CONSCIOUS YOUTH BEHAVIOURS
IN EMERGING REALITIES

R5. Policy Recommendation Paper on Data security and Cyber security, specifically tailored for schools, following the ISO 27001, 27002, 27701, 22301 and 31000 standards

Conscious Youth Behaviours in Emerging Realities

Lead partner: 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.

Πληροφορίες εγγράφου

Συμφωνία επιχορήγησης #	**2023-1-EL01-KA220-SCH-000156982**
Ακρωνύμιο	**C.Y.B.E.R.**
Τίτλος	**Conscious Youth Behaviours in Emerging Realities**
Ημερομηνία Έναρξης:	16/11/2023
Αποτέλεσμα:	Έγγραφο με συστάσεις πολιτικής R5
Σχετικές δραστηριότητες:	A4.5 - Σχεδιασμός και ανάπτυξη του R5
Επικεφαλής οργανισμός:	SIGMA Τουρνής Συμβουλευτική ΕΕ, Ελλάδα
Συνεργαζόμενοι εταίροι:	• PRISM IMPRESA SOCIALE S.R.L., Ιταλία • Νομαρχιακό Κέντρο Εκπαιδευτικών Πόρων και Υποστήριξης Μποτοσάνι, Ρουμανία • CPM-Centrum Prevencie Mladeze, Σλοβακία • Casa Do Professor, Πορτογαλία • Vitale Tecnologie Comunicazione - VITECO SRL, Ιταλία • EUROCERT Ευρωπαϊκή Εταιρεία Εκπαίδευσης και Πιστοποιήσεων Ανώνυμη Εταιρεία, Ελλάδα
Επίπεδο διάδοσης	Δημόσιο
Αποποίηση ευθύνης	Η υποστήριξη της Ευρωπαϊκής Επιτροπής για την έκδοση του παρόντος εντύπου δεν συνιστά έγκριση του περιεχομένου του, το οποίο αντανακλά αποκλειστικά τις απόψεις των συγγραφέων, και η Επιτροπή δεν φέρει καμία ευθύνη για οποιαδήποτε χρήση των πληροφοριών που περιέχονται σε αυτό.

Ιστορικό εγγράφου

Date	Submitted by	Reviewed by	Version (Notes)
26/06/2026	SIGMA	Theodora Ntinou	1.0

Σχετικά με το CYBER	
Τύπος ενέργειας	Erasmus+ KA220-SCH - Συνεργασίες στον τομέα της σχολικής εκπαίδευσης
Προτεραιότητα	ΣΧΟΛΙΚΗ ΕΚΠΑΙΔΕΥΣΗ: Ανάπτυξη βασικών ικανοτήτων ▪ Αντιμετώπιση του ψηφιακού μετασχηματισμού μέσω της ανάπτυξης της ψηφιακής ετοιμότητας, της ανθεκτικότητας και των ικανοτήτων ▪ Ενσωμάτωση και διαφορετικότητα σε όλους τους τομείς της εκπαίδευσης, της κατάρτισης, της νεολαίας και του αθλητισμού

Το έργο στοχεύει να εξετάσει ένα κρίσιμο ερώτημα: Πώς επηρεάζει ο κυβερνοχώρος την ανθρώπινη συμπεριφορά, ιδίως μεταξύ των νέων; Στη σημερινή ψηφιακή εποχή, η διαδικτυακή συμπεριφορά έχει ενσωματωθεί βαθιά στο ψυχολογικό περιβάλλον του κυβερνοχώρου. Προσφέρει μοναδικές ευκαιρίες για τη διαμόρφωση της ανθρώπινης αλληλεπίδρασης, αλλά ταυτόχρονα δημιουργεί ανησυχίες λόγω του χωρίς σύνορα χαρακτήρα της.

Το CYBER επιδιώκει να αναπτύξει την ανθεκτικότητα των ευρωπαϊκών σχολείων στον κυβερνοχώρο, δημιουργώντας εξατομικευμένες διαδικασίες ποιότητας της ΕΕ για το σχολικό σύστημα και εξοπλίζοντας τους εκπαιδευτικούς και τους μαθητές με τα εργαλεία και τις γνώσεις που απαιτούνται για να συζητήσουν τις συνειδητές και ασυνείδητες συμπεριφορές των εφήβων στο διαδίκτυο, την κυβερνοψυχολογία και τις αρνητικές συνέπειες της υπερβολικής χρήσης του Διαδικτύου, με στόχο να ενισχυθεί η κατανόηση μέσα στην τάξη σχετικά με τις επικίνδυνες αναδυόμενες συμπεριφορές στις οποίες μπορεί να υποπέσει ένας νεαρός χρήστης.

Το CYBER πρόκειται να διαμορφώσει μια μεθοδολογία για την ενσωμάτωση των κρίσιμων θεμάτων των κυβερνοαπειλών και της κυβερνοψυχολογίας στην τάξη και στο σχολικό σύστημα, προωθώντας τον διάλογο μεταξύ των μαθητών σχετικά με τις επικίνδυνες αναδυόμενες συμπεριφορές απέναντι στον εαυτό τους και στους συνομηλίκους τους. Επιπλέον, το έργο καθορίζει σαφείς διαδικασίες για την προστασία στον κυβερνοχώρο και την προστασία των δεδομένων, ώστε τα σχολεία να αποκτήσουν την πιστοποίηση CYBER, καθώς και απαιτήσεις για τη θέσπιση, την εφαρμογή, τη διατήρηση και τη βελτίωση της διαχείρισης της ασφάλειας των πληροφοριών στο σχολείο.

Τα αποτελέσματα του έργου προορίζονται να ωφελήσουν κάθε έφηβο σε κάθε ευρωπαϊκή χώρα, ειδικά εκείνους που γεννήθηκαν στην ψηφιακή εποχή. Το κοινωνικό πλαίσιο σε αυτά τα ζητήματα (παραβίαση προφίλ, ψευδείς ειδήσεις, πλαστές ταυτότητες, διαδικτυακή απάτη/εξαπάτηση, διαδικτυακός εκβιασμός, πορνογραφία εκδίκησης, hikikomori, διαδικτυακός εκφοβισμός κ.λπ.) έχει μεγαλύτερη σημασία, καθώς η εκπαίδευση και η ευαισθητοποίηση των νέων σχετικά με το πρόβλημα έχουν πολύ μεγαλύτερο αντίκτυπο από ό,τι ένας εθνικός κανονισμός.

Πίνακας περιεχομένων

Εισαγωγή

Το παρόν έγγραφο αποτελεί την Πολιτική Κυβερνοανθεκτικότητας για τα Σχολεία, η οποία εκπονήθηκε στο πλαίσιο του προγράμματος C.Y.B.E.R. (Conscious Youth Behaviours in Emerging Realities). Το πρόγραμμα συγχρηματοδοτείται από την Ευρωπαϊκή Ένωση στο πλαίσιο του προγράμματος Erasmus+ και συγκεντρώνει οργανισμούς-εταίρους από την Ελλάδα, την Ιταλία, την Πορτογαλία, τη Ρουμανία και τη Σλοβακία.

Σήμερα, τα σχολεία βασίζονται σε μεγάλο βαθμό στην ψηφιακή τεχνολογία. Οι μαθητές χρησιμοποιούν διαδικτυακές πλατφόρμες για να μαθαίνουν, οι εκπαιδευτικοί επικοινωνούν μέσω ψηφιακών εργαλείων και το προσωπικό διαχειρίζεται αρχεία σε συνδεδεμένα συστήματα. Πρόκειται για μια θετική εξέλιξη, αλλά σημαίνει επίσης ότι τα σχολεία αντιμετωπίζουν κινδύνους που δεν αντιμετώπιζαν στο παρελθόν: κυβερνοεπιθέσεις, παραβιάσεις δεδομένων, διαδικτυακό εκφοβισμό και τις επιπτώσεις της ψηφιακής ζωής στην ψυχική υγεία των μαθητών.

Η παρούσα πολιτική έχει σχεδιαστεί για να βοηθήσει κάθε σχολείο στις πέντε χώρες-εταίρους να αντιμετωπίσει αυτές τις προκλήσεις με πρακτικό τρόπο. Συνδυάζει την ευρωπαϊκή νομοθεσία, τους εθνικούς κανόνες κάθε χώρας, τα διεθνώς αναγνωρισμένα πρότυπα ασφάλειας και τις καλύτερες διαθέσιμες ερευνητικές γνώσεις, όλα σε ένα έγγραφο που κάθε σχολείο μπορεί να διαβάσει και να χρησιμοποιήσει.

Δεν πρόκειται για τεχνικό εγχειρίδιο. Είναι ένας οδηγός για όλους όσους εργάζονται σε ένα σχολείο: τον διευθυντή, τους εκπαιδευτικούς, το διοικητικό προσωπικό και τους συντονιστές πληροφορικής. Δεν απαιτείται νομική ή τεχνική κατάρτιση για τη χρήση του. Η πολιτική εξηγεί τι απαιτεί ο νόμος, πώς μοιάζουν οι ορθές πρακτικές και τι πρέπει να κάνει το σχολείο σας.

Τα πρότυπα και τα εργαλεία που παρέχονται στα παραρτήματα έχουν σχεδιαστεί ως ευέλικτα σημεία εκκίνησης. Τα σχολεία ενθαρρύνονται να τα τροποποιήσουν ώστε να ανταποκρίνονται στο εθνικό νομικό πλαίσιο, στις εσωτερικές διαδικασίες και στις συγκεκριμένες συνθήκες τους.

Σε ποιους απευθύνεται η παρούσα πολιτική

Η παρούσα πολιτική απευθύνεται σε όλους όσους εμπλέκονται στη λειτουργία ενός σχολείου: τον διευθυντή, τον υποδιευθυντή, τους εκπαιδευτικούς, τους συντονιστές πληροφορικής, το διοικητικό προσωπικό του σχολείου και τα σχολικά συμβούλια. Έχει συνταχθεί έτσι ώστε να είναι κατανοητή από όλους, ανεξάρτητα από το υπόβαθρό τους.

Πώς είναι δομημένο το παρόν έγγραφο

Μέρος	Περιεχόμενο
Μέρος 1: Το νομικό πλαίσιο	Τι ορίζει η ευρωπαϊκή νομοθεσία ότι πρέπει να κάνουν τα σχολεία, με απλά λόγια.
Μέρος 2: Τι εφαρμόζεται στη χώρα σας	Οι συγκεκριμένοι εθνικοί κανόνες που ισχύουν σε καθεμία από τις πέντε χώρες.

Μέρος	Περιεχόμενο
Διεθνή πρότυπα και σχολεία	Πώς πέντε διεθνώς αναγνωρισμένα πρότυπα διαχείρισης διαμορφώνουν τις πρακτικές συστάσεις της παρούσας πολιτικής.
Μέρος 3: Τι πρέπει να κάνει το σχολείο σας	Πρακτικά μέτρα οργανωμένα ανά θέμα, με βάση τα διεθνή πρότυπα και τη νομοθεσία της ΕΕ.
Μέρος 4: Τι δείχνουν τα στοιχεία	Τι μας δείχνει η επιστημονική έρευνα σχετικά με το τι λειτουργεί πραγματικά στα σχολεία.
Παραρτήματα	Πρότυπα εγγράφων και πρακτικά εργαλεία εφαρμογής που τα σχολεία μπορούν να προσαρμόσουν και να χρησιμοποιήσουν άμεσα.
Βιβλιογραφία	Τα εθνικά νομοθετικά κείμενα και οι επίσημες πηγές που χρησιμοποιήθηκαν για την προετοιμασία του Μέρους 2.

Μέρος 1: Το νομικό πλαίσιο

Τα σχολεία και στις πέντε χώρες-εταίρους πρέπει να τηρούν τους ευρωπαϊκούς νόμους που ρυθμίζουν τον τρόπο διαχείρισης των δεδομένων και την προστασία των μαθητών στο διαδίκτυο. Σε αυτό το μέρος εξηγούνται, με απλή γλώσσα, οι απαιτήσεις αυτών των νόμων. Υπάρχουν έξι βασικά νομικά κείμενα που κάθε σχολείο πρέπει να γνωρίζει. Μαζί καλύπτουν την προστασία των δεδομένων, την κυβερνοασφάλεια, την τεχνητή νοημοσύνη, τις διαδικτυακές πλατφόρμες, τις ψηφιακές επικοινωνίες και την ασφάλεια των ψηφιακών προϊόντων.

1.1 Γενικός Κανονισμός για την Προστασία Δεδομένων (GDPR)

Ο ΓΚΠΔ αποτελεί το θεμέλιο της προστασίας δεδομένων στην Ευρώπη. Ισχύει για κάθε οργανισμό που επεξεργάζεται προσωπικά δεδομένα, συμπεριλαμβανομένων των σχολείων. Σε ένα σχολείο, τα προσωπικά δεδομένα περιλαμβάνουν τα ονόματα και τους αριθμούς ταυτοποίησης των μαθητών, τα αρχεία παρουσίας, τους βαθμούς, τις πληροφορίες υγείας, τις φωτογραφίες και οποιαδήποτε άλλη πληροφορία που σχετίζεται με ένα ταυτοποιήσιμο πρόσωπο.

Ο ΓΚΠΔ αναγνωρίζει τα παιδιά ως μια ιδιαίτερα ευάλωτη ομάδα. Ως εκ τούτου, τα σχολεία πρέπει να εφαρμόζουν υψηλότερα πρότυπα προσοχής κατά την επεξεργασία των δεδομένων των μαθητών σε σύγκριση με αυτά που θα εφάρμοζαν για τους ενήλικες.

Τι απαιτεί ο ΓΚΠΔ από τα σχολεία:

- Τα σχολεία πρέπει να διαθέτουν σαφή νομική βάση για κάθε δραστηριότητα επεξεργασίας δεδομένων. Στις περισσότερες περιπτώσεις, αυτή θα αποτελεί νομική υποχρέωση που επιβάλλεται από την εθνική νομοθεσία για την εκπαίδευση, δημόσιο καθήκον απαραίτητο για τη λειτουργία του σχολείου ή, σε ορισμένες περιπτώσεις, συγκατάθεση.
- Τα σχολεία πρέπει να συλλέγουν μόνο τα δεδομένα που πραγματικά χρειάζονται. Δεν πρέπει να συλλέγουν επιπλέον πληροφορίες απλώς και μόνο επειδή ενδέχεται να φανούν χρήσιμες κάποια μέρα.

● Τα σχολεία πρέπει να ορίσουν έναν Υπεύθυνο Προστασίας Δεδομένων (DPO). Ανάλογα με τη χώρα, αυτό μπορεί να διαχειρίζεται σε επίπεδο αρχής ή ομάδας σχολείων και όχι για κάθε μεμονωμένο σχολείο.

● Τα σχολεία πρέπει να διενεργούν Εκτίμηση Επιπτώσεων στην Προστασία Δεδομένων (DPIA) πριν από την εισαγωγή οποιουδήποτε νέου ψηφιακού συστήματος που συνεπάγεται επεξεργασία δεδομένων μαθητών σε μεγάλη κλίμακα ή παρακολούθηση συμπεριφοράς. Στο Παράρτημα V περιλαμβάνεται ένα πρότυπο.

● Τα σχολεία πρέπει να αναφέρουν τις παραβιάσεις προσωπικών δεδομένων στην εθνική εποπτική αρχή εντός 72 ωρών από τη στιγμή που θα λάβουν γνώση αυτών.

● Τα σχολεία πρέπει να ενημερώνουν τους μαθητές και τους γονείς σχετικά με τον τρόπο χρήσης των δεδομένων τους, με σαφή και απλή γλώσσα.

● Οι μαθητές και οι γονείς έχουν το δικαίωμα πρόσβασης στα δεδομένα που τηρούνται για αυτούς, να ζητήσουν διορθώσεις και, σε ορισμένες περιπτώσεις, να ζητήσουν τη διαγραφή τους.

Ηλικία ψηφιακής συναίνεσης

Ο Γενικός Κανονισμός για την Προστασία Δεδομένων (GDPR) επιτρέπει σε κάθε χώρα της ΕΕ να καθορίζει την ηλικία κατά την οποία ένας νέος μπορεί να συναινέσει στη χρήση ψηφιακών πλατφορμών χωρίς τη συγκατάθεση των γονέων. Η ηλικία αυτή κυμαίνεται από 13 έως 16 έτη στις πέντε χώρες-εταίρους. Για τους μαθητές που δεν έχουν συμπληρώσει την εθνική ηλικία ψηφιακής συναίνεσης, τα σχολεία πρέπει να λάβουν γραπτή συγκατάθεση από τους γονείς ή τον κηδεμόνα πριν από την εγγραφή τους σε ψηφιακές πλατφόρμες. Η συγκεκριμένη ηλικία για κάθε χώρα παρατίθεται στο Μέρος 2.

1.2 Οδηγία NIS2

Η οδηγία NIS2 θεσπίζει ένα κοινό ευρωπαϊκό πλαίσιο για την κυβερνοασφάλεια. Απαιτεί από τους οργανισμούς να εφαρμόζουν επαρκή μέτρα κυβερνοασφάλειας, να διαχειρίζονται τους κινδύνους που ενέχουν οι ψηφιακοί προμηθευτές τους και να αναφέρουν σημαντικά περιστατικά κυβερνοασφάλειας στην εθνική αρχή.

Τα σχολεία δεν κατατάσσονται πάντα άμεσα ως ουσιώδεις ή σημαντικές οντότητες σύμφωνα με την οδηγία NIS2. Ωστόσο, τα σχολεία εξαρτώνται σε μεγάλο βαθμό από ψηφιακά συστήματα, και τα περιστατικά κυβερνοασφάλειας που επηρεάζουν τα συστήματα αυτά μπορούν να διαταράξουν την εκπαίδευση και να θέσουν σε κίνδυνο τα δεδομένα των μαθητών. Το πλαίσιο της οδηγίας NIS2 καθορίζει το πρότυπο προς το οποίο πρέπει να στοχεύουν όλα τα σχολεία, ανεξάρτητα από το αν έχουν ταξινομηθεί επίσημα.

Τι σημαίνει η Οδηγία NIS2 για τα σχολεία:

● Τα σχολεία πρέπει να εφαρμόζουν μέτρα κυβερνοασφάλειας που να ανταποκρίνονται στους κινδύνους που αντιμετωπίζουν. Αυτό σημαίνει, τουλάχιστον, ισχυρούς κωδικούς πρόσβασης, τακτικές δημιουργίες αντιγράφων ασφαλείας και προστατευμένα δίκτυα.

● Τα σχολεία πρέπει να ελέγχουν τις πρακτικές κυβερνοασφάλειας των προμηθευτών ψηφιακών υπηρεσιών τους. Μια πλατφόρμα που χρησιμοποιείται για τα αρχεία των μαθητών πρέπει να είναι εξίσου ασφαλής με το ίδιο το σχολείο.

● Τα σχολεία πρέπει να διαθέτουν διαδικασία για τον εντοπισμό και την αντιμετώπιση περιστατικών κυβερνοασφάλειας. Το προσωπικό πρέπει να γνωρίζει σε ποιον να απευθυνθεί και ποια βήματα να ακολουθήσει.

● Τα σχολεία πρέπει να παρέχουν τακτική εκπαίδευση ευαισθητοποίησης σε θέματα κυβερνοασφάλειας σε όλο το προσωπικό.

● Τα σημαντικά περιστατικά πρέπει να αναφέρονται στην εθνική αρχή κυβερνοασφάλειας. Οι προθεσμίες και οι αρμόδιες αρχές διαφέρουν ανά χώρα. Βλ. Μέρος 2.

1.3 Νόμος της ΕΕ για την Τεχνητή Νοημοσύνη

Ο Νόμος για την Τεχνητή Νοημοσύνη είναι ο πρώτος ολοκληρωμένος ευρωπαϊκός νόμος που ρυθμίζει τη χρήση της τεχνητής νοημοσύνης. Τέθηκε σε ισχύ τον Αύγουστο του 2024 και εφαρμόζεται σταδιακά έως την πλήρη εφαρμογή του τον Αύγουστο του 2026. Τα σχολεία χρησιμοποιούν όλο και περισσότερο εργαλεία που βασίζονται στην τεχνητή νοημοσύνη: πλατφόρμες προσαρμοστικής μάθησης, αυτοματοποιημένα συστήματα βαθμολόγησης, chatbots και αναλυτικά στοιχεία μάθησης. Ο Νόμος για την Τεχνητή Νοημοσύνη θεσπίζει σαφείς κανόνες για το πώς μπορούν και πώς δεν μπορούν να χρησιμοποιηθούν αυτά τα εργαλεία.

Τι απαιτεί ο νόμος για την τεχνητή νοημοσύνη από τα σχολεία:

● Ορισμένες χρήσεις της τεχνητής νοημοσύνης στα σχολεία απαγορεύονται πλήρως. Σε αυτές περιλαμβάνονται τα συστήματα αναγνώρισης συναισθημάτων που χρησιμοποιούνται για την παρακολούθηση των μαθητών, η βιομετρική κατηγοριοποίηση των μαθητών και η αναγνώριση προσώπου σε πραγματικό χρόνο σε εκπαιδευτικά περιβάλλοντα. Δεν υπάρχουν εξαιρέσεις για τα σχολεία.

● Τα συστήματα τεχνητής νοημοσύνης που χρησιμοποιούνται για την αξιολόγηση, την εισαγωγή ή την παρακολούθηση των μαθητών κατατάσσονται ως υψηλού κινδύνου και πρέπει να πληρούν αυστηρές απαιτήσεις όσον αφορά τη διαφάνεια, την ανθρώπινη εποπτεία και την τεκμηρίωση.

● Οι μαθητές και οι γονείς πρέπει να ενημερώνονται όταν τα εργαλεία τεχνητής νοημοσύνης χρησιμοποιούνται με τρόπους που επηρεάζουν τις εκπαιδευτικές αποφάσεις.

● Ένας εκπαιδευτικός πρέπει πάντα να εξετάζει και να αναλαμβάνει την ευθύνη για οποιαδήποτε σύσταση που παράγεται από την τεχνητή νοημοσύνη και επηρεάζει έναν μαθητή. Η τεχνητή νοημοσύνη δεν μπορεί να λαμβάνει τελικές αποφάσεις σχετικά με τους μαθητές.

● Τα σχολεία πρέπει να τηρούν γραπτό κατάλογο όλων των εργαλείων τεχνητής νοημοσύνης που χρησιμοποιούνται, συμπεριλαμβανομένου του τι κάνει κάθε εργαλείο και ποια δεδομένα επεξεργάζεται.

1.4 Νόμος για τις Ψηφιακές Υπηρεσίες (DSA)

Ο DSA ρυθμίζει τις διαδικτυακές πλατφόρμες και τις ψηφιακές υπηρεσίες. Απαιτεί από τις πλατφόρμες να είναι πιο διαφανείς, να παρέχουν προσιτούς τρόπους αναφοράς επιβλαβούς περιεχομένου και να ενισχύουν την προστασία των νέων. Τα σχολεία διαδραματίζουν σημαντικό ρόλο στο να βοηθήσουν τους μαθητές να κατανοήσουν πώς λειτουργούν οι διαδικτυακές πλατφόρμες και πώς να προστατεύουν τον εαυτό τους.

Τι σημαίνει ο νόμος DSA για τα σχολεία:

● Τα σχολεία πρέπει να διδάσκουν στους μαθητές πώς να αναγνωρίζουν και να αναφέρουν επιβλαβές περιεχόμενο στις πλατφόρμες που χρησιμοποιούν.

● Τα σχολεία πρέπει να βοηθούν τους μαθητές να κατανοήσουν πώς λειτουργούν οι αλγόριθμοι προτάσεων και πώς επηρεάζουν το περιεχόμενο που βλέπουν οι νέοι στο διαδίκτυο.

● Οι εκπαιδευτικοί πρέπει να γνωρίζουν τις υποχρεώσεις που επιβάλλει ο νόμος DSA στις μεγάλες πλατφόρμες και να είναι σε θέση να τις συζητούν με τους μαθητές στο πλαίσιο της εκπαίδευσης στην ψηφιακή παιδεία.

1.5 Οδηγία για την προστασία της ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες

Η οδηγία για την προστασία της ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες (ePrivacy) προστατεύει το απόρρητο των ηλεκτρονικών επικοινωνιών. Ισχύει για συστήματα ηλεκτρονικού ταχυδρομείου, πλατφόρμες ανταλλαγής μηνυμάτων, εργαλεία τηλεδιάσκεψης και οποιαδήποτε άλλη υπηρεσία ψηφιακής επικοινωνίας που χρησιμοποιείται στα σχολεία.

Τι σημαίνει η Οδηγία για την προστασία της ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες (ePrivacy) για τα σχολεία:

● Οι ψηφιακές επικοινωνίες μεταξύ μαθητών, γονέων, εκπαιδευτικών και διοικητικού προσωπικού πρέπει να είναι ασφαλείς και εμπιστευτικές.

● Τα εργαλεία τηλεδιάσκεψης που χρησιμοποιούνται για την εξ αποστάσεως μάθηση πρέπει να ρυθμίζονται έτσι ώστε να αποτρέπεται η μη εξουσιοδοτημένη πρόσβαση. Οι εικονικές αίθουσες διδασκαλίας πρέπει να απαιτούν σύνδεση πριν μπορέσει κάποιος να συμμετάσχει.

