței artificiale în educație 2025–2027. Disponibil la: https://ai.iedu.sk/

Standarde ISO

Elaborarea recomandărilor practice și a măsurilor de management formulate în cadrul prezentei politici are la bază următoarele standarde recunoscute la nivel internațional:

- Organizația Internațională de Standardizare (ISO), ISO/IEC 27001:2022 — Securitatea informației, securitatea cibernetică și protecția confidențialității. Sisteme de management al securității informației. Cerințe. Disponibil la: https://www.iso.org/standard/27001
- Organizația Internațională de Standardizare (ISO), ISO/IEC 27002:2022 — Securitatea informației, securitatea cibernetică și protecția confidențialității. Controale de securitate a informației. Disponibil la: https://www.iso.org/standard/75652.html
- Organizația Internațională de Standardizare (ISO), ISO/IEC 27701:2025 — Tehnici de securitate. Extindere la ISO/IEC 27001 și ISO/IEC 27002 pentru managementul informațiilor privind confidențialitatea. Cerințe și linii directoare. Disponibil la: https://www.iso.org/standard/27701
- Organizația Internațională de Standardizare (ISO), ISO 22301:2019 — Securitate și reziliență. Sisteme de management al continuității afacerii. Cerințe. Disponibil la: https://www.iso.org/standard/75106.html
- Organizația Internațională de Standardizare (ISO), ISO 31000:2018 — Managementul riscului. Linii directoare. Disponibil la: https://www.iso.org/standard/65694.html

Cercetare și fundamentare științifică

Elaborarea Părții a 4-a din prezenta politică are la bază următoarele publicații și surse de documentare:

- Comisia Europeană (2025). Vocile copiilor privind hărțuirea cibernetică: Consultare în rândul copiilor cu vârste între 12 și 17 ani. Disponibil la: https://eu-for-children.europa.eu/cyberbullying_en
- Comisia Europeană (2025). Instrucțiuni privind măsurile necesare garantării unui nivel ridicat de confidențialitate, siguranță și securitate pentru minori în mediul online. Disponibil la: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:C_202505519
- Comisia Europeană / Un Internet mai bun pentru copii (BIK+) / Rețeaua Insafe (2025-2026). Indicatori de politică publică BIK și statistici privind liniile de asistență (Helpline). Disponibil la: https://better-internet-for-kids.europa.eu/en
- Agenția Uniunii Europene pentru Securitate Cibernetică (ENISA) (2022). Inițiative privind educația în domeniul securității cibernetice în statele membre ale UE. Disponibil la: https://www.enisa.europa.eu/publications/cybersecurity-education-initiatives-in-the-eu-member-states
- Organizația pentru Cooperare și Dezvoltare Economică (OCDE) (2025). Cum este viața copiilor în era digitală? Disponibil la: 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). O revizuire sistematică și meta-analiză a intervențiilor pentru reducerea perpetrării și victimizării în cazul hărțuirii cibernetice. Prevention Science. Disponibil la: https://link.springer.com/article/10.1007/s11121-021-01259-y
- Torgal, C. și Aksoy, C. (2022). O meta-analiză a impactului programelor școlare de prevenire a hărțuirii cibernetice asupra comportamentului martorilor din mediul online. School Psychology Review, 52(2). Disponibil la: https://www.tandfonline.com/doi/full/10.1080/2372966X.2021.1913037
- Biroul Regional pentru Europa al Organizației Mondiale a Sănătății (2024). Comportamentul legat de sănătate la copiii de vârstă școlară (studiul HBSC): Rezultate privind hărțuirea și hărțuirea cibernetică. Disponibil la: https://www.who.int/europe/initiatives/health-behaviour-in-school-aged-children-(hbsc)-study
- Hărțuirea cibernetică și tinerii LGBTQ: Revizuire sistematică a literaturii de specialitate și recomandări pentru prevenire și intervenție (2018). Disponibil la: https://pmc.ncbi.nlm.nih.gov/articles/PMC7163911/
- Corelații între dependența de rețelele sociale și anxietate, depresie, teama de a nu rata ceva (FoMO), singurătate și stima de sine în rândul elevilor și studenților: Revizuire sistematică și meta-analiză (2025). PLOS ONE. Disponibil la: https://journals.plos.org/plosone/article?id=10.1371/journal.pone.0329466