● Τα μαθήματα και οι συναντήσεις δεν πρέπει να καταγράφονται χωρίς τη ρητή συγκατάθεση όλων των συμμετεχόντων.

● Οι ιστοσελίδες και οι πλατφόρμες των σχολείων που χρησιμοποιούν cookies πρέπει να εμφανίζουν μια ειδοποίηση σχετικά με τα cookies που συμμορφώνεται με τη νομοθεσία.

1.6 Νόμος για την Κυβερνοασφάλεια

Ο νόμος για την κυβερνοασφάλεια ενισχύει τον ρόλο της ENISA, του Οργανισμού της ΕΕ για την Κυβερνοασφάλεια, και θεσπίζει ένα ευρωπαϊκό πλαίσιο για την πιστοποίηση της ασφάλειας των ψηφιακών προϊόντων και υπηρεσιών. Υποστηρίζει την υιοθέτηση αξιόπιστων τεχνολογιών σε ολόκληρη την ΕΕ, μεταξύ άλλων και στα σχολεία.

Τι σημαίνει ο Νόμος για την Κυβερνοασφάλεια για τα σχολεία:

● Όταν τα σχολεία επιλέγουν ψηφιακά εργαλεία, πλατφόρμες ή εξοπλισμό, θα πρέπει να λαμβάνουν υπόψη την κυβερνοασφάλεια και, όπου είναι δυνατόν, να προτιμούν πιστοποιημένα ή εγκεκριμένα προϊόντα.

● Οι συνδεδεμένες συσκευές στις αίθουσες διδασκαλίας, όπως οι έξυπνοι πίνακες, τα tablet και οι κάμερες, θα πρέπει να ρυθμίζονται με ασφάλεια και να ενημερώνονται τακτικά.

● Τα σχολεία μπορούν να συμβουλεύονται τις οδηγίες και τα εργαλεία της ENISA για να σχεδιάσουν την προσέγγισή τους όσον αφορά την κυβερνοασφάλεια.

1.7 Πώς λειτουργούν από κοινού αυτοί οι νόμοι

Αυτά τα έξι νομικά κείμενα δεν αποτελούν ξεχωριστές υποχρεώσεις που πρέπει να αντιμετωπιστούν μία προς μία. Αποτελούν ένα ολοκληρωμένο πλαίσιο. Ένα σχολείο που προστατεύει τα δεδομένα των μαθητών σύμφωνα με το GDPR, διαχειρίζεται την κυβερνοασφάλεια σύμφωνα με τον NIS2, χρησιμοποιεί την τεχνητή νοημοσύνη υπεύθυνα σύμφωνα με τον Νόμο για την Τεχνητή Νοημοσύνη, διδάσκει ψηφιακή παιδεία σύμφωνα με τον DSA, διασφαλίζει τις επικοινωνίες του σύμφωνα με την Οδηγία για την Ηλεκτρονική Ιδιωτικότητα και επιλέγει αξιόπιστες τεχνολογίες σύμφωνα με τον Νόμο για την Κυβερνοασφάλεια θα έχει εκπληρώσει το σύνολο των νομικών του υποχρεώσεων.

Νόμος	Η βασική υποχρέωση των σχολείων
GDPR	Προστατεύστε τα προσωπικά δεδομένα, ορίστε έναν υπεύθυνο προστασίας δεδομένων (DPO), λάβετε τη συγκατάθεση όπου απαιτείται, αναφέρετε τις παραβιάσεις εντός 72 ωρών.
Οδηγία NIS2	Εφαρμόστε μέτρα κυβερνοασφάλειας, ελέγξτε τους προμηθευτές σας, αναφέρετε τα περιστατικά, εκπαιδεύστε το προσωπικό σας.
Νόμος της ΕΕ για την Τεχνητή Νοημοσύνη	Μην χρησιμοποιείτε απαγορευμένη τεχνητή νοημοσύνη, αφήστε τους ανθρώπους να λαμβάνουν τις αποφάσεις, ενημερώστε τους μαθητές και τους γονείς.
Νόμος για τις Ψηφιακές Υπηρεσίες (DSA)	Διδάξτε στους μαθητές να αναφέρουν επιβλαβές περιεχόμενο και να κατανοούν τον τρόπο λειτουργίας των αλγορίθμων.
Οδηγία για την προστασία της ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες (ePrivacy)	Εξασφαλίστε την ασφάλεια των ψηφιακών επικοινωνιών, προστατεύστε τις εικονικές αίθουσες διδασκαλίας, τηρείτε τους κανόνες για τα cookies.
Νόμος για την Κυβερνοασφάλεια	Λάβετε υπόψη την ασφάλεια κατά την αγορά τεχνολογικού εξοπλισμού, εξασφαλίστε την ασφάλεια των συνδεδεμένων συσκευών, ακολουθήστε τις οδηγίες της ENISA.

Μέρος 2: Τι ισχύει στη χώρα σας

Η ευρωπαϊκή νομοθεσία καθορίζει το κοινό πλαίσιο, αλλά κάθε χώρα διαθέτει επίσης τους δικούς της εθνικούς νόμους και οδηγίες, τους οποίους πρέπει να τηρούν τα σχολεία. Σε αυτό το τμήμα συνοψίζονται οι σημαντικότεροι εθνικοί κανόνες για καθεμία από τις πέντε χώρες-εταίρους. Βρείτε τη χώρα σας και ενημερωθείτε για το τι ισχύει στην περίπτωσή σας.

2.1 Ελλάδα

Η Ελλάδα εφαρμόζει ένα εξαιρετικά συγκεντρωτικό μοντέλο ψηφιακής διακυβέρνησης των σχολείων. Η κυβερνοασφάλεια, η προστασία των δεδομένων και η ψηφιακή υποδομή διαχειρίζονται κυρίως σε εθνικό επίπεδο από το Υπουργείο Παιδείας και το Υπουργείο Ψηφιακής Διακυβέρνησης. Τα μεμονωμένα σχολεία λειτουργούν κυρίως ως χρήστες συστημάτων που διαχειρίζονται κεντρικά, όπως το σύστημα πληροφοριών μαθητών «MySchool», η πλατφόρμα μάθησης «e-Class» και το Πανελλήνιο Σχολικό Δίκτυο (PSN).

Τομέας	Τι σημαίνει αυτό για τα σχολεία
Μεταφορά της οδηγίας NIS2 Νόμος 5160/2024	• Τα σχολεία πρέπει να εφαρμόζουν μέτρα διαχείρισης κινδύνων και να διασφαλίζουν ότι οι ψηφιακές πλατφόρμες τρίτων (π.χ. Webex) συμμορφώνονται με τα πρότυπα κυβερνοασφάλειας.

Τομέας	Τι σημαίνει αυτό για τα σχολεία
Υπουργική Απόφαση 1689/2025 Υπουργική Απόφαση 1899/2025	• Υποχρεωτική αναφορά περιστατικών: τα σχολεία πρέπει να ενημερώνουν την Εθνική Αρχή Κυβερνοασφάλειας (ΕΑΚΕ) για σημαντικά περιστατικά κυβερνοασφάλειας. • Απαιτούνται επίσημες πολιτικές ασφάλειας που να καλύπτουν τον έλεγχο πρόσβασης στα δεδομένα των μαθητών, τις διαδικασίες δημιουργίας αντιγράφων ασφαλείας, την κρυπτογράφηση των επικοινωνιών και την ασφάλεια της αλυσίδας εφοδιασμού για το λογισμικό και τον εξοπλισμό που χρησιμοποιούνται στα σχολεία. • Απαιτείται εκπαίδευση του προσωπικού και τήρηση καλών πρακτικών στον κυβερνοχώρο: το προσωπικό των σχολείων αποτελεί συχνό στόχο επιθέσεων ηλεκτρονικού ψαρέματος (phishing) και κοινωνικής μηχανικής. • Τα σχολεία πρέπει να τηρούν τεκμηρίωση που περιλαμβάνει πολιτικές ασφάλειας, αρχεία εκπαίδευσης, διαγράμματα δικτύου και αποτελέσματα περιοδικών ελέγχων ασφάλειας. • Η υπουργική απόφαση 1899/2025 απαιτεί τον ορισμό ενός υπεύθυνου για την κυβερνοασφάλεια καθώς και επίσημες διαδικασίες αντιμετώπισης και αναφοράς περιστατικών.
Προστασία Δεδομένων Νόμος 4624/2019	• Ρυθμίζει την επεξεργασία δεδομένων προσωπικού χαρακτήρα από φορείς του δημόσιου τομέα, συμπεριλαμβανομένων των σχολείων, σύμφωνα με τις αρχές του Γενικού Κανονισμού για την Προστασία Δεδομένων (GDPR). • Καθορίζει τον ρόλο και τις εποπτικές εξουσίες της Ελληνικής Αρχής Προστασίας Δεδομένων (ΕΑΠΔ). • Οι αρμοδιότητες του Υπεύθυνου Προστασίας Δεδομένων (DPO) διαχειρίζονται σε επίπεδο Αρχής και όχι σε επίπεδο κάθε μεμονωμένου σχολείου. • Τα σχολεία πρέπει να ενημερώνουν την ΕΑΠΔ (Ελληνική Αρχή Προστασίας Δεδομένων) εντός 72 ωρών για οποιαδήποτε παραβίαση προσωπικών δεδομένων που ενδέχεται να δημιουργήσει κίνδυνο για τα φυσικά πρόσωπα. • Τα σχολεία πρέπει να εφαρμόζουν τα κατάλληλα μέτρα ασφαλείας για τα δεδομένα των μαθητών, των γονέων και του προσωπικού.
Ηλικία ψηφιακής συναίνεσης	• 15 ετών. • Τα σχολεία πρέπει να λαμβάνουν γραπτή συγκατάθεση από τους γονείς ή τους κηδεμόνες πριν εγγράψουν μαθητές κάτω των 15 ετών σε οποιαδήποτε ψηφιακή πλατφόρμα που επεξεργάζεται τα προσωπικά τους δεδομένα.

Τομέας	Τι σημαίνει αυτό για τα σχολεία
Διαδικτυακός εκφοβισμός Νόμος 5029/2023	• Παρέχει ένα δομημένο νομικό πλαίσιο για την πρόληψη και τη διαχείριση του διαδικτυακού εκφοβισμού στα σχολεία. • Εισάγει την εθνική πλατφόρμα αναφοράς stop-bullying.gov.gr για την επίσημη υποβολή και παρακολούθηση περιστατικών. • Τα σχολεία πρέπει να συμμετέχουν ενεργά στον εντοπισμό, την αναφορά και τη διαχείριση των περιπτώσεων διαδικτυακού εκφοβισμού. • Τα σχολεία πρέπει να διαθέτουν γραπτή διαδικασία για την αντιμετώπιση περιστατικών διαδικτυακού εκφοβισμού.
Κινητά τηλέφωνα	• Απαγορεύεται στους μαθητές να έχουν στην κατοχή τους ή να χρησιμοποιούν κινητά τηλέφωνα εντός των σχολικών εγκαταστάσεων. • Η πολιτική μηδενικής ανοχής ισχύει από το 2024. • Οι παραβάσεις συνεπάγονται άμεσες πειθαρχικές κυρώσεις, συμπεριλαμβανομένης της αποβολής.
Η τεχνητή νοημοσύνη στην εκπαίδευση	• Δεν έχουν εκδοθεί συγκεκριμένες εθνικές κατευθυντήριες γραμμές για τη χρήση της τεχνητής νοημοσύνης στα σχολεία. • Ο νόμος της ΕΕ για την τεχνητή νοημοσύνη εφαρμόζεται άμεσα. • Τα σχολεία θα πρέπει να επιδεικνύουν προσοχή κατά τη χρήση εργαλείων τεχνητής νοημοσύνης που επεξεργάζονται δεδομένα μαθητών.
Ψηφιακή υποδομή	• MySchool: εθνικό σύστημα πληροφοριών για τους μαθητές, το οποίο διαχειρίζεται κεντρικά. • e-Class: εθνική πλατφόρμα διαχείρισης της μάθησης. • Πανελλήνιο Σχολικό Δίκτυο (PSN): ασφαλής εθνική υποδομή συνδεσιμότητας για όλα τα δημόσια σχολεία.
Βασικές επικοινωνίες	• Κυβερνοασφάλεια: EAKE (cyber.gov.gr) • Προστασία δεδομένων: Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (dpa.gr) • Κυβερνοεκφοβισμός: stop-bullying.gov.gr

2.2 Ιταλία

Η Ιταλία εφαρμόζει ένα κατά κύριο λόγο συγκεντρωτικό μοντέλο, αν και τα σχολεία διατηρούν κάποιο βαθμό οργανωτικής αυτονομίας. Η Εθνική Υπηρεσία Κυβερνοασφάλειας (ACN) διαδραματίζει κεντρικό ρόλο στον συντονισμό και τη διαχείριση περιστατικών. Τα σχολεία εξαρτώνται σε μεγάλο βαθμό από τις υπουργικές κατευθυντήριες οδηγίες και τις κεντρικά διαχειριζόμενες πλατφόρμες, συμπεριλαμβανομένης της εθνικής πλατφόρμας Unica. Η Garante έχει εκδώσει ειδικές για τα σχολεία κατευθυντήριες οδηγίες και συχνές ερωτήσεις, τις οποίες τα σχολεία θα πρέπει να συμβουλεύονται παράλληλα με τον GDPR.

Τομέας	Τι σημαίνει αυτό για τα σχολεία
Μεταφορά της οδηγίας NIS2 Νομοθετικό διάταγμα 138/2024 Νόμος 109/2021	• Το νομοθετικό διάταγμα 138/2024 καθορίζει τις απαιτήσεις όσον αφορά την εκτίμηση κινδύνων, την ασφάλεια των προμηθευτών και την αναφορά περιστατικών, ακόμη και για σχολεία που δεν έχουν ταξινομηθεί άμεσα ως οντότητες NIS. • Τα σχολεία πρέπει να διαχειρίζονται τις υπηρεσίες Τεχνολογίες Πληροφορίας και Επικοινωνιών (ΤΠΕ) τρίτων και να διατηρούν δομημένα κανάλια αναφοράς όταν τα περιστατικά επηρεάζουν τις εκπαιδευτικές δραστηριότητες ή τα δεδομένα των μαθητών. • Ο νόμος 109/2021 ιδρύει την Εθνική Υπηρεσία Κυβερνοασφάλειας (ACN), η οποία διαδραματίζει κεντρικό συντονιστικό ρόλο στη διακυβέρνηση της κυβερνοασφάλειας σε όλους τους δημόσιους φορείς, συμπεριλαμβανομένων των σχολείων.
Προστασία Δεδομένων Νομοθετικό διάταγμα 196/2003 (όπως τροποποιήθηκε με το διάταγμα 101/2018)	• Ρυθμίζει την επεξεργασία των δεδομένων μαθητών, γονέων, εκπαιδευτικών και προσωπικού στο πλαίσιο των σχολικών δραστηριοτήτων. • Η εποπτική αρχή είναι η Ιταλική Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα. • Ο διορισμός Υπεύθυνου Προστασίας Δεδομένων (DPO) είναι υποχρεωτικός για τα δημόσια σχολεία, αλλά μπορεί να οργανωθεί σε επίπεδο σχολείου ή μέσω κοινών ρυθμίσεων μεταξύ πολλαπλών σχολείων. • Απαιτείται γονική συγκατάθεση για την επεξεργασία των δεδομένων των παιδιών, όταν παρέχονται ψηφιακές υπηρεσίες απευθείας σε μαθητές κάτω της ηλικίας ψηφιακής συγκατάθεσης. • Τα σχολεία πρέπει να ενημερώνουν τους μαθητές και τους γονείς σχετικά με τα δικαιώματά τους όσον αφορά τα δεδομένα και να διαχειρίζονται τις παραβιάσεις δεδομένων σύμφωνα με τις απαιτήσεις του ΓΚΠΔ.
Ηλικία ψηφιακής συναίνεσης	• 14 ετών. • Για μαθητές κάτω των 14 ετών απαιτείται γονική συγκατάθεση για την εγγραφή σε συστήματα διαχείρισης μάθησης, τη δημοσίευση φωτογραφιών και οποιαδήποτε επεξεργασία δεδομένων που αφορά ανηλίκους σε εκπαιδευτικό περιβάλλον.
Διαδικτυακός εκφοβισμός Νόμος 71/2017	• Παρέχει ένα νομικό πλαίσιο για την καταπολέμηση του διαδικτυακού εκφοβισμού στα σχολεία. • Τα σχολεία πρέπει να διαθέτουν γραπτές διαδικασίες για τη διαχείριση περιστατικών και την υποστήριξη των θυμάτων.

Τομέας	Τι σημαίνει αυτό για τα σχολεία
	• Τα σχολεία μπορούν να ζητήσουν την αφαίρεση επιβλαβούς περιεχομένου από διαδικτυακές πλατφόρμες.
Κινητά Τηλέφωνα MIM Υπόμνημα 5274/2024 MIM Εγκύκλιος 3392/2025	• Η χρήση των smartphone απαγορεύεται κατά τη διάρκεια όλων των σχολικών δραστηριοτήτων σε όλους τους εκπαιδευτικούς κύκλους. • Οι περιορισμοί αποσκοπούν στην προστασία του εκπαιδευτικού περιβάλλοντος και στην προώθηση της κατάλληλης για την ηλικία χρήσης των ψηφιακών εργαλείων. • Ισχύουν περιορισμένες εξαιρέσεις για συγκεκριμένες εκπαιδευτικές δραστηριότητες ή ανάγκες προσβασιμότητας.
Η ΤΝ στην Εκπαίδευση Υπουργική Απόφαση 166/2025	• Οι εθνικές κατευθυντήριες γραμμές απαιτούν διαφάνεια όσον αφορά τη χρήση της τεχνητής νοημοσύνης στα σχολεία. • Η ανθρώπινη εποπτεία των εκπαιδευτικών αποφάσεων που υποστηρίζονται από την τεχνητή νοημοσύνη είναι υποχρεωτική. • Τα εργαλεία τεχνητής νοημοσύνης που επεξεργάζονται δεδομένα μαθητών πρέπει να συμμορφώνονται με τις απαιτήσεις του ΓΚΠΔ.
Ψηφιακές πλατφόρμες	• Unica: εθνική πλατφόρμα για διοικητικές και εκπαιδευτικές λειτουργίες. • Microsoft 365 for Education: σουίτα εφαρμογών που διαχειρίζεται το εκπαιδευτικό ίδρυμα, για διδασκαλία και επικοινωνία. • Το πλαίσιο της Ψηφιακής Ολοκληρωμένης Διδασκαλίας (DDI) (Υπουργική Απόφαση 89/2020) απαιτεί από τα σχολεία να ρυθμίζουν τη χρήση των ψηφιακών πλατφορμών, την πρόσβαση των μαθητών και τις ευθύνες των εκπαιδευτικών στα διαδικτυακά εκπαιδευτικά περιβάλλοντα.
Βασικές επικοινωνίες	• Κυβερνοασφάλεια: ACN (acn.gov.it) • Προστασία δεδομένων: Garante (garanteprivacy.it)

2.3 Πορτογαλία

Η Πορτογαλία διαθέτει ένα από τα πιο δομημένα εθνικά πλαίσια για την ψηφιακή διακυβέρνηση των σχολείων μεταξύ των πέντε χωρών. Τα σχολεία επωφελούνται από το υποχρεωτικό PADDE (Σχέδιο Δράσης για την Ψηφιακή Ανάπτυξη των Σχολείων), το πρόγραμμα υποστήριξης SeguraNet και το CERT.PT για την αντιμετώπιση περιστατικών. Η οδηγία NIS2 μεταφέρθηκε στο εθνικό δίκαιο μέσω του νομοθετικού διατάγματος 125/2025, το οποίο τέθηκε σε ισχύ στις 3 Απριλίου 2026.

Τομέας	Τι σημαίνει αυτό για τα σχολεία
Μεταφορά της Οδηγίας NIS2 Νομοθετικό διάταγμα 125/2025 (σε ισχύ από τις 3 Απριλίου 2026) Νόμος 46/2018	• Τα σχολεία που πληρούν τις προϋποθέσεις ως «Σχετικοί Δημόσιοι Φορείς» (Ομάδα Α ή Β) πρέπει να εφαρμόζουν μέτρα διαχείρισης κινδύνων στον τομέα της κυβερνοασφάλειας. • Υποχρεωτικός διορισμός υπεύθυνου για θέματα κυβερνοασφάλειας. • Τα σημαντικά περιστατικά πρέπει να αναφέρονται στην CNCS εντός 24 ωρών. • Τα σχολεία πρέπει να προσδιορίσουν τα κρίσιμα ψηφιακά περιουσιακά στοιχεία, να θεσπίσουν διαδικασίες αντιμετώπισης συμβάντων και να διασφαλίσουν τη συνέχεια των λειτουργιών. • Ο νόμος 46/2018 παραμένει το θεμελιώδες πλαίσιο που καθιερώνει την CNCS ως την εθνική αρχή για την κυβερνοασφάλεια.
Προστασία δεδομένων Νόμος 58/2019	• Ο διορισμός Υπεύθυνου Προστασίας Δεδομένων (DPO) είναι υποχρεωτικός σε επίπεδο κάθε σχολικού συγκροτήματος (agrupamento de escolas) και όχι σε επίπεδο μεμονωμένων σχολείων. • Ο Υπεύθυνος Προστασίας Δεδομένων (DPO) πρέπει να είναι εγγεγραμμένος στην CNPD (Comissão Nacional de Proteção de Dados) και είναι υπεύθυνος για την παρακολούθηση της συμμόρφωσης με τον ΓΚΠΔ, την παροχή συμβουλών στο προσωπικό, τη διεξαγωγή εκπαιδεύσεων και τη συνεργασία με την CNPD. • Τα σχολεία πρέπει να ενημερώνουν την CNPD εντός 72 ωρών σε περίπτωση παραβίασης προσωπικών δεδομένων που ενδέχεται να θέσει σε κίνδυνο τα φυσικά πρόσωπα. • Τα σχολεία πρέπει να τηρούν μητρώο δραστηριοτήτων επεξεργασίας και να εφαρμόζουν τα κατάλληλα μέτρα ασφαλείας.
Ηλικία ψηφιακής συναίνεσης	• 13 έτη. Πρόκειται για το χαμηλότερο όριο μεταξύ των πέντε χωρών. • Απαιτείται επαληθεύσιμη συγκατάθεση των γονέων ή του κηδεμόνα πριν από την εγγραφή μαθητών ηλικίας κάτω των 13 ετών σε οποιαδήποτε ψηφιακή πλατφόρμα ή διαδικτυακό εργαλείο που επεξεργάζεται προσωπικά δεδομένα. • Αυτό ισχύει για τα συστήματα διαχείρισης μάθησης, τη δημοσίευση φωτογραφιών και κάθε είδους επεξεργασία που αφορά ανηλίκους.
Διαδικτυακός εκφοβισμός	• Το SeguraNet (το οποίο διαχειρίζεται η DGE σε συνεργασία με το CNCS) παρέχει συγκεκριμένες οδηγίες για την

Τομέας	Τι σημαίνει αυτό για τα σχολεία
Πρόγραμμα SeguraNet	πρόληψη και την αντιμετώπιση του διαδικτυακού εκφοβισμού. • Τα σχολεία πρέπει να ενσωματώσουν την πρόληψη του διαδικτυακού εκφοβισμού στο PADDE και στους εσωτερικούς κανονισμούς τους. • Πρότυπα εγγράφων για τις διαδικασίες αντιμετώπισης περιστατικών και την Πολιτική Αποδεκτής Χρήσης διατίθενται μέσω του SeguraNet.
Κινητά Τηλέφωνα Νομοθετικό διάταγμα 95/2025 (σε ισχύ από τον Σεπτέμβριο του 2025)	• Η χρήση smartphone απαγορεύεται νομικά για όλους τους μαθητές των τάξεων 1 έως 6 σε όλα τα δημόσια και ιδιωτικά σχολεία. • Για τον 3ο κύκλο και τη δευτεροβάθμια εκπαίδευση, το Υπουργείο έχει εκδώσει συστάσεις που ενθαρρύνουν την επιβολή περιορισμών, ενώ τα σχολεία διατηρούν την αυτονομία να θεσπίζουν κανόνες στους εσωτερικούς τους κανονισμούς. • Οποιαδήποτε καταγραφή μαθητών απαιτεί ρητή συγκατάθεση σύμφωνα με τον Γενικό Κανονισμό για την Προστασία Δεδομένων (GDPR).
Υποχρεωτικό σχέδιο ψηφιακής μεταρρύθμισης των σχολείων Πλαίσιο PADDE	• Κάθε σχολικό σύμπλεγμα πρέπει να καταρτίζει και να τηρεί ένα PADDE (Σχέδιο Δράσης για την Ψηφιακή Ανάπτυξη του Σχολείου). • Το PADDE πρέπει να περιλαμβάνει ρητά μέτρα κυβερνοασφάλειας και να καλύπτει τρεις διαστάσεις: οργανωτική (ηγεσία και διακυβέρνηση), παιδαγωγική (ψηφιακή ιθαγένεια και εκπαίδευση για την ασφαλή χρήση του διαδικτύου) και τεχνολογική (υποδομή και ασφάλεια). • Τα σχολεία πρέπει να υιοθετήσουν μια Πολιτική Αποδεκτής Χρήσης και να θεσπίσουν διαδικασίες αντιμετώπισης περιστατικών, σε συντονισμό με το CERT.PT.
Η τεχνητή νοημοσύνη στην εκπαίδευση	• Δεν έχουν εκδοθεί ακόμη συγκεκριμένες εθνικές κατευθυντήριες γραμμές. • Ο νόμος της ΕΕ για την τεχνητή νοημοσύνη (AI Act) εφαρμόζεται άμεσα. • Η Γενική Διεύθυνση Εκπαίδευσης (DGE) έχει αναγνωρίσει την ανάγκη για ένα εθνικό πλαίσιο και αναμένεται να εκδώσει συστάσεις. • Τα σχολεία θα πρέπει να επιδεικνύουν προσοχή κατά τη χρήση εργαλείων τεχνητής νοημοσύνης που επεξεργάζονται δεδομένα μαθητών.
Ψηφιακή υποδομή	• RCTS (υπό τη διαχείριση του FCCN): εθνικό ασφαλές δίκτυο υψηλής ταχύτητας για όλες τις σχολικές ομάδες των δημόσιων σχολείων.

Τομέας	Τι σημαίνει αυτό για τα σχολεία
	• Microsoft 365 for Education: σουίτα εφαρμογών που διαχειρίζεται σε εθνικό επίπεδο για διδασκαλία και επικοινωνία. • CERT.PT (υπό τη διαχείριση του CNCS): εθνικό CSIRT και σημείο επαφής για την αντιμετώπιση περιστατικών στον τομέα της εκπαίδευσης.
Βασικές επικοινωνίες	• Κυβερνοασφάλεια: CNCS (cncs.gov.pt) • Αντιμετώπιση περιστατικών: CERT.PT • Προστασία δεδομένων: CNPD (cnpd.pt) • Ψηφιακή ασφάλεια: SeguraNet (seguranet.pt)

2.4 Ρουμανία

Το εθνικό πλαίσιο συντονίζεται από το Υπουργείο Παιδείας σε συνεργασία με την Εθνική Διεύθυνση Κυβερνοασφάλειας (DNSC), στο πλαίσιο της ευρύτερης εθνικής και ευρωπαϊκής πολιτικής για την κυβερνοασφάλεια. Σε πολλά σχολεία, τις αρμοδιότητες που σχετίζονται με την κυβερνοασφάλεια αναλαμβάνει ο διευθυντής του σχολείου, ο συντονιστής ΤΠΕ ή ένας καθορισμένος εκπαιδευτικός, καθώς το εξειδικευμένο προσωπικό στον τομέα της κυβερνοασφάλειας είναι σπάνιο. Η Ρουμανία αντιμετωπίζει μερικά από τα μεγαλύτερα κενά στην εφαρμογή μεταξύ των πέντε χωρών-εταίρων, αλλά παρατηρείται αυξανόμενη δυναμική για την αντιμετώπισή τους.

Τομέας	Τι σημαίνει αυτό για τα σχολεία
Μεταφορά της Οδηγίας NIS2 Επείγουσα Κυβερνητική Διάταξη (OUG) αριθ. 155/2024 (εγκρίθηκε με τον Νόμο 124/2025) Νόμος 58/2023	• Η Επείγουσα Κυβερνητική Διάταξη (OUG) αριθ. 155/2024, εφαρμόζεται άμεσα στην τριτοβάθμια εκπαίδευση. Όσον αφορά τα προπανεπιστημιακά εκπαιδευτικά ιδρύματα, η εφαρμογή της δεν είναι απολύτως σαφής, αλλά τα ιδρύματα που συνδέονται με κυβερνητικά δίκτυα (π.χ. SIIIR) αναμένεται να ακολουθούν τα πρωτόκολλα NIS2. • Τα εκπαιδευτικά ιδρύματα αναμένεται να αναφέρουν σημαντικά περιστατικά στο DNSC εντός 24 ωρών μέσω της πλατφόρμας PNRISC. • Τα απαιτούμενα μέτρα περιλαμβάνουν: τμηματοποίηση του δικτύου (ξεχωριστό Wi-Fi για τη διοίκηση και τους μαθητές), έλεγχο ταυτότητας πολλαπλών παραγόντων για την πρόσβαση σε επίσημες πλατφόρμες, πολιτικές ανάλυσης κινδύνων και υποχρεωτική εκπαίδευση σε θέματα κυβερνοασφάλειας για όλο το προσωπικό. • Ασφάλεια της εφοδιαστικής αλυσίδας: οι ιδιωτικοί πάροχοι πλατφορμών ηλεκτρονικής μάθησης ή λογισμικού λογιστικής που χρησιμοποιούνται από τα σχολεία πρέπει να συμμορφώνονται με το NIS2. • Ο νόμος 58/2023 ορίζει ότι η ευθύνη για την κυβερνοασφάλεια βαρύνει τον φορέα που κατέχει ή

Τομέας	Τι σημαίνει αυτό για τα σχολεία
	διαχειρίζεται το δίκτυο, καθιστώντας τη διοίκηση του σχολείου άμεσα υπεύθυνη.
Προστασία δεδομένων Νόμος 190/2018	• Τα σχολεία θεωρούνται ανεξάρτητοι υπεύθυνοι επεξεργασίας δεδομένων και πρέπει να διασφαλίζουν την πλήρη συμμόρφωση με τον ΓΚΠΔ. • Επιτρέπεται η ρύθμιση κοινής θέσης υπεύθυνου προστασίας δεδομένων (DPO) σε επίπεδο νομαρχιακής επιθεώρησης ή σε κεντρικό επίπεδο. • Τα σχολεία πρέπει να εφαρμόζουν υποχρεωτικές διαδικασίες γονικής συγκατάθεσης για τις πλατφόρμες ηλεκτρονικής μάθησης και για τη χρήση εικόνων των μαθητών. • Η βιντεοεπιτήρηση επιτρέπεται μόνο για την προστασία προσώπων και περιουσίας, με υποχρεωτική ενημέρωση των μαθητών, των εκπαιδευτικών και των επισκεπτών. Οι εγγραφές δεν πρέπει να διατηρούνται για περισσότερο από 30 ημέρες, εκτός από περιπτώσεις που αποτελούν αντικείμενο έρευνας. • Τα αποτελέσματα των εξετάσεων πρέπει να δημοσιεύονται με ανωνυμοποίηση ή ψευδωνυμοποίηση, σύμφωνα με τις κατευθυντήριες γραμμές της Εθνικής Εποπτικής Αρχής Επεξεργασίας Δεδομένων Προσωπικού Χαρακτήρα της Ρουμανίας (ANSPDCP).
Ηλικία ψηφιακής συναίνεσης	• 16 έτη. Αυτό είναι το υψηλότερο όριο μεταξύ των πέντε χωρών. • Απαιτείται η συγκατάθεση των γονέων ή του κηδεμόνα πριν από την εγγραφή μαθητών κάτω των 16 ετών σε οποιαδήποτε ψηφιακή πλατφόρμα. • Στην πράξη, αυτό ισχύει για σχεδόν όλα τα ψηφιακά εκπαιδευτικά εργαλεία που χρησιμοποιούνται στα ρουμάνικα σχολεία.
Διαδικτυακός εκφοβισμός ROFUIP 2025/2026 Κανονισμός Φοιτητών (Απόφαση 5707/2024)	• Ο Κανονισμός-Πλαίσιο Οργάνωσης και Λειτουργίας Μονάδων Προπανεπιστημιακής Εκπαίδευσης της Ρουμανίας (ROFUIP) ορίζει και επιβάλλει κυρώσεις για τον διαδικτυακό εκφοβισμό ως απαγορευμένη συμπεριφορά εντός του σχολικού περιβάλλοντος. • Απαγορεύεται η μη εξουσιοδοτημένη βιντεοσκόπηση ή ηχογράφηση των διδακτικών δραστηριοτήτων. • Το προσωπικό πρέπει να χρησιμοποιεί μόνο επίσημα εγκεκριμένα ψηφιακά εργαλεία και να χειρίζεται τα δεδομένα των μαθητών με αυστηρή εμπιστευτικότητα. • Ο Κανονισμός Μαθητών απαγορεύει ρητά κάθε μορφή επιθετικής συμπεριφοράς στο εικονικό περιβάλλον. • Δεν υπάρχει ειδική εθνική πλατφόρμα αναφοράς. Τα περιστατικά αντιμετωπίζονται μέσω του σχολείου και

Τομέας	Τι σημαίνει αυτό για τα σχολεία
	παραπέμπονται στην Εθνική Εποπτική Αρχή Επεξεργασίας Δεδομένων Προσωπικού Χαρακτήρα της Ρουμανίας (ANSPDCP) όταν εμπλέκονται προσωπικά δεδομένα.
Κινητά Τηλέφωνα Νόμος 198/2023 ROFUIP	• Η χρήση κινητών τηλεφώνων κατά τη διάρκεια των μαθημάτων απαγορεύεται για τους μαθητές του νηπιαγωγείου, του δημοτικού και της πρώτης βαθμίδας της δευτεροβάθμιας εκπαίδευσης, εκτός εάν επιτρέπεται από τον εκπαιδευτικό για εκπαιδευτικούς σκοπούς. • Τα κινητά τηλέφωνα πρέπει να είναι απενεργοποιημένα ή σε αθόρυβη λειτουργία κατά τη διάρκεια των μαθημάτων και να φυλάσσονται σε καθορισμένο χώρο, σύμφωνα με τον ROFUIP. • Οι κανόνες για τη χρήση των κινητών τηλεφώνων κατά τη διάρκεια των διαλειμμάτων καθορίζονται από τον Εσωτερικό Κανονισμό κάθε σχολείου.
Η τεχνητή νοημοσύνη στην εκπαίδευση	• Δεν έχουν εκδοθεί συγκεκριμένες εθνικές κατευθυντήριες γραμμές. Ο νόμος της ΕΕ για την τεχνητή νοημοσύνη (AI Act) εφαρμόζεται άμεσα. • Το Υπουργείο Παιδείας δεν έχει εκδώσει κατευθυντήριες οδηγίες σχετικά με τα εργαλεία γενετικής τεχνητής νοημοσύνης, όπως το ChatGPT, γεγονός που δημιουργεί ένα σημαντικό κενό. • Τα σχολεία θα πρέπει να εφαρμόζουν τις απαιτήσεις του νόμου για την τεχνητή νοημοσύνη όσον αφορά τη διαφάνεια, την ανθρώπινη εποπτεία και την προστασία των δεδομένων, όταν χρησιμοποιούν οποιοδήποτε εργαλείο τεχνητής νοημοσύνης με τους μαθητές.
Ψηφιακή υποδομή	• Δεν υπάρχει ενιαίο εθνικό δίκτυο σχολείων. Τα σχολεία βασίζονται σε εμπορικούς παρόχους διαδικτύου, γεγονός που οδηγεί σε ανομοιογενή πρότυπα κυβερνοασφάλειας. • Το Ολοκληρωμένο Πληροφοριακό Σύστημα Εκπαίδευσης της Ρουμανίας (SIIIR) (το οποίο διαχειρίζεται κεντρικά το Υπουργείο) αποτελεί την κύρια εθνική βάση δεδομένων για τα στοιχεία των μαθητών. • Τα σχολεία χρησιμοποιούν εμπορικές πλατφόρμες (Google Workspace, Microsoft 365) στο πλαίσιο ατομικών συμβάσεων.
Βασικές επικοινωνίες	• Κυβερνοασφάλεια: DNSC (dnsc.ro) • Προστασία δεδομένων: ANSPDCP (dataprotection.ro)

2.5 Σλοβακία

Η Σλοβακία έχει επιδείξει έντονη νομοθετική δυναμική στον τομέα της ψηφιακής διακυβέρνησης στα σχολεία. Ο Νόμος 366/2024 για την Κυβερνοασφάλεια, οι περιορισμοί στη χρήση κινητών τηλεφώνων που θα τεθούν σε ισχύ από τον Ιανουάριο του 2025, οι ειδικές κατευθυντήριες οδηγίες για τον διαδικτυακό εκφοβισμό (Κατευθυντήρια Οδηγία 1/2025) και ένα εθνικό σχέδιο για την τεχνητή νοημοσύνη στην εκπαίδευση για την περίοδο 2025-2027 αντανακλούν μια ολοκληρωμένη και δομημένη προσέγγιση. Σύμφωνα με τη σλοβακική νομοθεσία, ο διευθυντής του σχολείου φέρει άμεση νομική ευθύνη για την κυβερνοασφάλεια. Το πρόγραμμα υποδομών DigiEDU/DigiNET παρέχει ασφαλή, κεντρική σύνδεση στο διαδίκτυο σε όλα τα σχολεία της Σλοβακίας.

Τομέας	Τι σημαίνει αυτό για τα σχολεία
Μεταφορά της Οδηγίας NIS2 Νόμος 366/2024 Νόμος 69/2018	• Ο νόμος 366/2024 συνδέει άμεσα τις υποχρεώσεις στον τομέα της κυβερνοασφάλειας με τη νόμιμη ευθύνη του διευθυντή του σχολείου, σύμφωνα με τον νόμο 596/2003 περί σχολείων. Ο διευθυντής φέρει προσωπική και νομική ευθύνη για την προστασία των πληροφοριακών συστημάτων του σχολείου και των προσωπικών δεδομένων. • Τα σχολεία πρέπει να εφαρμόζουν βασικά μέτρα ασφαλείας: ισχυρούς κωδικούς πρόσβασης, λογισμικό προστασίας από ιούς, τακτικές ενημερώσεις, δημιουργία αντιγράφων ασφαλείας των δεδομένων και ελέγχους πρόσβασης. • Τα σχολεία πρέπει να είναι σε θέση να ανταποκρίνονται σε επιθέσεις ηλεκτρονικού ψαρέματος (phishing), λογισμικού εκβιασμού (ransomware), διαρροών δεδομένων και παραβιάσεων συστημάτων. • Πρέπει να τηρούνται υποχρεωτικές διαδικασίες αναφοράς για σοβαρά περιστατικά κυβερνοασφάλειας. • Ο νόμος 69/2018 παρέχει το θεμελιώδες πλαίσιο για την προστασία των πληροφοριακών συστημάτων και δικτύων, διασφαλίζοντας την ασφάλεια των δεδομένων των μαθητών και την ασφαλή χρήση των ψηφιακών τεχνολογιών στα σχολεία.
Προστασία Δεδομένων Νόμος 18/2018	• Ο διορισμός Υπεύθυνου Προστασίας Δεδομένων (DPO) είναι υποχρεωτικός για τα δημόσια σχολεία, αλλά δεν απαιτείται ένας DPO ανά σχολείο: επιτρέπεται η ύπαρξη ενός κοινού DPO για πολλά σχολεία. • Τα σχολεία πρέπει να εφαρμόζουν την αρχή της ελαχιστοποίησης των δεδομένων: να συλλέγουν και να χρησιμοποιούν μόνο τα προσωπικά δεδομένα των μαθητών που είναι απολύτως απαραίτητα για εκπαιδευτικούς και διοικητικούς σκοπούς. • Η πρόσβαση στα δεδομένα πρέπει να περιορίζεται σε εξουσιοδοτημένα πρόσωπα (εκπαιδευτικούς, διευθυντικό προσωπικό, διοικητικό προσωπικό) ανάλογα με τις ανάγκες. • Τα ηλεκτρονικά συστήματα, τα μηνύματα ηλεκτρονικού ταχυδρομείου, τα έγγραφα σε χαρτί και οι συσκευές

Τομέας	Τι σημαίνει αυτό για τα σχολεία
	αποθήκευσης πρέπει να προστατεύονται από απώλεια ή μη εξουσιοδοτημένη πρόσβαση. • Φωτογραφίες, κατάλογοι μαθητών, αποτελέσματα ή ευαίσθητες πληροφορίες δεν πρέπει να δημοσιεύονται χωρίς νομική βάση ή ρητή συγκατάθεση. • Κάθε παραβίαση της προστασίας δεδομένων πρέπει να αναφέρεται στην αρμόδια αρχή εντός 72 ωρών, εάν ενέχει κίνδυνο για τα φυσικά πρόσωπα.
Ηλικία ψηφιακής συναίνεσης	• 16 ετών. • Απαιτείται η συγκατάθεση των γονέων ή του κηδεμόνα πριν από την εγγραφή μαθητών κάτω των 16 ετών σε ψηφιακές πλατφόρμες.
Διαδικτυακός εκφοβισμός Οδηγία 1/2025	• Η Οδηγία 1/2025 παρέχει συγκεκριμένους κανόνες για την πρόληψη και την αντιμετώπιση του διαδικτυακού εκφοβισμού στα σχολεία και τις εκπαιδευτικές εγκαταστάσεις. • Ορίζει τα βασικά σημάδια, τις μορφές και τις εκδηλώσεις του διαδικτυακού εκφοβισμού. • Καθορίζει διαδικασίες πρόληψης και μεθόδους αντιμετώπισης των περιστατικών. • Περιλαμβάνει διαδικασίες για την υποστήριξη των θυμάτων. • Τα σχολεία πρέπει να εφαρμόζουν τις διαδικασίες που ορίζονται στην παρούσα οδηγία.
Κινητά Τηλέφωνα Νόμος 245/2008 (τροποποιημένος από τον Ιανουάριο του 2025)	• Οι μαθητές της 1ης έως της 3ης τάξης δεν επιτρέπεται να χρησιμοποιούν καθόλου κινητά τηλέφωνα ή παρόμοιες συσκευές κατά τη διάρκεια του σχολικού ωραρίου. • Οι μαθητές των τάξεων 4 έως 9 μπορούν να τις χρησιμοποιούν μόνο για εκπαιδευτικούς σκοπούς, όταν ο δάσκαλος το επιτρέπει ρητά. • Εξαίρεση αποτελούν οι μαθητές με αναπηρίες που χρησιμοποιούν τη συσκευή σε σχέση με την κατάσταση της υγείας τους. • Σε περίπτωση παράβασης, το σχολείο μπορεί να κατασχέσει προσωρινά τη συσκευή. • Οι λεπτομερείς όροι διέπονται από τον εσωτερικό κανονισμό του σχολείου.
Η τεχνητή νοημοσύνη στην εκπαίδευση Σχέδιο Τεχνητής Νοημοσύνης 2025-2027	• Το Σχέδιο του Υπουργείου Παιδείας για την Υπεύθυνη Χρήση της ΤΝ στην Εκπαίδευση 2025-2027 παρέχει πρακτικές εθνικές κατευθυντήριες γραμμές για τα σχολεία. • Τα σχολεία θα πρέπει να χρησιμοποιούν το σχέδιο αυτό σε συνδυασμό με τον Νόμο της ΕΕ για την ΤΝ, προκειμένου να αξιολογούν και να ρυθμίζουν τη χρήση οποιωνδήποτε εργαλείων ΤΝ που εισάγουν.

Τομέας	Τι σημαίνει αυτό για τα σχολεία
	• Δίνεται έμφαση στην ασφάλεια, την ηθική χρήση και τη διαφάνεια.
Ψηφιακή υποδομή	• DigiEDU/DigiNET: πρόγραμμα ασφαλούς, κεντρικά διαχειριζόμενης σύνδεσης στο Διαδίκτυο για όλα τα σχολεία της Σλοβακίας. • Η κυβερνοασφάλεια εποπτεύεται από το Εθνικό Γραφείο Ασφάλειας (NBU), το οποίο διαχειρίζεται το SK-CERT για την αντιμετώπιση περιστατικών. • Το Εθνικό Γραφείο Ασφάλειας (NBU) παρέχει καθοδήγηση και υποστήριξη σε δημόσιους φορείς, συμπεριλαμβανομένων των σχολείων.
Βασικές επικοινωνίες	• Κυβερνοασφάλεια: NBU/SK-CERT (nbu.gov.sk) • Προστασία δεδομένων: UOOU (dataprotection.gov.sk)

Διεθνή πρότυπα και σχολεία

Οι πρακτικές συστάσεις στο Μέρος 3 της παρούσας πολιτικής βασίζονται σε μια σειρά διεθνώς αναγνωρισμένων προτύπων διαχείρισης. Σε αυτή τη σύντομη ενότητα εξηγείται ποια είναι αυτά τα πρότυπα και γιατί είναι σημαντικά για τα σχολεία. Δεν είναι απαραίτητο να είστε εξοικειωμένοι με τα ίδια τα πρότυπα για να ακολουθήσετε τις οδηγίες του Μέρους 3. Τα πρότυπα αυτά παρέχουν ένα δοκιμασμένο και ευρέως αποδεκτό θεμέλιο που προσδίδει στη συγκεκριμένη πολιτική τη δομή και την αξιοπιστία της.

Πέντε πρότυπα έχουν σημασία σε αυτό το πλαίσιο. Κάθε ένα από αυτά αφορά μια διαφορετική πτυχή του τρόπου με τον οποίο τα σχολεία μπορούν να προστατεύουν τους μαθητές τους, τα δεδομένα τους και τα συστήματά τους.

Το ISO/IEC 27001 είναι το διεθνές πρότυπο για τη διαχείριση της ασφάλειας των πληροφοριών. Παρέχει ένα πλαίσιο για τον προσδιορισμό των πληροφοριών που κατέχει ένα σχολείο, την κατανόηση των κινδύνων που διατρέχουν αυτές οι πληροφορίες και τη λήψη των κατάλληλων μέτρων για την προστασία τους. Στο σχολικό πλαίσιο, αυτό σημαίνει τα αρχεία των μαθητών, τα δεδομένα του προσωπικού, τις ψηφιακές πλατφόρμες και όλα τα συστήματα που υποστηρίζουν τη διδασκαλία και τη διοίκηση. Το ISO 27001 δεν ορίζει συγκεκριμένες τεχνικές λύσεις. Αντίθετα, καθορίζει έναν τρόπο συστηματικής προσέγγισης της ασφάλειας, διασφαλίζοντας ότι δεν παραβλέπεται τίποτα σημαντικό. Οι πρακτικές ενέργειες στις ενότητες 3.1 έως 3.7 βασίζονται όλες σε αυτό το πλαίσιο.

Το πρότυπο ISO/IEC 27002 συμπληρώνει το ISO 27001 και παρέχει τους λεπτομερείς ελέγχους που εφαρμόζουν στην πράξη την ασφάλεια των πληροφοριών. Ενώ το ISO 27001 περιγράφει το πλαίσιο διαχείρισης, το ISO 27002 περιγράφει τα συγκεκριμένα μέτρα: πώς να ελέγχεται η πρόσβαση στα συστήματα, πώς να διαχειρίζονται οι κωδικοί πρόσβασης, πώς να αντιμετωπίζονται τα περιστατικά, πώς να διαμορφώνονται οι συσκευές με ασφάλεια. Οι ενότητες 3.2 και 3.3 βασίζονται άμεσα σε αυτό το πρότυπο.

Το ISO/IEC 27701 επεκτείνει το πλαίσιο ασφάλειας των πληροφοριών ώστε να καλύπτει συγκεκριμένα την προστασία των προσωπικών δεδομένων. Συνδέεται άμεσα με τον Γενικό Κανονισμό για την Προστασία Δεδομένων (GDPR) και βοηθά τα σχολεία να αποδείξουν ότι διαχειρίζονται υπεύθυνα τα δεδομένα των μαθητών και του προσωπικού. Η ενότητα 3.1 βασίζεται σε αυτό το πρότυπο.

Το ISO 22301 είναι το πρότυπο για τη διαχείριση της επιχειρησιακής συνέχειας. Για τα σχολεία, αυτό σημαίνει να είναι προετοιμασμένα για διακοπές λειτουργίας: μια κυβερνοεπίθεση, μια βλάβη συστήματος, ένα περιστατικό ransomware που κλειδώνει την πρόσβαση στα αρχεία των μαθητών. Το ISO 22301 ενθαρρύνει τους οργανισμούς να σχεδιάζουν εκ των προτέρων για αυτές τις καταστάσεις, να διαθέτουν αντίγραφα ασφαλείας και διαδικασίες αποκατάστασης, και να τις δοκιμάζουν τακτικά ώστε να λειτουργούν όταν χρειαστεί. Ένα σχολείο που ακολουθεί αυτή την προσέγγιση μπορεί να ανακάμψει γρήγορα από ένα περιστατικό, αντί να αντιμετωπίζει εβδομάδες διακοπής της λειτουργίας. Η ενότητα 3.2 και η διαδικασία αντιμετώπισης περιστατικών στο Παράρτημα IV αντανακλούν αυτό το πρότυπο.

Το ISO 31000 είναι το πρότυπο για τη διαχείριση κινδύνων. Προσφέρει έναν τρόπο προσέγγισης του κινδύνου που εφαρμόζεται σε όλους τους τομείς της σχολικής ζωής, όχι μόνο στον τομέα της κυβερνοασφάλειας. Πριν υιοθετήσει μια νέα ψηφιακή πλατφόρμα, πριν εισαγάγει ένα εργαλείο τεχνητής νοημοσύνης, πριν αλλάξει τον τρόπο διαχείρισης των δεδομένων των μαθητών, ένα σχολείο θα πρέπει να αναρωτηθεί: τι θα μπορούσε να πάει στραβά, πόσο πιθανό είναι αυτό και ποιες θα ήταν οι συνέπειες; Αυτή είναι η λογική που διέπει τη διαδικασία DPIA στο Παράρτημα V, την προσέγγιση αξιολόγησης πλατφορμών στην Ενότητα 3.3 και την ευρύτερη προσέγγιση με γνώμονα τον κίνδυνο σε ολόκληρο το Μέρος 3.

Συνολικά, αυτά τα πέντε πρότυπα αποτελούν τη ραχοκοκαλιά του Μέρους 3. Αποτελούν τον λόγο για τον οποίο οι συστάσεις της παρούσας πολιτικής δεν είναι αυθαίρετες. Αντιπροσωπεύουν δεκαετίες συσσωρευμένης γνώσης σχετικά με τον τρόπο με τον οποίο οι οργανισμοί μπορούν να προστατεύουν τις πληροφορίες τους, να διαχειρίζονται τους κινδύνους τους και να συνεχίζουν να λειτουργούν όταν τα πράγματα πάνε στραβά. Οι οδηγίες που ακολουθούν μετατρέπουν αυτή τη γνώση σε πρακτικά μέτρα που μπορεί να λάβει κάθε σχολείο.

Μέρος 3: Τι πρέπει να κάνει το σχολείο σας

Το παρόν τμήμα χωρίζεται σε επτά ενότητες. Κάθε ενότητα ξεκινά με μια σύντομη εξήγηση του λόγου για τον οποίο είναι σημαντική, ακολουθούμενη από έναν πίνακα που παρουσιάζει τι πρέπει να κάνει το σχολείο σας, γιατί κάθε δράση είναι σημαντική και πώς να την υλοποιήσετε.

Οι συστάσεις αυτού του τμήματος είναι πιο αποτελεσματικές όταν εμπλέκουν ολόκληρη τη σχολική κοινότητα. Οι διευθυντές των σχολείων, οι εκπαιδευτικοί, το διοικητικό προσωπικό, οι μαθητές, οι γονείς και οι εξωτερικοί φορείς υποστήριξης έχουν όλοι να διαδραματίσουν έναν ρόλο στη δημιουργία ενός ασφαλούς ψηφιακού περιβάλλοντος. Η τακτική επικοινωνία, η πρακτική εκπαίδευση και τα αξιόπιστα κανάλια αναφοράς βοηθούν τα σχολεία να καλλιεργήσουν μια

κουλτούρα ανθεκτικότητας στον κυβερνοχώρο, αντί να περιορίζονται απλώς στην αντιμετώπιση περιστατικών.

3.1 Προστασία των προσωπικών δεδομένων

Τα σχολεία διαθέτουν μεγάλο όγκο προσωπικών δεδομένων σχετικά με τους μαθητές, τους γονείς και το προσωπικό. Αυτά περιλαμβάνουν ονόματα, αριθμούς ταυτότητας, παρουσιολόγια, βαθμολογίες, πληροφορίες υγείας και στοιχεία επικοινωνίας των οικογενειών. Η προστασία αυτών των δεδομένων αποτελεί νομική υποχρέωση. Είναι επίσης θέμα εμπιστοσύνης. Οι οικογένειες μοιράζονται ευαίσθητες πληροφορίες με τα σχολεία επειδή είναι αναγκασμένες να το κάνουν. Τα σχολεία έχουν την ευθύνη να τις χειρίζονται με προσοχή.

Όταν η προστασία των δεδομένων δεν λειτουργεί σωστά, οι συνέπειες μπορεί να είναι σοβαρές. Οι πληροφορίες των μαθητών ενδέχεται να εκτεθούν σε άτομα που δεν θα έπρεπε να έχουν πρόσβαση σε αυτές. Το σχολείο μπορεί να βρεθεί αντιμέτωπο με επίσημη έρευνα. Και η εμπιστοσύνη των μαθητών και των οικογενειών μπορεί να είναι δύσκολο να αποκατασταθεί. Είναι πολύ πιο εύκολο να τεθούν σωστά τα βασικά από την αρχή, παρά να αντιμετωπιστούν οι συνέπειες μιας παραβίασης.

Τι να κάνετε	Γιατί έχει σημασία	Πώς να το κάνετε
Διορισμός Υπεύθυνου Προστασίας Δεδομένων (DPO)	Ο Υπεύθυνος Προστασίας Δεδομένων (DPO) είναι το πρόσωπο που φέρει την ευθύνη να διασφαλίζει ότι το σχολείο σας συμμορφώνεται με τη νομοθεσία περί προστασίας δεδομένων. Χωρίς αυτόν, δεν υπάρχει σαφής λογοδοσία όταν κάτι πάει στραβά. Ο Υπεύθυνος Προστασίας Δεδομένων (DPO) αποτελεί επίσης τον κύριο υπεύθυνο επικοινωνίας για τους μαθητές, τους γονείς και την εθνική εποπτική αρχή.	Ανατρέξτε στο Μέρος 2 για να μάθετε αν το σχολείο σας χρειάζεται δικό του Υπεύθυνο Προστασίας Δεδομένων (DPO) ή αν ο ρόλος αυτός καλύπτεται σε επίπεδο ομάδας σχολείων ή αρμόδιας αρχής. Ο Υπεύθυνος Προστασίας Δεδομένων πρέπει να είναι προσβάσιμος στο προσωπικό, στους μαθητές και στους γονείς. Είναι υπεύθυνος για την παρακολούθηση της συμμόρφωσης, την παροχή συμβουλών σε θέματα προστασίας δεδομένων, την εκπαίδευση του προσωπικού και τη συνεργασία με την εποπτική αρχή.
Τηρείτε αρχείο όλων των δραστηριοτήτων επεξεργασίας δεδομένων	Το παρόν αρχείο απαιτείται από το νόμο, σύμφωνα με το άρθρο 30 του ΓΚΠΔ (GDPR). Σε αυτό αναφέρονται τα προσωπικά δεδομένα που διατηρεί το σχολείο σας, ο λόγος για τον οποίο τα διατηρεί, ποιοι έχουν πρόσβαση σε αυτά και για πόσο χρονικό διάστημα διατηρούνται. Εάν το ζητήσει η εποπτική αρχή, πρέπει να	Το μητρώο πρέπει να καλύπτει κάθε κατηγορία προσωπικών δεδομένων που επεξεργάζεται το σχολείο σας: αρχεία μαθητών, στοιχεία επικοινωνίας γονέων, δεδομένα προσωπικού, πληροφορίες υγείας κ.λπ. Για κάθε κατηγορία, καταγράψτε τον σκοπό, τη νομική βάση, ποιος έχει πρόσβαση, για πόσο χρονικό διάστημα διατηρούνται τα δεδομένα και τι συμβαίνει όταν δεν είναι πλέον απαραίτητα. Ο Υπεύθυνος Προστασίας Δεδομένων

Τι να κάνετε	Γιατί έχει σημασία	Πώς να το κάνετε
	είστε σε θέση να το προσκομίσετε.	(DPO) είναι υπεύθυνος για την ενημέρωσή του.
Συλλέγετε μόνο τα δεδομένα που πραγματικά χρειάζεστε	Κάθε στοιχείο δεδομένων που συλλέγετε αποτελεί κίνδυνο. Σε περίπτωση παραβίασης, μόνο τα δεδομένα που διατηρείτε πραγματικά μπορούν να εκτεθούν. Η συλλογή περισσότερων δεδομένων από όσα χρειάζεστε συνεπάγεται επίσης περισσότερο έργο διαχείρισης και μεγαλύτερο κίνδυνο μη συμμόρφωσης.	Ελέγξτε όλα τα έντυπα συλλογής δεδομένων, τις διαδικασίες εγγραφής και τις ρυθμίσεις της πλατφόρμας. Καταργήστε όλα τα πεδία που ζητούν πληροφορίες τις οποίες το σχολείο δεν χρειάζεται πραγματικά. Εάν μια πλατφόρμα ζητά περισσότερα δεδομένα από τα απαραίτητα, επιμείνετε στον προμηθευτή ή επιλέξτε μια διαφορετική πλατφόρμα. Καθιερώστε ως κανόνα την απενεργοποίηση της προαιρετικής συλλογής δεδομένων από προεπιλογή.
Να υπογράφονται συμφωνίες με κάθε προμηθευτή που επεξεργάζεται δεδομένα μαθητών	Όταν μια εταιρεία επεξεργάζεται δεδομένα μαθητών ή προσωπικού για λογαριασμό σας - για παράδειγμα, μια πλατφόρμα cloud, ένα εργαλείο βαθμολόγησης ή μια εφαρμογή επικοινωνίας -, το σχολείο σας εξακολουθεί να φέρει τη νομική ευθύνη για τον τρόπο διαχείρισης των δεδομένων αυτών. Χωρίς γραπτή συμφωνία, δεν μπορείτε να αποδείξετε ότι έχετε εκπληρώσει τις υποχρεώσεις σας.	Πριν οποιοσδήποτε προμηθευτής θέσει σε λειτουργία μια υπηρεσία που αφορά προσωπικά δεδομένα, πρέπει να υπογράψει μια Συμφωνία Επεξεργασίας Δεδομένων. Σε αυτή πρέπει να προσδιορίζεται ποια δεδομένα υποβάλλονται σε επεξεργασία, για ποιο σκοπό, ποια μέτρα ασφαλείας έχουν ληφθεί και τι συμβαίνει με τα δεδομένα όταν λήξει η σύμβαση. Φυλάξτε αντίγραφα όλων των συμφωνιών στα αρχεία σας.
Περιορισμός του κύκλου των ατόμων που έχουν πρόσβαση στα προσωπικά δεδομένα	Όσο περισσότεροι άνθρωποι έχουν πρόσβαση στα δεδομένα, τόσο μεγαλύτερος είναι ο κίνδυνος να γίνει κατάχρηση αυτών, να αποκαλυφθούν κατά λάθος ή να κλαπούν. Κάθε περιττό σημείο πρόσβασης αποτελεί ευπάθεια.	Ρυθμίστε την πρόσβαση βάσει ρόλων, έτσι ώστε κάθε μέλος του προσωπικού να έχει πρόσβαση μόνο στα δεδομένα που χρειάζεται για τις συγκεκριμένες αρμοδιότητές του. Ένας εκπαιδευτικός θα πρέπει να έχει πρόσβαση μόνο στα αρχεία των δικών του μαθητών, όχι σε αυτά ολόκληρου του σχολείου. Το διοικητικό προσωπικό θα πρέπει να έχει πρόσβαση σε διοικητικά δεδομένα, όχι σε αρχεία υγείας ή ψυχολογικά αρχεία. Ελέγχετε ποιος έχει πρόσβαση τουλάχιστον μία φορά το χρόνο και αφαιρείτε αμέσως την πρόσβαση όταν κάποιος αλλάζει ρόλο ή αποχωρεί.

Τι να κάνετε	Γιατί έχει σημασία	Πώς να το κάνετε
Ενημερώστε τους μαθητές και τους γονείς για τον τρόπο με τον οποίο χρησιμοποιούνται τα δεδομένα τους	Οι μαθητές και οι γονείς έχουν το νόμιμο δικαίωμα να γνωρίζουν ποια δεδομένα τηρούνται για αυτούς και πώς χρησιμοποιούνται. Η παροχή αυτών των πληροφοριών δεν είναι προαιρετική. Τα σχολεία που επιδεικνύουν διαφάνεια όσον αφορά τη χρήση των δεδομένων τείνουν επίσης να αντιμετωπίζουν λιγότερες διαμάχες και καταγγελίες.	Συντάξτε μια δήλωση προστασίας προσωπικών δεδομένων σε απλή γλώσσα, ώστε να είναι κατανοητή από κάθε γονέα ή μεγαλύτερο μαθητή. Πρέπει να εξηγεί ποια δεδομένα συλλέγονται, για ποιο λόγο, ποιος έχει πρόσβαση σε αυτά και για πόσο χρονικό διάστημα διατηρούνται. Παρέχετε τη δήλωση αυτή κατά την εγγραφή των μαθητών και κάθε φορά που επέρχεται κάποια σημαντική αλλαγή. Φροντίστε να είναι μόνιμα διαθέσιμη, για παράδειγμα στον ιστότοπο του σχολείου. Στο Παράρτημα II περιλαμβάνεται ένα πρότυπο επιστολής.
Λάβετε τη συγκατάθεση των γονέων για τους μαθητές που δεν έχουν συμπληρώσει την ηλικία ψηφιακής συγκατάθεσης	Για τους μαθητές που δεν έχουν συμπληρώσει την εθνική ηλικία ψηφιακής συναίνεσης, δεν μπορείτε να τους εγγράψετε σε μια ψηφιακή πλατφόρμα χωρίς τη γραπτή συναίνεση ενός γονέα ή κηδεμόνα. Πρόκειται για νομική απαίτηση. Η ηλικία αυτή κυμαίνεται μεταξύ 13 και 16 ετών στις πέντε χώρες, πράγμα που σημαίνει ότι η ίδια πλατφόρμα ενδέχεται να απαιτεί συναίνεση σε μια χώρα, αλλά όχι σε μια άλλη.	Καθορίστε μια σαφή διαδικασία για τη συλλογή, την καταγραφή και την ανανέωση της γονικής συγκατάθεσης. Η συγκατάθεση πρέπει να αφορά συγκεκριμένα κάθε πλατφόρμα, να παρέχεται ελεύθερα και να μπορεί να ανακληθεί εύκολα. Μην θεωρείτε δεδομένο ότι η υπογραφή ενός γενικού εντύπου εγγραφής καλύπτει όλες τις ψηφιακές πλατφόρμες. Ελέγξτε την ηλικία που απαιτείται για την παροχή ψηφιακής συγκατάθεσης στη χώρα σας στο Μέρος 2.
Αναφέρετε τις παραβιάσεις δεδομένων εντός 72 ωρών	Η προθεσμία των 72 ωρών αποτελεί αυστηρή νομική απαίτηση. Εάν το σχολείο σας διαπιστώσει μια παραβίαση και δεν την αναφέρει εγκαίρως, ή προσπαθήσει να τη διαχειριστεί διακριτικά χωρίς να ενημερώσει την εποπτική αρχή, οι συνέπειες μπορεί να είναι σημαντικά χειρότερες από ό,τι εάν η παραβίαση είχε αναφερθεί αμέσως.	Θέστε σε εφαρμογή μια γραπτή διαδικασία αντιμετώπισης παραβιάσεων πριν συμβεί οτιδήποτε. Όταν συμβεί παραβίαση, ο Υπεύθυνος Προστασίας Δεδομένων (DPO) πρέπει να αξιολογήσει αμέσως εάν αυτή ενέχει κίνδυνο για τα φυσικά πρόσωπα. Εάν ναι, η εθνική εποπτική αρχή πρέπει να ενημερωθεί εντός 72 ωρών. Εάν ο κίνδυνος είναι υψηλός, τα επηρεαζόμενα φυσικά πρόσωπα πρέπει επίσης να ενημερωθούν απευθείας. Χρησιμοποιήστε το μητρώο συμβάντων στο Παράρτημα IV για να καταγράψετε κάθε βήμα.

Τι είναι η παραβίαση δεδομένων;

Παραβίαση δεδομένων είναι κάθε περιστατικό που έχει ως αποτέλεσμα την τυχαία ή παράνομη απώλεια, καταστροφή, αλλοίωση, αποκάλυψη ή πρόσβαση σε προσωπικά δεδομένα από κάποιον που δεν θα έπρεπε να τα έχει. Αυτό περιλαμβάνει την απώλεια μιας μονάδας USB που περιέχει αρχεία μαθητών, την αποστολή ενός email σε λάθος παραλήπτη, μια επίθεση ransomware που κλειδώνει τα δεδομένα του σχολείου ή μια ρύθμιση πλατφόρμας που καθιστά κατά λάθος τα αρχεία των μαθητών ορατά στο κοινό. Πολλές από τις πιο συνηθισμένες παραβιάσεις στα σχολεία προκαλούνται από ανθρώπινο λάθος και όχι από εξωτερικές επιθέσεις.

3.2 Διασφάλιση της ασφάλειας των σχολικών συστημάτων

Η κυβερνοασφάλεια σημαίνει την προστασία των υπολογιστών, των δικτύων και των δεδομένων του σχολείου σας από επιθέσεις και μη εξουσιοδοτημένη πρόσβαση. Τα σχολεία αποτελούν ελκυστικό στόχο για τους κυβερνοεγκληματίες, καθώς διαθέτουν ευαίσθητα δεδομένα για τα παιδιά και συχνά διαθέτουν περιορισμένους πόρους ασφάλειας. Μια επιτυχημένη επίθεση μπορεί να θέσει εκτός λειτουργίας τα σχολικά συστήματα, να εκθέσει τα αρχεία των μαθητών, να διακόψει τη μάθηση για εβδομάδες και να προκαλέσει μόνιμη ζημιά στη φήμη του σχολείου.

Τα καλά νέα είναι ότι οι περισσότερες επιτυχημένες κυβερνοεπιθέσεις εκμεταλλεύονται απλές αδυναμίες που μπορούν να διορθωθούν χωρίς εξειδικευμένη τεχνογνωσία ή μεγάλους προϋπολογισμούς. Αδύναμοι κωδικοί πρόσβασης, λογισμικό που δεν έχει ενημερωθεί, προσωπικό που δεν αναγνωρίζει τα μηνύματα ηλεκτρονικού «ψαρέματος» (phishing) και η έλλειψη αντιγράφων ασφαλείας βρίσκονται πίσω από την πλειονότητα των περιστατικών. Η διόρθωση αυτών των βασικών στοιχείων κάνει τεράστια διαφορά.

Εξίσου σημαντικό είναι να είμαστε προετοιμασμένοι για τη στιγμή που κάτι θα πάει στραβά. Η ύπαρξη ενός δοκιμασμένου αντιγράφου ασφαλείας και μιας σαφούς διαδικασίας αποκατάστασης σημαίνει τη διαφορά μεταξύ μιας διακοπής που διαρκεί λίγες ώρες και μιας που διαρκεί εβδομάδες. Αυτή είναι η λογική πίσω από τον σχεδιασμό επιχειρησιακής συνέχειας: όχι μόνο η πρόληψη περιστατικών, αλλά και η διασφάλιση ότι το σχολείο μπορεί να συνεχίσει να λειτουργεί και να ανακάμψει γρήγορα όταν αυτά συμβούν.

Τι να κάνετε	Γιατί έχει σημασία	Πώς να το κάνετε
Χρησιμοποιήστε ισχυρούς κωδικούς πρόσβασης και έλεγχο ταυτότητας πολλαπλών παραγόντων	Οι αδύναμοι κωδικοί πρόσβασης αποτελούν τον πιο συνηθισμένο τρόπο με τον οποίο οι εισβολείς αποκτούν πρόσβαση στα σχολικά συστήματα. Ένας κωδικός πρόσβασης που είναι εύκολο να μαντευτεί ή που χρησιμοποιείται σε πολλούς λογαριασμούς σημαίνει ότι η κλοπή ενός μόνο κωδικού πρόσβασης μπορεί να δώσει σε έναν εισβολέα πρόσβαση σε όλα. Η πολυπαραγοντική	Όλοι οι λογαριασμοί του προσωπικού πρέπει να χρησιμοποιούν ισχυρούς κωδικούς πρόσβασης τουλάχιστον 12 χαρακτήρων, που να συνδυάζουν γράμματα, αριθμούς και σύμβολα. Οι κωδικοί πρόσβασης πρέπει να αλλάζουν εάν υπάρχει οποιοσδήποτε λόγος να πιστεύεται ότι έχουν παραβιαστεί. Η πολυπαραγοντική επαλήθευση ταυτότητας πρέπει να είναι ενεργοποιημένη για όλα τα συστήματα που περιέχουν δεδομένα μαθητών. Μετά την εισαγωγή του κωδικού πρόσβασής του, το μέλος του προσωπικού πρέπει να επιβεβαιώσει την ταυτότητά του

Τι να κάνετε	Γιατί έχει σημασία	Πώς να το κάνετε
	επαλήθευση ταυτότητας προσθέτει έναν δεύτερο έλεγχο που προστατεύει τους λογαριασμούς	μέσω μιας δεύτερης μεθόδου, όπως ένας κωδικός που αποστέλλεται στο κινητό του.
Φροντίστε να ενημερώνετε τακτικά όλα τα προγράμματα και τις συσκευές	Οι ενημερώσεις λογισμικού περιλαμβάνουν συχνά διορθώσεις για κενά ασφαλείας τα οποία εκμεταλλεύονται ενεργά οι επιτιθέμενοι. Πολλές από τις χειρότερες επιθέσεις με λογισμικό εκβιασμού (ransomware) εναντίον σχολείων είχαν ως στόχο συστήματα που χρησιμοποιούσαν παλιό λογισμικό το οποίο δεν είχε ενημερωθεί. Πρόκειται για μία από τις πιο εύκολα αποτρέψιμες ευπάθειες που υπάρχουν.	Καθορίστε ένα τακτικό πρόγραμμα για την εγκατάσταση ενημερώσεων σε όλες τις συσκευές του σχολείου, τα λειτουργικά συστήματα, τις εφαρμογές και το λογισμικό ασφαλείας. Εγκαταστήστε τις κρίσιμες ενημερώσεις ασφαλείας αμέσως μόλις γίνουν διαθέσιμες. Εάν μια συσκευή δεν μπορεί πλέον να λαμβάνει ενημερώσεις, αποσυνδέστε την από το δίκτυο ή αντικαταστήστε την. Αναθέστε σε ένα συγκεκριμένο μέλος του προσωπικού την ευθύνη να διασφαλίζει ότι οι ενημερώσεις πραγματοποιούνται.
Δημιουργήστε τακτικά αντίγραφα ασφαλείας όλων των σημαντικών δεδομένων σας	Οι επιθέσεις με λογισμικό εκβιασμού (ransomware) λειτουργούν κρυπτογραφώντας τα δεδομένα σας και απαιτώντας πληρωμή για την αποκατάσταση της πρόσβασης. Ο μόνος αξιόπιστος τρόπος ανάκτησης χωρίς πληρωμή είναι να διαθέτετε ένα αντίγραφο ασφαλείας που δημιουργήθηκε πριν από την επίθεση. Χωρίς ένα δοκιμασμένο αντίγραφο ασφαλείας, ένα σχολείο μπορεί να χάσει εβδομάδες εργασίας και μόνιμα αρχεία.	Ρυθμίστε την αυτόματη δημιουργία καθημερινών αντιγράφων ασφαλείας για όλα τα κρίσιμα δεδομένα του σχολείου. Φυλάξτε τουλάχιστον ένα αντίγραφο κάθε αντιγράφου ασφαλείας σε θέση που δεν είναι συνδεδεμένη με το κύριο δίκτυο του σχολείου, ώστε να μην μπορεί να κρυπτογραφηθεί κατά τη διάρκεια της ίδιας επίθεσης. Ελέγξτε τη διαδικασία ανάκτησης τουλάχιστον μία φορά το χρόνο, για να βεβαιωθείτε ότι τα αντίγραφα ασφαλείας λειτουργούν πράγματι και ότι τα δεδομένα μπορούν να αποκατασταθούν σε εύλογο χρονικό διάστημα.
Χρησιμοποιήστε ξεχωριστά δίκτυα για τη διοίκηση και τους μαθητές	Εάν το δίκτυο που χρησιμοποιεί το διοικητικό προσωπικό, στο οποίο διαχειρίζονται τα αρχεία και οι βαθμολογίες των μαθητών, είναι το ίδιο με αυτό που χρησιμοποιούν οι μαθητές και	Δημιουργήστε ξεχωριστά δίκτυα Wi-Fi: ένα για διοικητική χρήση και ένα για μαθητές και επισκέπτες. Βεβαιωθείτε ότι το διοικητικό δίκτυο δεν είναι ορατό ούτε προσβάσιμο από το δίκτυο των μαθητών. Ρυθμίστε τους ελέγχους πρόσβασης έτσι ώστε μόνο οι εξουσιοδοτημένες συσκευές

Τι να κάνετε	Γιατί έχει σημασία	Πώς να το κάνετε
	οι επισκέπτες, τότε μια συσκευή μαθητή που έχει παραβιαστεί ή ένας φορητός υπολογιστής επισκέπτη που έχει μολυνθεί θα μπορούσε ενδεχομένως να αποκτήσει πρόσβαση στα διοικητικά συστήματα του σχολείου. Πρόκειται για έναν βασικό κίνδυνο που εξαλείφεται με τον διαχωρισμό των δικτύων.	του σχολείου να μπορούν να συνδεθούν στο διοικητικό δίκτυο.
Προστατέψτε όλες τις συσκευές του σχολείου	Οι συσκευές που διαθέτουν εργοστασιακούς κωδικούς πρόσβασης, δεν έχουν ενημερωθεί ποτέ ή δεν διαθέτουν εγκατεστημένη προστασία από ιούς αποτελούν εύκολο στόχο. Πολλά σχολεία διαθέτουν συσκευές στις αίθουσες διδασκαλίας ή στα γραφεία τους, οι οποίες εγκαταστάθηκαν πριν από χρόνια και δεν έχουν ελεγχθεί έκτοτε.	Εγκαταστήστε λογισμικό προστασίας από ιούς και κακόβουλο λογισμικό σε όλες τις συσκευές του σχολείου και φροντίστε να το διατηρείτε ενημερωμένο. Αλλάξτε όλους τους προεπιλεγμένους κωδικούς πρόσβασης σε δρομολογητές, κάμερες, εκτυπωτές και οποιονδήποτε άλλο συνδεδεμένο εξοπλισμό αμέσως μετά την εγκατάστασή τους. Διενεργείτε τακτικό έλεγχο όλων των συνδεδεμένων συσκευών. Πριν από την απόρριψη παλαιών συσκευών, βεβαιωθείτε ότι όλα τα δεδομένα έχουν διαγραφεί οριστικά και με ασφάλεια.
Να έχετε ένα γραπτό σχέδιο για την αντιμετώπιση περιστατικών	Χωρίς ένα γραπτό σχέδιο, το προσωπικό που θα βρεθεί να αντιμετωπίζει μια κυβερνοεπίθεση δεν θα ξέρει τι να κάνει. Αποφάσεις που λαμβάνονται υπό την επήρεια πανικού ή με καλή πρόθεση αλλά είναι λανθασμένες, όπως η άμεση απενεργοποίηση μιας συσκευής ή η προσπάθεια καταβολής λύτρων, μπορούν να επιδεινώσουν σημαντικά μια ήδη δύσκολη κατάσταση.	Συντάξτε μια διαδικασία αντιμετώπισης συμβάντων στον κυβερνοχώρο, στην οποία θα καθορίζεται ποιος συντονίζει την αντιμετώπιση, ποια μέτρα πρέπει να ληφθούν και με ποια σειρά, σε ποιες εθνικές αρχές πρέπει να απευθυνθείτε και εντός ποιας προθεσμίας, καθώς και πώς θα επικοινωνείτε με τους μαθητές, τους γονείς και το προσωπικό κατά τη διάρκεια και μετά από ένα συμβάν. Βεβαιωθείτε ότι όλο το αρμόδιο προσωπικό γνωρίζει τη διαδικασία πριν από κάποιο συμβάν. Στο Παράρτημα IV παρέχεται ένα πρότυπο.
Να πραγματοποιείται εκπαίδευση όλου του προσωπικού τουλάχιστον μία φορά το χρόνο	Τα μηνύματα ηλεκτρονικού ταχυδρομείου τύπου «phishing» ευθύνονται για την πλειονότητα των επιτυχημένων κυβερνοεπιθέσεων εναντίον σχολείων. Ένας υπάλληλος	Παρέχετε υποχρεωτική ετήσια εκπαίδευση ευαισθητοποίησης σε θέματα κυβερνοασφάλειας για όλο το προσωπικό. Η εκπαίδευση πρέπει να καλύπτει τον τρόπο αναγνώρισης ενός μηνύματος ηλεκτρονικού «phishing», τον τρόπο δημιουργίας και διαχείρισης ισχυρών

Τι να κάνετε	Γιατί έχει σημασία	Πώς να το κάνετε
	που δεν μπορεί να αναγνωρίσει ένα μήνυμα ηλεκτρονικού ταχυδρομείου τύπου «phishing» αποτελεί ένα σημείο ευπάθειας από το οποίο κανένα τεχνικό σύστημα δεν μπορεί να προστατευθεί πλήρως. Ένα μόνο κλικ σε έναν κακόβουλο σύνδεσμο μπορεί να δώσει σε έναν εισβολέα πλήρη πρόσβαση στα συστήματα του σχολείου.	κωδικών πρόσβασης, τι πρέπει να γίνει σε περίπτωση απώλειας ή κλοπής μιας συσκευής, καθώς και σε ποιον πρέπει να απευθυνθεί κανείς αν κάτι φαίνεται ύποπτο. Προσθέστε περιοδικές υπενθυμίσεις καθ' όλη τη διάρκεια του έτους. Όπου είναι δυνατόν, διοργανώστε ασκήσεις προσομοίωσης «phishing»: αυτές αποτελούν έναν από τους πιο αποτελεσματικούς τρόπους για την αλλαγή της συμπεριφοράς του προσωπικού.

Τι είναι μια επίθεση phishing;

Το phishing συμβαίνει όταν ένας εισβολέας στέλνει ένα email, ένα μήνυμα ή μια ειδοποίηση που φαίνεται να προέρχεται από κάποιον αξιόπιστο, όπως το Υπουργείο Παιδείας, έναν πάροχο λογισμικού ή έναν συνάδελφο. Ο στόχος είναι να οδηγήσει τον παραλήπτη να κάνει κλικ σε έναν κακόβουλο σύνδεσμο, να εισαγάγει τα στοιχεία σύνδεσής του σε έναν πλαστό ιστότοπο ή να ανοίξει ένα μολυσμένο αρχείο. Το phishing αποτελεί τη συνηθέστερη μορφή κυβερνοεπίθεσης εναντίον σχολείων. Οποιοδήποτε απροσδόκητο μήνυμα που ζητά έναν κωδικό πρόσβασης, ζητά από κάποιον να κάνει κλικ σε έναν σύνδεσμο επειγόντως ή του ζητά να προβεί σε μια ασυνήθιστη ενέργεια πρέπει να αντιμετωπίζεται με καχυποψία και να επαληθεύεται μέσω ξεχωριστού καναλιού πριν απαντήσει κανείς.

3.3 Ασφαλής επιλογή και χρήση ψηφιακών πλατφορμών

Τα σχολεία χρησιμοποιούν έναν αυξανόμενο αριθμό ψηφιακών πλατφορμών για τη διδασκαλία, την επικοινωνία και τη διοίκηση. Κάθε πλατφόρμα που επεξεργάζεται δεδομένα μαθητών αποτελεί πιθανή πηγή κινδύνου. Μια πλατφόρμα με ανεπαρκή ασφάλεια, η οποία μοιράζεται δεδομένα με διαφημιστές ή αποθηκεύει πληροφορίες μαθητών εκτός της ΕΕ χωρίς τις κατάλληλες διασφαλίσεις, μπορεί να προκαλέσει πραγματική ζημιά. Τα σχολεία έχουν νομική υποχρέωση να ελέγχουν τις πλατφόρμες πριν από την υιοθέτησή τους και να τις διαχειρίζονται προσεκτικά μόλις τεθούν σε χρήση.

Το ίδιο ισχύει και για τα εργαλεία τεχνητής νοημοσύνης. Η τεχνητή νοημοσύνη έχει όλο και μεγαλύτερη παρουσία στην εκπαίδευση, αλλά δεν είναι όλα τα εργαλεία ασφαλή για χρήση με μαθητές. Ο νόμος της ΕΕ για την τεχνητή νοημοσύνη θέτει σαφή όρια, και τα σχολεία πρέπει να γνωρίζουν πού βρίσκονται αυτά τα όρια πριν εισαγάγουν οποιοδήποτε εργαλείο τεχνητής νοημοσύνης στην τάξη ή σε διαδικασίες που αφορούν τους μαθητές.

Τι να κάνετε	Γιατί έχει σημασία	Πώς να το κάνετε
Ελέγξτε κάθε πλατφόρμα πριν	Μια πλατφόρμα που υιοθετείται χωρίς τους κατάλληλους ελέγχους	Πριν υιοθετήσετε οποιαδήποτε νέα πλατφόρμα, βεβαιωθείτε ότι συμμορφώνεται με τον ΓΚΠΔ, ότι δεν

Τι να κάνετε	Γιατί έχει σημασία	Πώς να το κάνετε
τη χρησιμοποιήσετε	ενδέχεται να επεξεργάζεται τα δεδομένα των μαθητών με τρόπους που το σχολείο δεν έχει εγκρίνει, να αποθηκεύει δεδομένα εκτός της ΕΕ ή να παρουσιάζει κενά ασφαλείας. Μόλις τα δεδομένα κοινοποιηθούν σε λάθος πάροχο, είναι πολύ δύσκολο να ανατραπεί η κατάσταση.	χρησιμοποιεί τα δεδομένα των μαθητών για διαφημιστικούς σκοπούς ούτε τα κοινοποιεί σε τρίτους χωρίς συγκατάθεση, και ότι αποθηκεύει τα δεδομένα εντός της ΕΕ. Εάν η πλατφόρμα συνεπάγεται επεξεργασία δεδομένων μαθητών σε μεγάλη κλίμακα, πραγματοποιήστε μια Εκτίμηση Αντικτύπου σχετικά με την Προστασία Δεδομένων πριν από τη θέση της σε λειτουργία (βλ. Παράρτημα V). Υπογράψτε συμφωνία επεξεργασίας δεδομένων με τον πάροχο πριν από οποιαδήποτε κοινοποίηση δεδομένων
Τηρείτε κατάλογο με τις εγκεκριμένες πλατφόρμες	Χωρίς ένα κεντρικό αρχείο καταγραφής, τα σχολεία χάνουν την εικόνα για το ποιες πλατφόρμες χρησιμοποιούνται, πότε ελέγχθηκαν για τελευταία φορά ή ποιος τις ενέκρινε. Το προσωπικό ενδέχεται να αρχίσει να χρησιμοποιεί πλατφόρμες ανεπίσημα, χωρίς καμία αξιολόγηση. Οι μαθητές ενδέχεται να χρησιμοποιούν προσωπικούς λογαριασμούς σε μη εγκεκριμένα εργαλεία για τις σχολικές τους εργασίες, με αποτέλεσμα τα δεδομένα να βγαίνουν εκτός του ελέγχου του σχολείου.	Τηρείτε γραπτό μητρώο όλων των ψηφιακών πλατφορμών και εργαλείων που έχουν εγκριθεί για χρήση στο σχολείο σας. Καταγράψτε το όνομα της πλατφόρμας, τον σκοπό χρήσης της, πότε αξιολογήθηκε και πότε προβλέπεται η επόμενη επανεξέταση. Ελέγχετε το μητρώο τουλάχιστον μία φορά το χρόνο. Το προσωπικό δεν πρέπει να εισάγει νέες πλατφόρμες για χρήση στο σχολείο χωρίς να ακολουθήσει πρώτα τη διαδικασία έγκρισης.
Τοποθετήστε τις πλατφόρμες με ασφάλεια	Οι προεπιλεγμένες ρυθμίσεις στις πλατφόρμες συνήθως έχουν σχεδιαστεί με γνώμονα την ευκολία χρήσης και όχι την ασφάλεια. Μια εικονική τάξη στην οποία μπορεί να συμμετάσχει οποιοσδήποτε χωρίς να συνδεθεί, μια λειτουργία	Κάθε πλατφόρμα πρέπει να ρυθμιστεί με ασφάλεια πριν αρχίσουν να τη χρησιμοποιούν οι μαθητές ή το προσωπικό. Τα εργαλεία τηλεδιάσκεψης πρέπει να απαιτούν σύνδεση πριν μπορέσει οποιοσδήποτε να συμμετάσχει σε μια εικονική τάξη. Η λειτουργία εγγραφής πρέπει να είναι απενεργοποιημένη από προεπιλογή και να ενεργοποιείται μόνο με τη ρητή συγκατάθεση όλων των

Τι να κάνετε	Γιατί έχει σημασία	Πώς να το κάνετε
	εγγραφής που είναι ενεργοποιημένη από προεπιλογή ή λογαριασμοί μαθητών με υπερβολικά δικαιώματα: όλα αυτά δημιουργούν κινδύνους που είναι εύκολο να αποφευχθούν.	παρευρισκομένων. Οι λογαριασμοί των μαθητών πρέπει να διαθέτουν μόνο τα δικαιώματα που χρειάζονται για τις εκπαιδευτικές τους δραστηριότητες. Ελέγξτε τις ρυθμίσεις τουλάχιστον μία φορά το χρόνο.
Μάθετε ποιες χρήσεις της τεχνητής νοημοσύνης απαγορεύονται	Ορισμένες πρακτικές χρήσης της τεχνητής νοημοσύνης σε εκπαιδευτικά περιβάλλοντα απαγορεύονται από τη νομοθεσία της ΕΕ. Αυτό ισχύει ανεξάρτητα από τον τρόπο προώθησης του εργαλείου στην αγορά ή από τους ισχυρισμούς του προμηθευτή. Η απαγόρευση είναι απόλυτη και ισχύει για όλα τα σχολεία και στις πέντε χώρες.	Μην χρησιμοποιείτε κανένα εργαλείο τεχνητής νοημοσύνης που περιλαμβάνει την αναγνώριση των συναισθημάτων των μαθητών, την κατηγοριοποίησή τους με βάση βιομετρικά δεδομένα ή την ταυτοποίησή τους σε πραγματικό χρόνο μέσω αναγνώρισης προσώπου. Οι χρήσεις αυτές απαγορεύονται βάσει του άρθρου 5 του νόμου της ΕΕ για την τεχνητή νοημοσύνη. Εάν ένας προμηθευτής προσφέρει αυτές τις λειτουργίες, το σχολείο δεν πρέπει να τις χρησιμοποιεί. Εάν το σχολείο χρησιμοποιεί ήδη ένα τέτοιο εργαλείο, πρέπει να σταματήσει τη χρήση του.
Οι άνθρωποι πρέπει να έχουν τον έλεγχο των αποφάσεων που αφορούν τους μαθητές	Τα εργαλεία τεχνητής νοημοσύνης μπορούν να παράγουν συστάσεις που είναι λανθασμένες, μεροληπτικές ή άδικες. Όταν αυτές οι συστάσεις επηρεάζουν την τύχη ενός μαθητή —όπως για παράδειγμα έναν βαθμό, μια παραπομπή ή μια αξιολόγηση των μαθησιακών αναγκών—, οι συνέπειες μπορεί να είναι σοβαρές. Ο νόμος απαιτεί να υπάρχει υπεύθυνος άνθρωπος ακριβώς για αυτόν τον λόγο.	Ένας εκπαιδευτικός ή ένας υπεύθυνος ενήλικας πρέπει πάντα να ελέγχει και να αναλαμβάνει την ευθύνη για κάθε αποτέλεσμα που προκύπτει από ένα εργαλείο τεχνητής νοημοσύνης και επηρεάζει έναν μαθητή. Τα εργαλεία τεχνητής νοημοσύνης μπορούν να βοηθήσουν, αλλά δεν μπορούν να λαμβάνουν τελικές αποφάσεις. Καταγράψτε τον τρόπο με τον οποίο ασκείται η ανθρώπινη εποπτεία για κάθε εργαλείο τεχνητής νοημοσύνης που χρησιμοποιείται στη λήψη εκπαιδευτικών αποφάσεων.
Ενημερώστε τους μαθητές και	Οι μαθητές και οι γονείς έχουν το δικαίωμα να	Όταν ένα εργαλείο τεχνητής νοημοσύνης χρησιμοποιείται με τρόπο που επηρεάζει

Τι να κάνετε	Γιατί έχει σημασία	Πώς να το κάνετε
τους γονείς όταν χρησιμοποιείται τεχνητή νοημοσύνη.	γνωρίζουν πότε χρησιμοποιούνται εργαλεία τεχνητής νοημοσύνης με τρόπους που επηρεάζουν την εκπαίδευση ενός μαθητή. Η χρήση εργαλείων τεχνητής νοημοσύνης χωρίς να ενημερώνονται ενδέχεται να αποτελεί παραβίαση τόσο του Νόμου για την Τεχνητή Νοημοσύνη όσο και του Γενικού Κανονισμού για την Προστασία Δεδομένων (GDPR).	τη μάθηση ή την αξιολόγηση ενός μαθητή, ενημερώστε τους μαθητές και τους γονείς με σαφήνεια και απλή γλώσσα: τι κάνει το εργαλείο, ποια δεδομένα χρησιμοποιεί, πώς χρησιμοποιούνται τα αποτελέσματά του και πώς λειτουργεί η ανθρώπινη εποπτεία. Παρέχετε αυτές τις πληροφορίες πριν από τη χρήση του εργαλείου και φροντίστε να είναι μόνιμα προσβάσιμες.
Τηρείτε αρχείο με όλα τα εργαλεία τεχνητής νοημοσύνης που χρησιμοποιείτε	Τα σχολεία που δεν γνωρίζουν ποια εργαλεία τεχνητής νοημοσύνης χρησιμοποιούν, ποια δεδομένα επεξεργάζονται τα εργαλεία αυτά ή ποια αξιολόγηση πραγματοποιήθηκε πριν από την υιοθέτησή τους δεν μπορούν να εκπληρώσουν τις νομικές τους υποχρεώσεις βάσει του Νόμου για την Τεχνητή Νοημοσύνη ή του ΓΚΠΔ.	Τηρείτε μητρώο εργαλείων τεχνητής νοημοσύνης ως μέρος του καταλόγου των εγκεκριμένων πλατφορμών σας. Για κάθε εργαλείο τεχνητής νοημοσύνης, καταγράψτε τη λειτουργία του, την κατηγορία κινδύνου στην οποία εμπίπτει σύμφωνα με τον Νόμο για την Τεχνητή Νοημοσύνη, τα δεδομένα που επεξεργάζεται, την αξιολόγηση που πραγματοποιήθηκε πριν από την υιοθέτησή του και ποιος είναι υπεύθυνος για την εποπτεία του. Ελέγχετε αυτό το αρχείο τουλάχιστον μία φορά το χρόνο.

3.4 Διαχείριση κινητών τηλεφώνων και προσωπικών συσκευών

Και οι πέντε χώρες-εταίροι έχουν θεσπίσει νομικούς περιορισμούς στη χρήση κινητών τηλεφώνων στα σχολεία. Οι συγκεκριμένοι κανόνες διαφέρουν από χώρα σε χώρα (βλ. Μέρος 2), αλλά οι λόγοι είναι οι ίδιοι παντού: τα τηλέφωνα στις αίθουσες διδασκαλίας αποσπούν την προσοχή των μαθητών από τη μάθηση, δημιουργούν κινδύνους για την ιδιωτικότητα και την προστασία των δεδομένων, διευκολύνουν τον διαδικτυακό εκφοβισμό και επιτείνουν τις ψηφιακές πιέσεις που επηρεάζουν την ψυχική υγεία των μαθητών.

Μια πολιτική για τα κινητά τηλέφωνα είναι κάτι περισσότερο από έναν πειθαρχικό κανόνα. Αποτελεί μέτρο προστασίας των δεδομένων, μέτρο για την ευημερία και δήλωση των αξιών του σχολείου. Μια πολιτική που είναι σαφώς διατυπωμένη, κατανοείται πραγματικά από τους μαθητές,

τους γονείς και το προσωπικό και εφαρμόζεται με συνέπεια είναι πολύ πιο αποτελεσματική από μια πολιτική που υπάρχει μόνο στα χαρτιά.

Τι να κάνετε	Γιατί έχει σημασία	Πώς να το κάνετε
Διαθέστε μια σαφή, γραπτή πολιτική σχετικά με τη χρήση κινητών τηλεφώνων	Χωρίς γραπτή πολιτική, οι κανόνες εφαρμόζονται με διαφορετικό τρόπο από τους διάφορους εκπαιδευτικούς. Οι μαθητές και οι γονείς δεν μπορούν να υποχρεωθούν να τηρούν κανόνες για τους οποίους δεν έχουν ενημερωθεί σαφώς. Η ασυνεπής εφαρμογή των κανόνων δημιουργεί συγκρούσεις και υπονομεύει την εμπιστοσύνη στους κανόνες του σχολείου.	Συντάξτε έναν κανονισμό για τη χρήση κινητών τηλεφώνων, ο οποίος να καθορίζει πότε επιτρέπεται και πότε δεν επιτρέπεται η χρήση τους, πού πρέπει να φυλάσσονται κατά τις ώρες απαγόρευσης, ποιες εξαιρέσεις ισχύουν για ιατρικούς λόγους ή συγκεκριμένες εκπαιδευτικές δραστηριότητες, καθώς και τι συμβαίνει σε περίπτωση παράβασης των κανόνων. Κοινοποιήστε τον κανονισμό στους μαθητές και στους γονείς στην αρχή κάθε σχολικού έτους μέσω της «Πολιτικής Αποδεκτής Χρήσης» (Παράρτημα III). Ενσωματώστε τον στους εσωτερικούς κανονισμούς του σχολείου.
Περιορίστε τη χρήση των κινητών τηλεφώνων κατά τη διάρκεια των μαθημάτων	Η απεριόριστη χρήση κινητών τηλεφώνων κατά τη διάρκεια των μαθημάτων διαταράσσει τη μάθηση, δημιουργεί ευκαιρίες για διαδικτυακό εκφοβισμό και μη εξουσιοδοτημένη καταγραφή, και επιτείνει τις ψηφιακές πιέσεις που επηρεάζουν την ευημερία των μαθητών. Οι έρευνες δείχνουν με συνέπεια ότι οι μαθητές σε σχολεία με σαφείς περιορισμούς στη χρήση κινητών τηλεφώνων έχουν καλύτερες ακαδημαϊκές επιδόσεις και αναφέρουν υψηλότερα επίπεδα ευημερίας.	Οι μαθητές δεν πρέπει να χρησιμοποιούν τα προσωπικά τους κινητά τηλέφωνα κατά τη διάρκεια των μαθημάτων, εκτός εάν ο καθηγητής το έχει επιτρέψει ρητά για μια συγκεκριμένη εκπαιδευτική δραστηριότητα. Σε χώρες όπου ισχύει νομική απαγόρευση, αυτή πρέπει να τηρείται. Να διευκρινίζετε πού πρέπει να φυλάσσονται τα τηλέφωνα κατά τις ώρες που ισχύει ο περιορισμός. Οι εξαιρέσεις για ιατρικούς λόγους πρέπει να τεκμηριώνονται.
Απαγόρευση της μη εξουσιοδοτημένης εγγραφής	Οι μη εξουσιοδοτημένες ηχογραφήσεις μαθητών, εκπαιδευτικών ή άλλων μελών του προσωπικού αποτελούν σοβαρή	Καταστήστε απολύτως σαφές στους μαθητές και το προσωπικό ότι απαγορεύεται η καταγραφή οποιουδήποτε ατόμου στο σχολείο χωρίς τη ρητή συγκατάθεσή του, είτε κατά τη

Τι να κάνετε	Γιατί έχει σημασία	Πώς να το κάνετε
	παραβίαση της ιδιωτικής ζωής και ενδέχεται να συνιστούν ποινικό αδίκημα σύμφωνα με την εθνική νομοθεσία. Οι ηχογραφήσεις που κοινοποιούνται στο διαδίκτυο μπορούν να προκαλέσουν μόνιμη ζημιά στα εμπλεκόμενα άτομα και στο σχολείο. Η δημοτικότητα των πλατφορμών σύντομων βίντεο καθιστά τον κίνδυνο αυτό ολοένα και μεγαλύτερο.	διάρκεια των μαθημάτων, είτε στους διαδρόμους, είτε σε εκδρομές, είτε σε εκδηλώσεις. Αναφέρετε με σαφήνεια τις συνέπειες. Αντιμετωπίστε κάθε μη εξουσιοδοτημένη καταγραφή που αφορά μαθητές ή προσωπικό ως σοβαρό πειθαρχικό παράπτωμα και, όπου κρίνεται απαραίτητο, παραπέμψτε την υπόθεση στις αρμόδιες αρχές.
Εφαρμόστε τα πρότυπα ασφαλείας στις προσωπικές συσκευές που χρησιμοποιούνται για σχολικές εργασίες	Όταν ένας εκπαιδευτικός χρησιμοποιεί προσωπική συσκευή για να συνδεθεί στα συστήματα του σχολείου, η προστασία των δεδομένων του σχολείου εξαρτάται από τον πιο αδύναμο κρίκο. Μια προσωπική συσκευή με αδύναμο κωδικό πρόσβασης, ξεπερασμένο λογισμικό ή δεδομένα μαθητών που είναι αποθηκευμένα τοπικά αποτελεί πραγματικό σημείο ευπάθειας.	Τα μέλη του προσωπικού που χρησιμοποιούν προσωπικές συσκευές για σχολικές εργασίες πρέπει να τις προστατεύουν με ισχυρό κωδικό πρόσβασης ή PIN, να διατηρούν το λογισμικό τους ενημερωμένο, να χρησιμοποιούν ασφαλή σύνδεση όταν εργάζονται εξ αποστάσεως και να μην αποθηκεύουν δεδομένα μαθητών τοπικά στις προσωπικές τους συσκευές. Δώστε σαφείς οδηγίες στο προσωπικό σχετικά με το τι αναμένεται από αυτό.

3.5 Πρόληψη και αντιμετώπιση του διαδικτυακού εκφοβισμού

Ο διαδικτυακός εκφοβισμός είναι ο εκφοβισμός που λαμβάνει χώρα μέσω ψηφιακών συσκευών και πλατφορμών. Περιλαμβάνει την αποστολή απειλητικών ή ταπεινωτικών μηνυμάτων, τη διανομή ιδιωτικών εικόνων χωρίς συγκατάθεση, τη διάδοση ψευδών πληροφοριών στο διαδίκτυο και τον σκόπιμο αποκλεισμό κάποιου από διαδικτυακές ομάδες. Ο διαδικτυακός εκφοβισμός μπορεί να προκαλέσει σοβαρή και μακροχρόνια βλάβη στην ψυχική υγεία, τις ακαδημαϊκές επιδόσεις και τις κοινωνικές σχέσεις των μαθητών.

Τα σχολεία έχουν τόσο νομική υποχρέωση όσο και καθήκον φροντίδας να προλαμβάνουν τον διαδικτυακό εκφοβισμό και να αντιδρούν όταν συμβαίνει. Ο διαδικτυακός εκφοβισμός δεν σταματάει στην πύλη του σχολείου. Ό,τι συμβαίνει στο διαδίκτυο στο σπίτι το βράδυ μπορεί να

επηρεάσει την εμπειρία ενός μαθητή στο σχολείο την επόμενη μέρα, και το αντίστροφο. Τα σχολεία πρέπει να αντιμετωπίζουν τον διαδικτυακό εκφοβισμό με την ίδια σοβαρότητα όπως τον φυσικό εκφοβισμό, ακόμη και όταν συμβαίνει εκτός σχολικού ωραρίου.

Τι να κάνετε	Γιατί έχει σημασία	Πώς να το κάνετε
Συμπεριλάβετε ρητά τον διαδικτυακό εκφοβισμό στην πολιτική σας κατά του εκφοβισμού	Μια γενική πολιτική κατά του εκφοβισμού που δεν αναφέρεται στον εκφοβισμό στο διαδίκτυο αφήνει περιθώρια αμφιβολίας ως προς το αν καλύπτεται η συμπεριφορά στο διαδίκτυο. Οι μαθητές που υφίστανται εκφοβισμό στο διαδίκτυο ενδέχεται να μην το αναφέρουν, επειδή πιστεύουν ότι το σχολείο θα ισχυριστεί ότι δεν αποτελεί δικό του πρόβλημα.	Ενημερώστε την πολιτική σας κατά του εκφοβισμού, ώστε να περιλαμβάνει ένα ειδικό τμήμα για τον εκφοβισμό στο διαδίκτυο. Η πολιτική αυτή θα πρέπει να ορίζει τι είναι ο εκφοβισμός στο διαδίκτυο, να καθιστά σαφές ότι αντιμετωπίζεται με την ίδια σοβαρότητα όπως ο φυσικός εκφοβισμός και να επιβεβαιώνει ότι η πολιτική ισχύει και για τη συμπεριφορά στο διαδίκτυο εκτός των σχολικών ωρών, όταν αυτή επηρεάζει άμεσα τη σχολική κοινότητα. Επανεξετάστε την πολιτική τουλάχιστον μία φορά το χρόνο.
Ενημερώστε τους μαθητές σχετικά με τον διαδικτυακό εκφοβισμό	Οι μαθητές που κατανοούν τι είναι ο διαδικτυακός εκφοβισμός, γιατί προκαλεί βλάβη και τι πρέπει να κάνουν όταν τον παρατηρούν, είναι πιο πιθανό να τον αναφέρουν και να στηρίξουν έναν συμμαθητή τους που έχει γίνει στόχος. Το να διδάσκουμε στους μαθητές να είναι ενεργοί και υποστηρικτικοί μάρτυρες αποτελεί μία από τις πιο αποτελεσματικές προσεγγίσεις που υπάρχουν.	Η εκπαίδευση σχετικά με τον διαδικτυακό εκφοβισμό πρέπει να είναι κατάλληλη για την ηλικία των μαθητών και να αποτελεί τακτικό μέρος του προγράμματος σπουδών, όχι μια μεμονωμένη δραστηριότητα. Πρέπει να καλύπτει τις διάφορες μορφές του διαδικτυακού εκφοβισμού στις διάφορες πλατφόρμες, τη βλάβη που προκαλεί, τον τρόπο υποστήριξης ενός ατόμου που έχει γίνει στόχος, καθώς και τον τρόπο αναφοράς του περιστατικού. Εμπλέξτε τους μαθητές στη διαμόρφωση του περιεχομένου: τα μηνύματα στα οποία έχουν συμβάλει στη δημιουργία τους τα αφορούν περισσότερο.
Παρέχετε στους μαθητές έναν σαφή και ασφαλή τρόπο να αναφέρουν περιστατικά	Πολλοί μαθητές που υφίστανται διαδικτυακό εκφοβισμό δεν το αναφέρουν. Ανησυχούν ότι δεν θα τους πιστέψουν, ότι η	Προσφέρετε περισσότερους από έναν τρόπους αναφοράς περιστατικών διαδικτυακού εκφοβισμού: έναν έμπιστο ενήλικα, μια ανώνυμη φόρμα ή θυρίδα και, όπου είναι διαθέσιμη, την εθνική πλατφόρμα αναφοράς (βλ. Μέρος 2). Προωθήστε ενεργά αυτές τις επιλογές καθ' όλη

Τι να κάνετε	Γιατί έχει σημασία	Πώς να το κάνετε
	αναφορά θα επιδεινώσει την κατάσταση ή ότι θα χάσουν την πρόσβαση στο κινητό τους. Χωρίς έναν αξιόπιστο και προσιτό τρόπο αναφοράς, τα περιστατικά παραμένουν κρυφά και επιδεινώνονται.	τη διάρκεια του σχολικού έτους, όχι μόνο τον Σεπτέμβριο. Όταν ένας μαθητής υποβάλλει αναφορά, ανταποκριθείτε γρήγορα και καταστήστε σαφές ότι το αντιμετωπίζετε με σοβαρότητα.
Εκπαίδευση όλου του προσωπικού ώστε να αναγνωρίζει και να αντιμετωπίζει τον διαδικτυακό εκφοβισμό	Πολλοί εκπαιδευτικοί δεν ξέρουν πώς να αντιδράσουν στο διαδικτυακό εκφοβισμό, ειδικά όταν αυτός αφορά πλατφόρμες με τις οποίες δεν είναι εξοικειωμένοι. Η αβεβαιότητα αυτή οδηγεί σε ασυνεπείς αντιδράσεις, οι οποίες υπονομεύουν τόσο την ικανότητα του θύματος όσο και του σχολείου να διαχειριστούν αποτελεσματικά τα περιστατικά.	Παρέχετε σε όλο το προσωπικό εκπαίδευση που να καλύπτει τους τρόπους αναγνώρισης των ενδείξεων ότι ένας μαθητής ενδέχεται να υφίσταται διαδικτυακό εκφοβισμό, ποια είναι η διαδικασία του σχολείου και ποιος είναι ο ρόλος του προσωπικού σε αυτήν, πώς να διατηρούν τα αποδεικτικά στοιχεία, συμπεριλαμβανομένων των στιγμιότυπων οθόνης, πότε πρέπει να εμπλέκονται ο σχολικός σύμβουλος, οι γονείς ή εξωτερικές αρχές, καθώς και πώς να υποστηρίζουν έναν μαθητή χωρίς να επιδεινώσουν κατά λάθος την κατάσταση.
Ανταποκριθείτε γρήγορα και καταγράψτε τα πάντα	Μια αργή ή ασυνεπής αντίδραση δίνει την εντύπωση ότι το σχολείο δεν αντιμετωπίζει σοβαρά το φαινόμενο του διαδικτυακού εκφοβισμού. Επιπλέον, επιτρέπει την κλιμάκωση των περιστατικών και την απώλεια αποδεικτικών στοιχείων. Τα σχολεία που δεν τηρούν κατάλληλα αρχεία δυσκολεύονται να εντοπίσουν μοτίβα ή να αποδείξουν ότι ενήργησαν σωστά, σε περίπτωση που υποβληθεί επίσημη καταγγελία	Όταν αναφέρεται ένα περιστατικό διαδικτυακού εκφοβισμού, πρώτη προτεραιότητα είναι η ασφάλεια και η ευημερία του μαθητή που έγινε στόχος. Καταγράψτε αμέσως τις λεπτομέρειες: την ημερομηνία και την ώρα, τι συνέβη, ποιες πλατφόρμες εμπλέκονταν, ποιοι εμπλέκονταν, τυχόν αποδεικτικά στοιχεία που συλλέχθηκαν και κάθε ενέργεια που πραγματοποιήθηκε. Εφαρμόστε τη πειθαρχική διαδικασία με συνέπεια. Επικοινωνήστε με τον μαθητή που έγινε στόχος τις ημέρες και τις εβδομάδες μετά το περιστατικό.

Τι να κάνετε	Γιατί έχει σημασία	Πώς να το κάνετε
Να εμπλέξουμε τους γονείς ως συνεργάτες	Οι γονείς που κατανοούν το φαινόμενο του διαδικτυακού εκφοβισμού, ξέρουν πώς να μιλήσουν στα παιδιά τους για αυτό και αισθάνονται ότι συντονίζονται με την προσέγγιση του σχολείου, είναι πολύ πιο αποτελεσματικοί τόσο στην πρόληψη περιστατικών όσο και στη στήριξη των παιδιών τους όταν συμβαίνουν τέτοια περιστατικά.	Στην αρχή της σχολικής χρονιάς, ενημερώστε τους γονείς σχετικά με την προσέγγιση του σχολείου όσον αφορά τον διαδικτυακό εκφοβισμό, τι πρέπει να κάνουν αν το παιδί τους επηρεαστεί από αυτόν και πώς θα επικοινωνεί μαζί τους το σχολείο. Χρησιμοποιήστε το πρότυπο που βρίσκεται στο Παράρτημα II. Όταν συμβαίνουν περιστατικά, ενημερώστε τους γονείς όλων των μαθητών που έχουν επηρεαστεί, ακολουθώντας τις διαδικασίες του σχολείου.

3.6 Υποστήριξη της ψηφιακής ευημερίας των μαθητών

Οι μαθητές αντιμετωπίζουν κινδύνους στο διαδίκτυο που υπερβαίνουν τον διαδικτυακό εκφοβισμό και τις παραβιάσεις δεδομένων. Πολλοί βιώνουν άγχος, χαμηλή αυτοεκτίμηση και κοινωνική πίεση που συνδέονται με την ψηφιακή τους ζωή. Ο φόβος να χάσουν κάτι σημαντικό (FOMO), η πίεση να παρουσιάσουν μια εξιδανικευμένη εικόνα του εαυτού τους στο διαδίκτυο, η συνεχής σύγκριση με τους άλλους, ο υπερβολικός χρόνος μπροστά στην οθόνη και ο σχεδιασμός των πλατφορμών κοινωνικής δικτύωσης που δίνουν προτεραιότητα στην αλληλεπίδραση έναντι της ευημερίας, όλα αυτά συμβάλλουν σε προβλήματα ψυχικής υγείας που επηρεάζουν σημαντικό αριθμό νέων.

Ο περιορισμός της πρόσβασης από μόνος του δεν επιλύει αυτά τα προβλήματα. Οι μαθητές στους οποίους απλώς ζητείται να χρησιμοποιούν λιγότερο την τεχνολογία, χωρίς να τους βοηθούν να κατανοήσουν το γιατί ή να τους παρέχονται εργαλεία για τη διαχείριση της συμπεριφοράς τους, τείνουν να επιστρέφουν στις παλιές τους συνήθειες μόλις αρθεί ο περιορισμός. Τα σχολεία που επιτυγχάνουν διαρκή θετική αλλαγή είναι εκείνα που συνδυάζουν σαφή όρια με ειλικρινή, τεκμηριωμένη εκπαίδευση και μια κουλτούρα όπου οι μαθητές αισθάνονται ασφαλείς να μιλήσουν για ό,τι βιώνουν στο διαδίκτυο.

Τι να κάνετε	Γιατί έχει σημασία	Πώς να το κάνετε
Να εντάξετε την ψηφιακή ευημερία στη διακονική φροντίδα	Οι μαθητές που αντιμετωπίζουν δυσκολίες στη διαδικτυακή τους ζωή, αντιμετωπίζουν επίσης προβλήματα όσον αφορά τη γενική ψυχική τους υγεία και την κοινωνική τους εμπειρία. Εάν η ψηφιακή ευημερία αντιμετωπίζεται ως ξεχωριστό θέμα	Η ψηφιακή ευημερία θα πρέπει να αποτελεί ξεχωριστό τμήμα του ευρύτερου προγράμματος ευημερίας και ψυχολογικής υποστήριξης του σχολείου. Το προσωπικό που υποστηρίζει τους μαθητές σε άλλες δυσκολίες θα πρέπει επίσης να είναι έτοιμο να τους υποστηρίξει και σε ψηφιακά ζητήματα. Οι διαδικασίες παραπομπής θα πρέπει να είναι σαφείς: κάθε εκπαιδευτικός που εντοπίζει έναν μαθητή που αντιμετωπίζει δυσκολίες θα πρέπει να γνωρίζει ακριβώς σε ποιον να

Τι να κάνετε	Γιατί έχει σημασία	Πώς να το κάνετε
	πληροφορικής, οι μαθητές που χρειάζονται υποστήριξη ενδέχεται να παραμείνουν εκτός του πλαισίου των παρεχόμενων υπηρεσιών.	απευθυνθεί και ποια θα είναι τα επόμενα βήματα.
Διδάξτε στους μαθητές υγιείς ψηφιακές συνήθειες	Οι μαθητές που κατανοούν πώς έχουν σχεδιαστεί οι πλατφόρμες κοινωνικών μέσων ώστε να τους κρατούν κολλημένους στην οθόνη, που μπορούν να διακρίνουν τη διαφορά μεταξύ μιας επιμελημένης διαδικτυακής εικόνας και της πραγματικότητας, και που έχουν αναπτύξει τις δικές τους στρατηγικές για τη διαχείριση των ψηφιακών τους συνηθειών, είναι σε καλύτερη θέση να περιηγούνται με ασφάλεια στον διαδικτυακό κόσμο.	Εντάξτε την εκπαίδευση για την ψηφιακή ευημερία ως τακτικό μέρος του προγράμματος σπουδών. Διδάξτε στους μαθητές πώς λειτουργούν οι αλγόριθμοι προτάσεων και γιατί συχνά εμφανίζουν περιεχόμενο που προκαλεί έντονα συναισθήματα. Συζητήστε τις επιπτώσεις της παθητικής περιήγησης στα μέσα κοινωνικής δικτύωσης στη διάθεση και την αυτοεκτίμηση. Βοηθήστε τους μαθητές να αναπτύξουν πρακτικές στρατηγικές για τον καθορισμό ορίων όσον αφορά τη δική τους χρήση της τεχνολογίας.
Βεβαιωθείτε ότι οι μαθητές γνωρίζουν πού μπορούν να βρουν βοήθεια	Πολλοί μαθητές που αντιμετωπίζουν δυσκολίες με κάτι στο διαδίκτυο δεν ζητούν βοήθεια επειδή δεν γνωρίζουν ότι υπάρχει διαθέσιμη βοήθεια, επειδή ντρέπονται ή επειδή φοβούνται ότι θα τους πάρουν το κινητό. Αν η υποστήριξη δεν προωθείται ενεργά, παραμένει αόρατη για τους μαθητές που την έχουν περισσότερο ανάγκη.	Υπενθυμίζετε τακτικά στους μαθητές σε ποιον μπορούν να απευθυνθούν αν κάτι στο διαδίκτυο τους ενοχλεί. Αναφέρετε το θέμα αυτό στις συγκεντρώσεις, στα μαθήματα και στις καθημερινές σας συνομιλίες, όχι μόνο στο εγχειρίδιο. Το άτομο στο οποίο θα απευθυνθεί ένας μαθητής δεν χρειάζεται να είναι ειδικός στην τεχνολογία. Αρκεί να είναι κάποιος που ο μαθητής εμπιστεύεται, ο οποίος θα τον ακούσει χωρίς να τον κρίνει και θα τον κατευθύνει προς την κατάλληλη βοήθεια.
Μην επιβαρύνετε την ψηφιακή πίεση με σχολικές πρακτικές	Τα σχολεία μπορεί να δημιουργήσουν ακούσια τις ίδιες ψηφιακές πιέσεις που προσπαθούν να μειώσουν. Οι	Εξετάστε τον τρόπο με τον οποίο το σχολείο επικοινωνεί ψηφιακά και αν κάποιες από τις πρακτικές του συμβάλλουν στη δημιουργία ψηφιακής πίεσης. Αποφύγετε τις υποχρεωτικές ομαδικές συνομιλίες που θολώνουν τα όρια

Τι να κάνετε	Γιατί έχει σημασία	Πώς να το κάνετε
	υποχρεωτικές ομαδικές συνομιλίες στο σχολείο, η προσδοκία ότι οι μαθητές θα απαντούν σε μηνύματα εκτός σχολικού ωραρίου, καθώς και οι δημόσιες συγκρίσεις μεταξύ μαθητών στο διαδίκτυο μπορούν όλα να μεταδώσουν μηνύματα που δεν βοηθούν.	μεταξύ σχολικού και προσωπικού χρόνου. Μην περιμένετε από τους μαθητές ή τους γονείς να απαντούν σε μηνύματα εκτός των κανονικών ωρών. Αποφύγετε τη δημοσίευση κατατάξεων ή συγκρίσεων στο διαδίκτυο.
Να αναγνωρίζετε πότε ένας μαθητής αντιμετωπίζει δυσκολίες	Οι μαθητές που αντιμετωπίζουν δυσκολίες στη ψηφιακή τους ζωή μπορεί να μην το εκφράσουν άμεσα. Τα σημάδια είναι συχνά συμπεριφορικά και εύκολο να περάσουν απαρατήρητα, εκτός αν το προσωπικό γνωρίζει τι πρέπει να προσέξει.	Παρέχετε οδηγίες στο προσωπικό σχετικά με τα σημάδια που υποδηλώνουν ότι ένας μαθητής ενδέχεται να αντιμετωπίζει δυσκολίες στη ψηφιακή του ζωή: ασυνήθιστο άγχος λόγω της αδυναμίας να ελέγξει το κινητό του, εναλλαγές διάθεσης μετά από διαδικτυακές αλληλεπιδράσεις, απομάκρυνση από τις κοινωνικές δραστηριότητες μετά από κάποιο περιστατικό που συνέβη στο διαδίκτυο, δυσφορία που σχετίζεται με την εμφάνισή του ή με τον τρόπο που τον βλέπουν οι άλλοι στο διαδίκτυο, απροθυμία να έρθει στο σχολείο μετά από κάποιο διαδικτυακό περιστατικό, ή οποιοδήποτε σημάδι ότι δέχεται πίεση ή αποτελεί στόχο στο διαδίκτυο. Όταν εμφανίζονται αυτά τα σημάδια, το προσωπικό πρέπει να ακολουθεί τη διαδικασία παραπομπής του σχολείου για την παροχή ψυχολογικής υποστήριξης.

3.7 Ποικιλομορφία, ένταξη και ψηφιακή ισότητα

Δεν αντιμετωπίζουν όλοι οι μαθητές τους ίδιους ψηφιακούς κινδύνους ούτε έχουν την ίδια πρόσβαση σε υποστήριξη. Το φύλο, ο σεξουαλικός προσανατολισμός, η αναπηρία, το οικογενειακό εισόδημα και οι ανησυχίες σχετικά με την εικόνα του σώματος διαμορφώνουν την εμπειρία ενός μαθητή στο διαδίκτυο και την ικανότητά του να ζητήσει βοήθεια όταν κάτι πάει στραβά. Μια πολιτική που λειτουργεί καλά για τους περισσότερους μαθητές, αλλά παραβλέπει την εμπειρία άλλων, δεν είναι ολοκληρωμένη.

Η ανάπτυξη μιας προσέγγισης χωρίς αποκλεισμούς όσον αφορά την ψηφιακή ασφάλεια σημαίνει να σκεφτόμαστε ενεργά ποιοι μαθητές διατρέχουν τον μεγαλύτερο κίνδυνο και να διασφαλίζουμε ότι οι πολιτικές, η εκπαίδευση και τα συστήματα υποστήριξης του σχολείου τους φτάνουν.

Τι να κάνετε	Γιατί έχει σημασία	Πώς να το κάνετε
Να αντιμετωπιστούν ρητά οι διαδικτυακές βλάβες που βασίζονται στο φύλο και στην ταυτότητα	Τα κορίτσια αντιμετωπίζουν δυσανάλογα υψηλά ποσοστά σεξουαλικής παρενόχλησης στο διαδίκτυο, κακοποίησης μέσω εικόνων και διαδικτυακού εκφοβισμού που συνδέεται με την εμφάνιση. Οι μαθητές της LGBTQ+ κοινότητας είναι σημαντικά πιο πιθανό να υποστούν διαδικτυακή παρενόχληση και, ως αποτέλεσμα, να αντιμετωπίσουν προβλήματα ψυχικής υγείας. Έρευνες δείχνουν ότι η αναφερόμενη συχνότητα του διαδικτυακού εκφοβισμού μεταξύ των μαθητών της LGBTQ+ κοινότητας παρουσιάζει μεγάλες διακυμάνσεις: από περίπου 10% έως πάνω από 70%, ανάλογα με το πλαίσιο, και ότι οι μαθητές της LGB κοινότητας αναφέρουν ότι υφίστανται διαδικτυακό εκφοβισμό σε ποσοστό περίπου διπλάσιο από αυτό των ετεροφυλόφιλων συνομηλίκων τους. Οι έρευνες δείχνουν ότι ο διαδικτυακός εκφοβισμός συμβάλλει στατιστικά σε μεγάλο βαθμό στο αυξημένο άγχος, την κατάθλιψη και τη μοναξιά που αναφέρουν οι μαθητές που ανήκουν σε σεξουαλικές μειονότητες, πράγμα που σημαίνει ότι η προληπτική δράση χωρίς αποκλεισμούς αποτελεί κεντρικό μηχανισμό για την προστασία της ψυχικής υγείας αυτής της ομάδας. Μια πολιτική που δεν κατονομάζει αυτές τις συγκεκριμένες μορφές βλάβης αφήνει τους πιο ευάλωτους μαθητές χωρίς επαρκή προστασία.	Ενημερώστε την πολιτική του σχολείου κατά του διαδικτυακού εκφοβισμού ώστε να καλύπτει ρητά την διαδικτυακή παρενόχληση λόγω φύλου, τη σεξουαλική παρενόχληση, τη διανομή προσωπικών εικόνων χωρίς συγκατάθεση, καθώς και την παρενόχληση λόγω σεξουαλικού προσανατολισμού ή ταυτότητας φύλου. Βεβαιωθείτε ότι η εκπαίδευση του προσωπικού καλύπτει αυτές τις συγκεκριμένες μορφές βλάβης και τον τρόπο αντιμετώπισής τους. Δημιουργήστε ένα σχολικό περιβάλλον όπου κάθε μαθητής αισθάνεται εξίσου ασφαλής να αναφέρει ό,τι του συμβαίνει.
Να καταστεί η εκπαίδευση σε θέματα ψηφιακής ασφάλειας προσβάσιμη	Οι μαθητές με αναπηρίες, συμπεριλαμβανομένων των μαθησιακών διαφορών, ενδέχεται να είναι πιο ευάλωτοι σε διαδικτυακή χειραγώγηση και	Βεβαιωθείτε ότι όλη η εκπαίδευση σε θέματα ψηφιακής ασφάλειας παρέχεται με τρόπους που να ανταποκρίνονται στις ανάγκες των μαθητών με διαφορετικές μαθησιακές ανάγκες

Τι να κάνετε	Γιατί έχει σημασία	Πώς να το κάνετε
στους μαθητές με αναπηρίες	εκμετάλλευση. Μπορεί επίσης να αντιμετωπίζουν μεγαλύτερες δυσκολίες στην πρόσβαση σε εκπαίδευση για την ψηφιακή ασφάλεια που δεν έχει σχεδιαστεί λαμβάνοντας υπόψη τις ανάγκες τους. Εάν οι μηχανισμοί αναφοράς δεν είναι προσβάσιμοι σε αυτούς, ουσιαστικά δεν υπάρχουν.	Ελέγξτε αν οι ψηφιακές πλατφόρμες που χρησιμοποιούνται στο σχολείο πληρούν τα πρότυπα προσβασιμότητας. Βεβαιωθείτε ότι οι μηχανισμοί αναφοράς είναι προσβάσιμοι σε μαθητές που επικοινωνούν με διαφορετικούς τρόπους. Συνεργαστείτε με το προσωπικό που ασχολείται με τις ειδικές εκπαιδευτικές ανάγκες προκειμένου να εντοπίσετε τους μαθητές που ενδέχεται να χρειάζονται επιπλέον υποστήριξη στην κατανόηση και τη διαχείριση των διαδικτυακών κινδύνων.
Αναγνώριση και αντιμετώπιση του ψηφιακού χάσματος	Οι μαθητές που προέρχονται από οικογένειες με χαμηλό εισόδημα ενδέχεται να έχουν περιορισμένη ή ασταθή πρόσβαση στο διαδίκτυο στο σπίτι, παλαιότερες ή κοινόχρηστες συσκευές, καθώς και λιγότερη υποστήριξη από ενήλικες όσον αφορά την πλοήγησή τους στον διαδικτυακό κόσμο. Οι μαθητές που χρησιμοποιούν κοινόχρηστες συσκευές αντιμετωπίζουν μεγαλύτερους κινδύνους όσον αφορά την προστασία της ιδιωτικής τους ζωής. Αυτοί οι μαθητές ενδέχεται επίσης να είναι λιγότερο πιθανό να αναγνωρίσουν ή να αναφέρουν προβλήματα.	Μην σχεδιάζετε ψηφιακές δραστηριότητες ή πρακτικές επικοινωνίας που προϋποθέτουν ένα επίπεδο σύνδεσης στο σπίτι το οποίο δεν διαθέτουν όλοι οι μαθητές. Λάβετε υπόψη ότι οι μαθητές που χρησιμοποιούν συσκευές κοινής χρήσης αντιμετωπίζουν συγκεκριμένους κινδύνους όσον αφορά την προστασία της ιδιωτικής ζωής και παρέχετε συγκεκριμένες οδηγίες. Βεβαιωθείτε ότι η εκπαίδευση σε θέματα ψηφιακής ασφάλειας φτάνει σε όλους τους μαθητές. Εντοπίστε τους μαθητές που δεν διαθέτουν επαρκή σύνδεση στο σπίτι και αντιμετωπίστε το ζήτημα αυτό μέσω των διαθέσιμων εθνικών προγραμμάτων.
Να βοηθήσετε τους μαθητές να αναπτύξουν κριτική συνείδηση σχετικά με την εικόνα του σώματος στο διαδίκτυο	Τα μέσα κοινωνικής δικτύωσης εκθέτουν συνεχώς τους μαθητές σε επεξεργασμένες και φιλτραρισμένες εικόνες που θέτουν πρότυπα εμφάνισης τα οποία δεν είναι ρεαλιστικά. Αυτό συνδέεται με χαμηλή αυτοεκτίμηση και άγχος, ιδίως στις έφηβες, και σε ορισμένες περιπτώσεις με διατροφικές διαταραχές.	Εντάξτε την εκπαίδευση σχετικά με την εικόνα του σώματος και την παρουσία στο διαδίκτυο στο πρόγραμμα σπουδών για την ψηφιακή ευημερία. Διδάξτε στους μαθητές πώς επεξεργάζονται και φιλτράρονται οι εικόνες πριν από τη δημοσίευσή τους και βοηθήστε τους να κατανοήσουν ότι αυτό που βλέπουν στο διαδίκτυο αποτελεί μια «παράσταση» και όχι την πραγματικότητα. Συζητήστε πώς οι αλγόριθμοι των πλατφορμών ενισχύουν το περιεχόμενο που

	Τι να κάνετε	Γιατί έχει σημασία	Πώς να το κάνετε
			βασίζεται στην εμφάνιση. Προσεγγίστε αυτό το θέμα με ευαισθησία. Ορισμένοι μαθητές ενδέχεται να αντιμετωπίζουν ήδη δυσκολίες. Βεβαιωθείτε ότι υπάρχουν διαθέσιμες διαδρομές παραπομπής προς εξειδικευμένη υποστήριξη.
Μέρος 4: Τι δείχνουν τα στοιχεία Αυτό το μέρος συνοψίζει τα	Να εξετάσετε όλη αυτή την πολιτική από μια οπτική που προάγει την ένταξη	Μια πολιτική που έχει σχεδιαστεί χωρίς να λαμβάνονται υπόψη οι εμπειρίες των διαφόρων ομάδων μαθητών θα αντικατοπτρίζει την εμπειρία της πλειοψηφίας και θα αφήνει τους άλλους λιγότερο προστατευμένους. Οι μαθητές που αντιμετωπίζουν τους μεγαλύτερους κινδύνους στο διαδίκτυο είναι συχνά εκείνοι των οποίων οι εμπειρίες έχουν ληφθεί λιγότερο υπόψη.	Εξετάστε κάθε ενότητα της παρούσας πολιτικής και αναρωτηθείτε απευθύνεται αυτή στους μαθητές που διατρέχουν τον μεγαλύτερο κίνδυνο Είναι οι διαδρομές αναφοράς μας προσβάσιμες σε όλους; Καλύπτει η εκπαίδευση του προσωπικού μας τις συγκεκριμένες ευπάθειες των διαφόρων ομάδων; Εμπλέξτε τους μαθητές, συμπεριλαμβανομένων εκείνων που ανήκουν σε υποεκπροσωπούμενες ομάδες, στην αναθεώρηση και τη βελτίωση της προσέγγισης του σχολείου όσον αφορά την ψηφιακή ασφάλεια.

συμπεράσματα της έρευνας σχετικά με το τι αποδίδει πραγματικά όταν τα σχολεία αντιμετωπίζουν θέματα κυβερνοασφάλειας, διαδικτυακού εκφοβισμού και ψηφιακής ευημερίας. Χρησιμοποιήστε αυτή την ενότητα για να λάβετε τεκμηριωμένες αποφάσεις σχετικά με τα προγράμματα, τις προσεγγίσεις και τις παρεμβάσεις που υιοθετεί το σχολείο σας.

4.1 Ευαισθητοποίηση και εκπαίδευση σε θέματα κυβερνοασφάλειας

Η έρευνα για την κυβερνοασφάλεια στα σχολεία επισημαίνει σταθερά την ανθρώπινη συμπεριφορά ως τον σημαντικότερο παράγοντα κινδύνου. Οι περισσότερες επιτυχημένες επιθέσεις ξεκινούν με ένα ηλεκτρονικό μήνυμα phishing ή έναν αδύναμο κωδικό πρόσβασης. Τα τεχνικά μέτρα προστασίας βοηθούν, αλλά δεν μπορούν να αποτρέψουν μια επίθεση όταν το προσωπικό δεν έχει εκπαιδευτεί να αναγνωρίζει την απειλή. Αυτό σημαίνει ότι η επένδυση στην εκπαίδευση του προσωπικού είναι τουλάχιστον εξίσου σημαντική με την επένδυση σε τεχνικά εργαλεία.

Μελέτες σχετικά με την εκπαίδευση του προσωπικού στον τομέα της κυβερνοασφάλειας δείχνουν ότι η τακτική, πρακτική εκπαίδευση αποδίδει σημαντικά καλύτερα από μια μεμονωμένη συνεδρία ευαισθητοποίησης. Το προσωπικό που λαμβάνει ετήσια εκπαίδευση και περιστασιακές υπενθυμίσεις είναι αισθητά λιγότερο πιθανό να κάνει κλικ σε συνδέσμους ηλεκτρονικού ψαρέματος ή να ακολουθεί μη ασφαλείς πρακτικές κατά τη χρήση των σχολικών συστημάτων. Ο τρόπος διεξαγωγής της εκπαίδευσης έχει επίσης σημασία: οι διαδραστικές συνεδρίες με παραδείγματα από την πραγματική ζωή αποδίδουν καλύτερα από την παθητική ανάγνωση πληροφοριών ή την παρακολούθηση ενός βίντεο.

Οι προσομοιώσεις phishing, όπου το προσωπικό λαμβάνει ένα προσεκτικά σχεδιασμένο ψεύτικο email phishing για να δοκιμαστεί ο τρόπος αντίδρασής του, συγκαταλέγονται μεταξύ των πιο αποτελεσματικών μεθόδων εκπαίδευσης που υπάρχουν. Τα σχολεία και οι οργανισμοί που διεξάγουν τακτικά αυτές τις ασκήσεις παρατηρούν σαφείς βελτιώσεις στη συμπεριφορά του προσωπικού με την πάροδο του χρόνου. Η άσκηση είναι πιο αποτελεσματική όταν ακολουθείται αμέσως από ανατροφοδότηση που εξηγεί ποια ήταν τα σημάδια και ποια θα ήταν η σωστή αντίδραση.

Όσον αφορά τους μαθητές, τα στοιχεία δείχνουν ότι η εκπαίδευση στην κυβερνοασφάλεια αποδίδει καλύτερα όταν ενσωματώνεται στο πρόγραμμα σπουδών και όχι όταν παρέχεται ως μεμονωμένη δραστηριότητα. Οι μαθητές που μαθαίνουν για την ασφάλεια στο διαδίκτυο μέσω πραγματικών παραδειγμάτων, διαδραστικών δραστηριοτήτων και συζήτησης με τους συμμαθητές τους αφομοιώνουν καλύτερα τα μαθήματα και τα εφαρμόζουν με μεγαλύτερη συνέπεια στη ζωή τους σε σύγκριση με τους μαθητές που λαμβάνουν τις ίδιες πληροφορίες σε μια διάλεξη.

4.2 Πρόληψη του διαδικτυακού εκφοβισμού

Η έρευνα σχετικά με την πρόληψη του διαδικτυακού εκφοβισμού δείχνει σταθερά ότι οι προσεγγίσεις που εμπλέκουν ολόκληρο το σχολείο αποδίδουν καλύτερα. Αυτό σημαίνει προγράμματα που φέρνουν σε επαφή μαθητές, εκπαιδευτικούς, γονείς και τη σχολική διοίκηση γύρω από έναν κοινό στόχο: τη δημιουργία ενός ασφαλέστερου περιβάλλοντος. Τα σχολεία που αντιμετωπίζουν τον διαδικτυακό εκφοβισμό αποκλειστικά ως πειθαρχικό ζήτημα, το οποίο πρέπει να αντιμετωπιστεί μετά την εμφάνιση των περιστατικών, έχουν σταθερά χειρότερα αποτελέσματα από τα σχολεία που υιοθετούν μια προσέγγιση πρόληψης που εμπλέκει ολόκληρη τη σχολική κοινότητα.

Τα προγράμματα που εστιάζουν αποκλειστικά στη συμπεριφορά των θυτών είναι λιγότερο αποτελεσματικά από εκείνα που καλλιεργούν επίσης την ενσυναίσθηση και τις δεξιότητες των παρευρισκόμενων. Οι μαθητές που κατανοούν τη βλάβη που προκαλεί ο διαδικτυακός εκφοβισμός και στους οποίους έχει διδαχθεί πώς να υποστηρίξουν έναν συμμαθητή που αποτελεί στόχο εκφοβισμού είναι πιο πιθανό να αναφέρουν περιστατικά και να παρέμβουν για να βοηθήσουν. Το αν οι παρευρισκόμενοι παρεμβαίνουν ή παραμένουν σιωπηλοί αποτελεί έναν από τους ισχυρότερους παράγοντες πρόβλεψης του αν ο εκφοβισμός θα κλιμακωθεί ή θα σταματήσει.

Τα συστήματα ανώνυμης αναφοράς οδηγούν σταθερά σε αύξηση του αριθμού των περιστατικών που αναφέρονται. Οι μαθητές που υφίστανται διαδικτυακό εκφοβισμό συχνά δεν το λένε σε κανέναν, επειδή φοβούνται ότι δεν θα τους πιστέψουν, ότι η κατάσταση θα επιδεινωθεί ή ότι θα υποστούν κοινωνικές συνέπειες από τους συμμαθητές τους. Τα σχολεία που προσφέρουν έναν πραγματικά εμπιστευτικό και αξιόπιστο τρόπο αναφοράς σημειώνουν υψηλότερα ποσοστά αποκάλυψης των περιστατικών και ταχύτερη παρέμβαση.

Η κατάρτιση των εκπαιδευτικών είναι απαραίτητη και συχνά υποτιμάται. Έρευνες δείχνουν ότι πολλοί εκπαιδευτικοί αισθάνονται αβεβαιότητα ως προς τον τρόπο αντιμετώπισης του διαδικτυακού εκφοβισμού, ιδίως όταν αυτός αφορά εφαρμογές ή λειτουργίες με τις οποίες δεν είναι εξοικειωμένοι. Τα σχολεία που επενδύουν σε πρακτική και δομημένη κατάρτιση των εκπαιδευτικών σχετικά με την αναγνώριση και την αντιμετώπιση του διαδικτυακού εκφοβισμού σημειώνουν σταθερά καλύτερα αποτελέσματα για τους μαθητές.

Η συμμετοχή των γονέων επίσης κάνει σταθερά τη διαφορά. Οι γονείς που κατανοούν το διαδικτυακό εκφοβισμό, που γνωρίζουν πώς λειτουργούν οι πλατφόρμες που χρησιμοποιούν τα παιδιά τους και που αισθάνονται συνδεδεμένοι με την προσέγγιση του σχολείου, είναι πιο αποτελεσματικοί τόσο στην υποστήριξη των παιδιών τους όσο και στην ενίσχυση των μηνυμάτων του σχολείου στο σπίτι.

Η έρευνα παρέχει σαφή στοιχεία για την έκταση του προβλήματος. Σύμφωνα με τη μελέτη του Παγκόσμιου Οργανισμού Υγείας (ΠΟΥ) «Health Behaviour in School-aged Children» (2024), περίπου ένας στους έξι εφήβους στην Ευρώπη, δηλαδή περίπου το 15%, αναφέρει ότι έχει υποστεί διαδικτυακό εκφοβισμό, με τα ποσοστά να είναι γενικά παρόμοια μεταξύ αγοριών και κοριτσιών και να παρουσιάζουν ανοδική τάση σε σύγκριση με το 2018. Σύμφωνα με στοιχεία του Οργανισμού Οικονομικής Συνεργασίας και Ανάπτυξης (ΟΟΣΑ), παρατηρούνται διακυμάνσεις μεταξύ των χωρών που κυμαίνονται από περίπου 7,5% έως 27,1%. Τα στοιχεία των γραμμών βοήθειας του δικτύου Insafe της ΕΕ κατατάσσουν σταθερά τον διαδικτυακό εκφοβισμό μεταξύ των πιο συνηθισμένων λόγων για τους οποίους τα παιδιά και οι έφηβοι επικοινωνούν με τις υπηρεσίες υποστήριξης, ενώ το 4ο τρίμηνο του 2025 ήταν και πάλι το πιο συχνό ζήτημα που τέθηκε.

Όταν ερωτήθηκαν από την Ευρωπαϊκή Επιτροπή το 2025, πάνω από 6.000 παιδιά και έφηβοι ηλικίας 12 έως 17 ετών σε ολόκληρη την ΕΕ εξέφρασαν σαφείς προσδοκίες από τα σχολεία: η πλειοψηφία επιθυμούσε ρητούς κανόνες και συνέπειες για τον διαδικτυακό εκφοβισμό, άμεση διδασκαλία σχετικά με το θέμα και ψυχολογική υποστήριξη για τα θύματα. Τα κορίτσια ήταν σταθερά πιο πιθανό να ζητήσουν αυτά τα μέτρα σε σύγκριση με τα αγόρια.

Μια μετα-ανάλυση των Polanin et al. (2021), η οποία κάλυψε περισσότερους από 45.000 μαθητές, διαπίστωσε ότι τα ειδικά προγράμματα πρόληψης του διαδικτυακού εκφοβισμού οδήγησαν σε στατιστικά σημαντική μείωση τόσο της διάπραξης όσο και της θυματοποίησης, και ότι τα προγράμματα που σχεδιάστηκαν ειδικά για τον διαδικτυακό εκφοβισμό υπερέβησαν σε αποτελεσματικότητα τις γενικές προσεγγίσεις κατά του εκφοβισμού.

4.3 Ψηφιακή ευημερία

Η έρευνα σχετικά με τη χρήση της τεχνολογίας και την ψυχική υγεία των μαθητών δεν επιτρέπει την εξαγωγή απλών συμπερασμάτων. Δεν είναι επιβλαβής κάθε χρήση της τεχνολογίας. Η ενεργή χρήση της τεχνολογίας για δημιουργική εργασία, επικοινωνία ή μάθηση μπορεί να έχει θετικά αποτελέσματα. Το διαρκές πρόβλημα είναι η παθητική χρήση: η περιήγηση στα μέσα κοινωνικής δικτύωσης χωρίς σκοπό ή ουσιαστική αλληλεπίδραση. Αυτός ο τύπος χρήσης συνδέεται στενότερα με το άγχος, τη μοναξιά και τη χαμηλή αυτοεκτίμηση, με τα αποτελέσματα να είναι ιδιαίτερα έντονα στις έφηβες.

Τα στοιχεία υποστηρίζουν σαφώς την εκπαίδευση έναντι των περιορισμών. Τα σχολεία που επικεντρώνονται αποκλειστικά στον περιορισμό της πρόσβασης στην τεχνολογία, χωρίς να βοηθούν τους μαθητές να κατανοήσουν γιατί ορισμένα πρότυπα χρήσης είναι επιβλαβή ή να τους παρέχουν εργαλεία για τη διαχείριση της συμπεριφοράς τους, παρατηρούν λιγότερο διαρκείς αλλαγές. Οι μαθητές που κατανοούν το πρόβλημα και έχουν αναπτύξει τις δικές τους στρατηγικές παρουσιάζουν πιο σταθερές βελτιώσεις στην ευημερία τους.

Προγράμματα που διδάσκουν στους μαθητές να σκέφτονται κριτικά σχετικά με τις ψηφιακές τους συνήθειες, να κατανοούν πώς οι πλατφόρμες κοινωνικών μέσων έχουν σχεδιαστεί για να μεγιστοποιούν την εμπλοκή των χρηστών και να αναγνωρίζουν το χάσμα μεταξύ των επιμελημένων εικόνων στο διαδίκτυο και της πραγματικότητας έχουν δείξει θετικά αποτελέσματα στη μείωση του άγχους και στη βελτίωση της αυτοεκτίμησης, όπως αποδεικνύεται από πολλές

μελέτες. Αυτά τα προγράμματα αποδίδουν καλύτερα όταν υλοποιούνται σε βάθος χρόνου ως μέρος του προγράμματος σπουδών, παρά ως μεμονωμένη δραστηριότητα.

Η συμμετοχή των μαθητών στη διαμόρφωση των σχολικών ψηφιακών κανόνων αυξάνει σταθερά τόσο το βαθμό συμμόρφωσής τους όσο και το αίσθημα ότι οι κανόνες αυτοί τους ανήκουν. Οι μαθητές που θεωρούν ότι οι κανόνες είναι δίκαιοι και ότι είχαν λόγο στη διαμόρφωσή τους είναι πιο πιθανό να τους τηρούν και να ενθαρρύνουν τους συμμαθητές τους να κάνουν το ίδιο.

Ένα ιδιαίτερα σημαντικό εύρημα αφορά το «Fear of Missing Out» (FOMO). Η έρευνα αντιλαμβάνεται όλο και περισσότερο το FOMO όχι ως μια παροδική διάθεση, αλλά ως ένα σχετικά σταθερό ψυχολογικό χαρακτηριστικό, ένα επίμονο άγχος για το ενδεχόμενο να χάσουν ικανοποιητικές εμπειρίες που βιώνουν οι άλλοι. Μελέτες συνδέουν το FOMO με συμπτώματα κατάθλιψης, διαταραχές ύπνου και καταναγκαστική συμπεριφορά ελέγχου. Μια συστηματική ανασκόπηση και μετα-ανάλυση του 2025 επιβεβαίωσε μια σταθερή στατιστική συσχέτιση μεταξύ της εξάρτησης από τα μέσα κοινωνικής δικτύωσης και των υψηλότερων επιπέδων άγχους, κατάθλιψης, μοναξιάς και χαμηλότερης αυτοεκτίμησης, με το FOMO να αναγνωρίζεται συχνά ως μεσολαβητικός παράγοντας. Τα σχολεία θα πρέπει να αντιμετωπίζουν ρητά το FOMO και τα μοτίβα καταναγκαστικής χρήσης στο πλαίσιο δραστηριοτήτων που απευθύνονται στους μαθητές, και όχι μόνο μέσω γενικών μηνυμάτων σχετικά με τον χρόνο χρήσης των οθονών.

Η έρευνα επισημαίνει επίσης ότι τα αποτελέσματα εξαρτώνται σε μεγάλο βαθμό όχι μόνο από το πόσο συχνά χρησιμοποιούν οι μαθητές τις ψηφιακές πλατφόρμες, αλλά και από τον τρόπο με τον οποίο τις χρησιμοποιούν. Τα μέσα κοινωνικής δικτύωσης μπορούν να λειτουργήσουν ως πηγή υποστήριξης για ορισμένους μαθητές, ιδίως για εκείνους που είναι απομονωμένοι ή ανήκουν σε μειονοτικές ομάδες. Οι προσεγγίσεις πρόληψης θα πρέπει να βοηθούν τους μαθητές να αναπτύξουν μια πιο συνειδητή και σκόπιμη σχέση με την τεχνολογία.

Η έγκαιρη αναγνώριση και παραπομπή είναι σημαντικές. Οι μαθητές που συνδέονται με την κατάλληλη υποστήριξη πριν οι δυσκολίες τους γίνουν σοβαρές παρουσιάζουν σημαντικά καλύτερα αποτελέσματα από εκείνους που εντοπίζονται μόνο όταν τα προβλήματα είναι ήδη ορατά μέσω της πτώσης των βαθμών ή σοβαρών αλλαγών στη συμπεριφορά. Τα σχολεία που διαθέτουν σαφείς και ευρέως γνωστές διαδικασίες για τον εντοπισμό και την υποστήριξη των μαθητών που αντιμετωπίζουν δυσκολίες βρίσκονται σε πολύ καλύτερη θέση να τους βοηθήσουν.

Παράρτημα Ι: Πίνακας εθνικών αναφορών

Χρησιμοποιήστε αυτόν τον πίνακα για να βρείτε τις βασικές εθνικές παραμέτρους για τη χώρα σας. Όπου η παρούσα πολιτική αναφέρει ότι πρέπει να ανατρέξετε στους εθνικούς κανόνες, εδώ είναι το σημείο που πρέπει να ανατρέξετε.

Παράμετρος	Ελλάδα	Ιταλία	Πορτογαλία	Ρουμανία	Σλοβακία

Ηλικία ψηφιακής συναίνεσης	15 χρόνια	14 χρόνια	13 χρόνια	16 χρόνια	16 χρόνια
Αρχή προστασίας δεδομένων	HDPA dpa.gr	Garante garanteprivacy.it	CNPD cnpd.pt	ANSPDCP dataprotection.ro	UOOU dataprotection.gov.sk
Αρχή Κυβερνοασφάλειας	EAKE cyber.gov.gr	ACN acn.gov.it	CNCS cncs.gov.pt	DNSC dnsc.ro	NBU nbu.gov.sk
Αναφορά περιστατικών στον κυβερνοχώρο	EAKE	ACN	CERT.PT (24h for NIS2)	DNSC/PNRISC (24h)	NBU/SK-CERT
Αναφορά περιστατικών παραβίασης δεδομένων	HDPA, 72 ώρες	Garante, 72 ώρες	CNPD, 72 ώρες	ANSPDCP, 72 ώρες	UOOU, 72 ώρες
Πληροφορίες για τον διαδικτυακό εκφοβισμό	stop-bullying.gov.gr	Αναφορά στο σχολείο ή στην αστυνομία	seguranet.pt	School or ANSPDCP	Κατευθυντήρια οδηγία 1/2025
Νόμος περί κινητών τηλεφώνων	Αυστηρή απαγόρευση 2018/2024	Όλοι οι κύκλοι 2024/25	Τάξεις 1-6 από τον Σεπτέμβριο του 2025	Κατά τη διάρκεια του μαθήματος, Νόμος 198/2023	Όλες οι βαθμίδες από τον Ιανουάριο του 2025
Κατευθυντήριες οδηγίες για τη χρήση της τεχνητής νοημοσύνης στα σχολεία	Μόνο ο νόμος της ΕΕ για την Τεχνητή Νοημοσύνη	Υπουργική Απόφαση 166/2025	Δεν έχει εκδοθεί ακόμα	Δεν έχει εκδοθεί ακόμα	Σχέδιο για την Τεχνητή Νοημοσύνη 2025-2027

Παράρτημα II: Πρότυπο επιστολής προς τους γονείς

Τα σχολεία μπορούν να προσαρμόσουν την παρούσα επιστολή για να ενημερώσουν τους γονείς σχετικά με τον τρόπο με τον οποίο το σχολείο διαχειρίζεται τα δεδομένα των μαθητών και τα μέτρα που λαμβάνει για την ασφάλεια των μαθητών στο διαδίκτυο. Αποστείλετέ την κατά την εγγραφή και

κάθε φορά που πραγματοποιούνται σημαντικές αλλαγές στα ψηφιακά συστήματα ή στις πολιτικές του σχολείου.

[Όνομα και διεύθυνση σχολείου]

[Ημερομηνία]

Αγαπητοί γονείς / κηδεμόνες,

Πώς προστατεύουμε τα δεδομένα του παιδιού σας και υποστηρίζουμε την ψηφιακή του ασφάλεια

Σας γράφουμε για να σας ενημερώσουμε σχετικά με τον τρόπο με τον οποίο το σχολείο μας διαχειρίζεται τα προσωπικά δεδομένα των μαθητών και τα μέτρα που λαμβάνουμε για τη διασφάλιση της ασφάλειας του παιδιού σας στο ψηφιακό μαθησιακό περιβάλλον.

Ποια δεδομένα συλλέγουμε και για ποιο λόγο. Συλλέγουμε προσωπικές πληροφορίες σχετικά με το παιδί σας που είναι απαραίτητες για εκπαιδευτικούς και διοικητικούς σκοπούς. Αυτές περιλαμβάνουν το όνομά του, τον αριθμό ταυτότητάς του, τα αρχεία παρουσίας και τους βαθμούς του. Σε ορισμένες περιπτώσεις, ενδέχεται επίσης να διατηρούμε πληροφορίες που σχετίζονται με την υγεία του, όταν αυτές είναι σχετικές με την εκπαίδευσή του. Συλλέγουμε μόνο τα στοιχεία που χρειαζόμαστε και τα διατηρούμε για όσο χρονικό διάστημα απαιτεί ο νόμος.

Ποιος έχει πρόσβαση σε αυτά. Η πρόσβαση στα προσωπικά δεδομένα του παιδιού σας περιορίζεται σε εξουσιοδοτημένα μέλη του προσωπικού που τα χρειάζονται για την εκτέλεση των καθηκόντων τους. Δεν κοινοποιούμε δεδομένα σε τρίτους, εκτός εάν αυτό απαιτείται από το νόμο ή έχετε δώσει τη ρητή συγκατάθεσή σας.

Ψηφιακές πλατφόρμες. Το σχολείο μας χρησιμοποιεί ψηφιακές πλατφόρμες για διδακτικούς και διοικητικούς σκοπούς. Πριν υιοθετήσουμε οποιαδήποτε πλατφόρμα, ελέγχουμε αν συμμορφώνεται με τον Γενικό Κανονισμό για την Προστασία Δεδομένων (GDPR). Το παιδί σας θα έχει πρόσβαση σε αυτές τις πλατφόρμες μέσω ενός λογαριασμού που θα του χορηγήσει το σχολείο. Μπορείτε να προμηθευτείτε έναν κατάλογο με τις πλατφόρμες που χρησιμοποιούμε επί του παρόντος από τη γραμματεία του σχολείου.

Η συγκατάθεσή σας. Για μαθητές ηλικίας κάτω των [εισαγάγετε την εθνική ηλικία ψηφιακής συγκατάθεσης], χρειαζόμαστε γραπτή γονική συγκατάθεση προτού μπορέσουμε να εγγράψουμε το παιδί σας σε μια ψηφιακή πλατφόρμα. Θα σας ζητηθεί να τη δώσετε κατά την εγγραφή και κάθε φορά που εισάγεται μια νέα πλατφόρμα.

Κυβερνοεκφοβισμός. Το σχολείο μας διαθέτει σαφείς διαδικασίες για την πρόληψη και την αντιμετώπιση του κυβερνοεκφοβισμού. Εάν το παιδί σας υποστεί ή γίνει μάρτυρας κυβερνοεκφοβισμού, παρακαλούμε να το ενθαρρύνετε να μιλήσει σε έναν ενήλικα της εμπιστοσύνης του στο σχολείο ή να επικοινωνήσει απευθείας μαζί μας στα [στοιχεία επικοινωνίας].

Τα δικαιώματά σας. Έχετε το δικαίωμα να δείτε τα δεδομένα που διατηρούμε για το παιδί σας, να ζητήσετε διορθώσεις και, σε ορισμένες περιπτώσεις, να ζητήσετε τη διαγραφή τους. Για να το κάνετε αυτό, παρακαλούμε επικοινωνήστε με τον Υπεύθυνο Προστασίας Δεδομένων μας στα [στοιχεία επικοινωνίας του ΥΠΔ].

Υποστήριξη της ψηφιακής ευημερίας στο σπίτι. Σας ενθαρρύνουμε να συζητάτε τακτικά με το παιδί σας για τις διαδικτυακές του εμπειρίες, χωρίς να το κρίνετε. Εάν το παιδί σας φαίνεται αναστατωμένο ή ασυνήθιστα ανήσυχο σχετικά με το κινητό του ή τις διαδικτυακές του αλληλεπιδράσεις, παρακαλούμε επικοινωνήστε με [τον σχολικό σύμβουλο / τον αρμόδιο υπεύθυνο]. Στη χώρα σας υπάρχουν επίσης εθνικές γραμμές βοήθειας για παιδιά και νέους.

Εάν έχετε οποιεσδήποτε ερωτήσεις, μην διστάσετε να επικοινωνήσετε μαζί μας.

Με εκτίμηση,

[Όνομα Διευθυντή και Σχολείο]

Παράρτημα III: Πρότυπο Πολιτικής Αποδεκτής Χρήσης

Προσαρμόστε αυτό το πρότυπο για να δημιουργήσετε τη δική σας Πολιτική Αποδεκτής Χρήσης για το σχολείο σας. Θα πρέπει να υπογράφεται από τους μαθητές, τους γονείς ή κηδεμόνες και το προσωπικό στην αρχή κάθε σχολικού έτους. Προσαρμόστε το ώστε να αντανακλά τα συστήματα του σχολείου σας, τους εθνικούς κανόνες και το συγκεκριμένο πλαίσιο.

Πολιτική Αποδεκτής Χρήσης

[Όνομα Σχολείου] | Σχολικό Έτος [XXXX-XXXX]

1. Σκοπός

Η παρούσα πολιτική καθορίζει τους κανόνες χρήσης των ψηφιακών συσκευών, του διαδικτύου και των ψηφιακών πλατφορμών στο σχολείο μας. Ισχύει για όλους τους μαθητές, το προσωπικό και τους επισκέπτες που χρησιμοποιούν τα συστήματα του σχολείου. Υπογράφοντας την παρούσα πολιτική, επιβεβαιώνετε ότι έχετε διαβάσει και κατανοήσει τους παρόντες κανόνες και συμφωνείτε να τους τηρείτε.

2. Για ποιους σκοπούς μπορείτε να χρησιμοποιείτε τους ψηφιακούς πόρους του σχολείου

- Την ολοκλήρωση σχολικών εργασιών και εκπαιδευτικών δραστηριοτήτων
- Την επικοινωνία με καθηγητές και συμμαθητές για σχολικούς σκοπούς
- Τη χρήση πλατφορμών που έχουν εγκριθεί από το σχολείο
- Εκπαιδευτικές δραστηριότητες που έχει εξουσιοδοτήσει ρητά ένας καθηγητής

3. Τι δεν πρέπει να κάνετε

- Να έχετε πρόσβαση, να δημιουργείτε ή να μοιράζεστε περιεχόμενο που είναι παράνομο, επιβλαβές, προσβλητικό ή διακριτικό
- Να εκφοβίζετε, να παρενοχλείτε, να απειλείτε ή να ταπεινώνετε άλλους μαθητές ή μέλη του προσωπικού μέσω ψηφιακών μέσων
- Να μοιράζεστε προσωπικές πληροφορίες σχετικά με άλλους μαθητές ή μέλη του προσωπικού χωρίς τη συγκατάθεσή τους
- Να καταγράφετε βίντεο ή ήχο από μαθητές, καθηγητές ή μέλη του προσωπικού χωρίς τη ρητή συγκατάθεσή τους
- Να χρησιμοποιείτε τον λογαριασμό άλλου ατόμου ή να κοινοποιείτε τα στοιχεία σύνδεσής σας
- Να εγκαθιστάτε λογισμικό ή εφαρμογές σε συσκευές του σχολείου χωρίς άδεια
- Να χρησιμοποιείτε προσωπικούς λογαριασμούς σε μη εγκεκριμένες πλατφόρμες για σχολικές δραστηριότητες

4. Κινητά τηλέφωνα

[Περιγράψτε εδώ τους κανόνες του σχολείου σας σχετικά με τα κινητά τηλέφωνα, σύμφωνα με την εθνική νομοθεσία της χώρας σας, όπως περιγράφεται στο Μέρος 2 της παρούσας πολιτικής. Αναφέρετε πού πρέπει να φυλάσσονται τα τηλέφωνα, ποιες εξαιρέσεις ισχύουν και τι συμβαίνει σε περίπτωση παράβασης των κανόνων.]

5. Μέσα κοινωνικής δικτύωσης

Οι μαθητές δεν πρέπει να δημοσιεύουν περιεχόμενο σχετικά με το σχολείο, άλλους μαθητές ή το προσωπικό που είναι επιβλαβές, παραπλανητικό ή που θα μπορούσε να βλάψει τη φήμη οποιουδήποτε. Η συμπεριφορά στο διαδίκτυο που συνιστά διαδικτυακό εκφοβισμό, είτε εντός είτε εκτός των σχολικών ωρών, καλύπτεται από την παρούσα πολιτική και από τις διαδικασίες του σχολείου κατά του εκφοβισμού.

6. Αναφορά

Εάν εντοπίσετε περιεχόμενο που κάνει εσάς ή κάποιον άλλο μαθητή να αισθάνεστε ανασφαλείς, ή εάν διαπιστώσετε παραβίαση της παρούσας πολιτικής, αναφέρετέ το σε έναν ενήλικα εμπιστοσύνης στο σχολείο ή στο [σημείο επικοινωνίας για αναφορές].

7. Συνέπειες

Η παραβίαση της παρούσας πολιτικής μπορεί να έχει ως αποτέλεσμα την αναστολή της πρόσβασης στα σχολικά συστήματα, τη λήψη άλλων πειθαρχικών μέτρων σύμφωνα με τους πειθαρχικούς κανόνες του σχολείου και, σε σοβαρές περιπτώσεις, την παραπομπή στις αρμόδιες αρχές επιβολής του νόμου.

Πλήρες όνομα φοιτητή	
Υπογραφή φοιτητή	
Όνομα γονέα ή κηδεμόνα	
Υπογραφή γονέα ή κηδεμόνα	
Ημερομηνία	

Παράρτημα IV: Διαδικασία αντιμετώπισης συμβάντων στον κυβερνοχώρο

Ακολουθήστε τα παρακάτω βήματα κάθε φορά που συμβαίνει κάτι στον κυβερνοχώρο στο σχολείο σας. Ως συμβάν στον κυβερνοχώρο ορίζεται κάθε περιστατικό που θέτει σε κίνδυνο την ασφάλεια, τη διαθεσιμότητα ή την εμπιστευτικότητα των δεδομένων ή των συστημάτων του σχολείου. Σε αυτά περιλαμβάνονται επιθέσεις με λογισμικό εκβιασμού (ransomware), η μη εξουσιοδοτημένη πρόσβαση στα συστήματα του σχολείου ή η παραβίαση προσωπικών δεδομένων.

Βήμα 1: Εντοπισμός και περιορισμός

Μόλις κάποιος εντοπίσει ένα περιστατικό, πρέπει να ενημερώσει αμέσως τον συντονιστή πληροφορικής ή τον διευθυντή του σχολείου. Μην προσπαθήσετε να επιλύσετε το πρόβλημα

μόνοι σας. Αποσυνδέστε τη συσκευή που έχει επηρεαστεί από το δίκτυο, αποσυνδέοντας το καλώδιο ή απενεργοποιώντας το Wi-Fi. Μην απενεργοποιήσετε τη συσκευή, εκτός εάν σας ζητηθεί ρητά να το κάνετε, καθώς αυτό μπορεί να καταστρέψει αποδεικτικά στοιχεία. Καταγράψτε την ώρα και μια περιγραφή του τι παρατηρήσατε.

Βήμα 2: Αξιολόγηση

Ο συντονιστής πληροφορικής και ο υπεύθυνος προστασίας δεδομένων (DPO) πρέπει να αξιολογήσουν από κοινού το περιστατικό. Προσδιορίστε ποια συστήματα, λογαριασμοί ή δεδομένα έχουν επηρεαστεί. Διαπιστώστε εάν τα προσωπικά δεδομένα έχουν ή ενδέχεται να έχουν παραβιαστεί. Ελέγξτε εάν το περιστατικό εξακολουθεί να βρίσκεται σε εξέλιξη ή έχει περιοριστεί.

Βήμα 3: Ενημέρωση

Αν έχει συμβεί αυτό...	Θα πρέπει να...
Τα προσωπικά δεδομένα έχουν παραβιαστεί ή ενδέχεται να έχουν παραβιαστεί	Ενημερώστε την εθνική αρχή προστασίας δεδομένων εντός 72 ωρών. Ανατρέξτε στο Μέρος 2 για να βρείτε την αρμόδια αρχή στη χώρα σας.
Έχει σημειωθεί ένα σοβαρό περιστατικό στον τομέα της κυβερνοασφάλειας	Ενημερώστε την εθνική αρχή για την κυβερνοασφάλεια. Στην Πορτογαλία, για τους φορείς που εμπίπτουν στο πεδίο εφαρμογής της οδηγίας NIS2, η ενημέρωση αυτή πρέπει να πραγματοποιηθεί εντός 24 ωρών. Ανατρέξτε στο Μέρος 2 για να βρείτε την αρμόδια αρχή της χώρας σας.
Εμπλέκεται εγκληματική δραστηριότητα	Επικοινωνήστε με την αστυνομία.
Οι φοιτητές ή το προσωπικό διατρέχουν άμεσο κίνδυνο ή έχουν υποστεί άμεση βλάβη	Παρέχετε άμεση υποστήριξη και ενημερώστε τους γονείς ή τους κηδεμόνες, ανάλογα με την περίπτωση.

Βήμα 4: Αποκατάσταση

Επαναφέρετε τα συστήματα από αντίγραφα ασφαλείας, όπου υπάρχουν. Αλλάξτε αμέσως όλους τους κωδικούς πρόσβασης και τα διαπιστευτήρια πρόσβασης που έχουν επηρεαστεί. Εγκαταστήστε τυχόν σχετικές ενημερώσεις ασφαλείας πριν θέσετε τα συστήματα ξανά σε λειτουργία. Βεβαιωθείτε ότι τα συστήματα που έχουν αποκατασταθεί λειτουργούν σωστά πριν τα διαθέσετε ξανά στους φοιτητές και το προσωπικό.

Βήμα 4α: Υποστήριξη των ατόμων που έχουν πληγεί

Παρέχετε άμεση ψυχολογική και πρακτική υποστήριξη σε κάθε μαθητή ή μέλος του προσωπικού που έχει πληγεί άμεσα από το περιστατικό. Αυτό πρέπει να γίνεται παράλληλα με την τεχνική αντιμετώπιση, όχι μετά από αυτήν. Επικοινωνήστε χωρίς καθυστέρηση με τον σχολικό σύμβουλο ή την ομάδα ψυχολογικής υποστήριξης. Ακολουθήστε το πρωτόκολλο ψυχολογικής υποστήριξης του σχολείου.

Βήμα 5: Ανασκόπηση

Μόλις επιλυθεί το περιστατικό, πραγματοποιήστε μια πλήρη ανασκόπηση. Καταγράψτε τι συνέβη, πώς συνέβη, τι έγινε και ποιο ήταν το αποτέλεσμα. Προσδιορίστε ποιες αλλαγές θα μείωναν τον κίνδυνο να επαναληφθεί το περιστατικό. Ενημερώστε το αρμόδιο προσωπικό για τα ευρήματα, ειδικά αν το περιστατικό αφορούσε ένα ηλεκτρονικό μήνυμα phishing ή ανθρώπινο λάθος. Ενημερώστε τη διαδικασία αντιμετώπισης περιστατικών, αν χρειαστεί.

Μητρώο συμβάντων

Ημερομηνία και ώρα του συμβάντος	
Πώς ανακαλύφθηκε και από ποιον;	
Τι συνέβη;	
Ποια συστήματα και δεδομένα επηρεάστηκαν;	
Άμεσες ενέργειες που αναλήφθηκαν	
Έχουν παραβιαστεί προσωπικά δεδομένα;	
Έχει ενημερωθεί η αρχή προστασίας δεδομένων; (Ημερομηνία)	
Ενημερώθηκε η αρμόδια αρχή για την κυβερνοασφάλεια; (Ημερομηνία)	
Ειδοποιήθηκε η αστυνομία; (Ημερομηνία)	
Μέτρα αποκατάστασης που ελήφθησαν	
Αποκατάσταση συστημάτων ημερομηνιών	
Ολοκληρώθηκε η αξιολόγηση; (Ημερομηνία)	
Αλλαγές που πραγματοποιήθηκαν ως αποτέλεσμα της επανεξέτασης	

Παράρτημα V: Πρότυπο εκτίμησης επιπτώσεων στην προστασία των δεδομένων (DPIA)

Απαιτείται η διενέργεια DPIA πριν το σχολείο σας εισαγάγει ένα νέο ψηφιακό σύστημα ή πλατφόρμα που περιλαμβάνει την επεξεργασία μεγάλου όγκου δεδομένων μαθητών, τη συστηματική παρακολούθηση των μαθητών, την αυτοματοποιημένη λήψη αποφάσεων που επηρεάζει τους μαθητές ή ευαίσθητες κατηγορίες δεδομένων. Εάν δεν είστε σίγουροι για το αν απαιτείται DPIA, ρωτήστε τον υπεύθυνο προστασίας δεδομένων (DPO) σας.

Μέρος Α: Τι θα υποβληθεί σε επεξεργασία

Όνομα του συστήματος ή της πλατφόρμας	
Πάροχος ή προμηθευτής	
Ποια προσωπικά δεδομένα θα υποβληθούν σε επεξεργασία;	
Ποιοι είναι τα υποκείμενα των δεδομένων; (μαθητές, προσωπικό, γονείς)	
Ποιος είναι ο σκοπός της επεξεργασίας;	
Ποια είναι η νομική βάση για την επεξεργασία;	
Πού θα αποθηκεύονται τα δεδομένα; (χώρα εντός του Ευρωπαϊκού Οικονομικού Χώρου (ΕΟΧ);)	
Ποιοι θα έχουν πρόσβαση;	
Για πόσο καιρό θα διατηρούνται τα δεδομένα;	
Θα κοινοποιηθούν τα δεδομένα σε τρίτους;	

Μέρος Β: Αξιολόγηση κινδύνου

Κίνδυνος	**Επίπεδο (Χαμηλό / Μέτριο / Υψηλό) και πώς θα αντιμετωπιστεί**
Μη εξουσιοδοτημένη πρόσβαση σε δεδομένα φοιτητών	

Κίνδυνος	Επίπεδο (Χαμηλό / Μέτριο / Υψηλό) και πώς θα αντιμετωπιστεί
Δεδομένα που έχουν χαθεί ή διαγραφεί κατά λάθος	
Δεδομένα που χρησιμοποιούνται για σκοπούς διαφορετικούς από τον αρχικό	
Μαθητές που παρακολουθούνται ή καταγράφονται χωρίς διαφάνεια	
Δεδομένα που διαβιβάζονται εκτός του Ευρωπαϊκού Οικονομικού Χώρου (ΕΟΧ) χωρίς εγγυήσεις	
Δεδομένα που διατηρούνται για περισσότερο χρόνο από ό,τι είναι απαραίτητο	

Μέρος Γ: Απόφαση

Συνολικό επίπεδο κινδύνου (Χαμηλό / Μέτριο / Υψηλό)	
Μπορεί να προχωρήσει η επεξεργασία; (Ναι / Ναι, με μέτρα μετριασμού / Όχι)	
Τι πρέπει να γίνει πριν ξεκινήσει η επεξεργασία;	
Ζητήθηκε η γνώμη του Υπεύθυνου Προστασίας Δεδομένων; (Ναι / Όχι / Ημερομηνία)	
Η αξιολόγηση ολοκληρώθηκε από	
Ημερομηνία αξιολόγησης	
Ημερομηνία επόμενης αναθεώρησης	

Παράρτημα VI: Μητρώο κινδύνων του σχολείου

Το Μητρώο κινδύνων του σχολείου βοηθά το σχολείο σας να εντοπίσει, να αξιολογήσει και να διαχειριστεί τους βασικούς κινδύνους στον τομέα της κυβερνοασφάλειας και της προστασίας δεδομένων που αντιμετωπίζει. Η συμπλήρωση αυτού του μητρώου αποτελεί ένα πρακτικό βήμα για την εφαρμογή της προσέγγισης διαχείρισης κινδύνων που περιγράφεται στο Μέρος 3 της παρούσας πολιτικής.

Τα παραδείγματα στον παρακάτω πίνακα είναι ενδεικτικά. Παρέχονται για να βοηθήσουν το σχολείο σας να ξεκινήσει και για να απεικονίσουν το είδος των κινδύνων που είναι πιο συνηθισμένοι σε ένα σχολικό περιβάλλον. Το σχολείο σας θα πρέπει να προσθέτει, να αφαιρεί ή να προσαρμόζει τις καταχωρήσεις ώστε να αντανακλούν τις δικές του συγκεκριμένες συνθήκες, τα συστήματά του και το πλαίσιο λειτουργίας του. Το μητρώο θα πρέπει να επανεξετάζεται τουλάχιστον μία φορά το χρόνο και να ενημερώνεται όποτε συμβαίνει μια σημαντική αλλαγή, όπως η εισαγωγή μιας νέας ψηφιακής πλατφόρμας ή ένα περιστατικό κυβερνοασφάλειας.

Πώς να βαθμολογήσετε τους κινδύνους

Για κάθε κίνδυνο, βαθμολογήστε την Πιθανότητα και τον Αντίκτυπο σε κλίμακα από 1 έως 5 (1 = πολύ χαμηλή, 5 = πολύ υψηλή). Πολλαπλασιάστε τις δύο βαθμολογίες για να υπολογίσετε τη Βαθμολογία Κινδύνου.

Υψηλός κίνδυνος (15-25): πρέπει να αντιμετωπιστεί αμέσως.

Μεσαίος-υψηλός κίνδυνος (8-14): πρέπει να αντιμετωπιστεί, δώστε προτεραιότητα σε εκείνους με υψηλό αντίκτυπο.

Μεσαίου-χαμηλού κινδύνου (4-7): πρέπει να αντιμετωπιστούν όταν ο αντίκτυπος είναι σημαντικός.

Χαμηλού κινδύνου (1-3): αποδεκτός, παρακολουθήστε τακτικά.

Στην επόμενη σελίδα (οριζόντια διάταξη) παρατίθεται ένας ενδεικτικός πίνακας καταλόγου κινδύνων

ID	Κίνδυνος	Τι θα μπορούσε να συμβεί	Πώς το μειώνουμε	Πιθανότητα (1-5)	Επίδραση (1-5)	Δείκτης κινδύνου	Υπεύθυνος	Αν συμβεί
1	Ηλεκτρονικό μήνυμα phishing που στοχεύει το προσωπικό	Το προσωπικό κάνει κλικ σε έναν κακόβουλο σύνδεσμο, παρέχοντας έτσι σε έναν εισβολέα πρόσβαση στα συστήματα του σχολείου και στα δεδομένα των μαθητών	Ετήσια εκπαίδευση του προσωπικού, ασκήσεις προσομοίωσης phishing, έλεγχος ταυτότητας πολλαπλών παραγόντων σε όλους τους λογαριασμούς	4	4	16	Διευθυντής / Συντονιστής Πληροφορικής	Απομονώστε τη συσκευή που έχει προσβληθεί, ενημερώστε την εθνική αρχή για την κυβερνοασφάλεια, επαναφέρετε τα δεδομένα από το αντίγραφο ασφαλείας
2	Επίθεση με λογισμικό εκβιασμού	Τα σχολικά συστήματα είναι κλειδωμένα, ενώ δεν είναι πλέον δυνατή η πρόσβαση στα αρχεία και τους βαθμούς των μαθητών	Τακτικά ελεγχόμενα αντίγραφα ασφαλείας που αποθηκεύονται εκτός δικτύου, ενημερωμένο λογισμικό προστασίας από ιούς, εκπαίδευση του προσωπικού	3	5	15	Συντονιστής Πληροφορικής	Επαναφορά από αντίγραφο ασφαλείας, υποβολή αναφοράς στην εθνική αρχή για την κυβερνοασφάλεια, ενημέρωση της αρχής προστασίας δεδομένων σε περίπτωση που επηρεάζονται δεδομένα μαθητών

ID	Κίνδυνος	Τι θα μπορούσε να συμβεί	Πώς το μειώνουμε	Πιθανότητα (1-5)	Επίδραση (1-5)	Δείκτης κινδύνου	Υπεύθυνος	Αν συμβεί
3	Τα στοιχεία των φοιτητών στάλθηκαν κατά λάθος σε λάθος πρόσωπο	Τα προσωπικά δεδομένα ενός μαθητή κοινοποιήθηκαν κατά λάθος σε μη εξουσιοδοτημένο πρόσωπο	Εκπαίδευση του προσωπικού σχετικά με τη διαχείριση δεδομένων, χρήση αποκλειστικά των επίσημων καναλιών επικοινωνίας του σχολείου	4	3	12	Υπεύθυνος Προστασίας Δεδομένων (DPO)	Επικοινωνήστε με τον παραλήπτη και ζητήστε τη διαγραφή, υποβάλετε αναφορά στην εθνική αρχή προστασίας δεδομένων εντός 72 ωρών, εάν απαιτείται, και καταγράψτε το περιστατικό
4	Κυβερνοεκφοβισμός μέσω της σχολικής πλατφόρμας	Ένας μαθητής χρησιμοποιεί ένα εργαλείο επικοινωνίας του σχολείου για να παρενοχλήσει έναν άλλο μαθητή	Πολιτική αποδεκτής χρήσης που υπογράφεται από όλους τους μαθητές και τους γονείς, ενημέρωση σχετικά με τον διαδικτυακό εκφοβισμό, σαφής διαδικασία αναφοράς	4	3	12	Διευθυντής / Τάξη	Ακολουθήστε τη σχολική διαδικασία κατά του εκφοβισμού, στηρίξτε τον μαθητή που έχει πληγεί, ενημερώστε τους γονείς, καταγράψτε το περιστατικό

Παράρτημα VII: Μητρώο Αντιστοίχισης Δεδομένων

Το Μητρώο αντιστοίχισης δεδομένων βοηθά το σχολείο σας να καταγράφει όλα τα προσωπικά δεδομένα που επεξεργάζεται. Η τήρηση αυτού του μητρώου αποτελεί νομική απαίτηση σύμφωνα με το άρθρο 30 του ΓΚΠΔ. Πρέπει να είναι διαθέσιμο στην εθνική αρχή προστασίας δεδομένων κατόπιν αιτήματος.

Τα παρακάτω παραδείγματα καλύπτουν τις πιο συνηθισμένες κατηγορίες προσωπικών δεδομένων που υποβάλλονται σε επεξεργασία από τα σχολεία. Είναι ενδεικτικά: το σχολείο σας θα πρέπει να προσθέσει τυχόν επιπλέον κατηγορίες που ισχύουν για τη δική σας περίπτωση και να αφαιρέσει όσες δεν ισχύουν. Ελέγξτε και ενημερώστε το μητρώο τουλάχιστον μία φορά το χρόνο και κάθε φορά που εισάγεται ένα νέο σύστημα ή μια νέα πλατφόρμα.

Τι είναι η νομική βάση;

Κάθε φορά που το σχολείο σας επεξεργάζεται προσωπικά δεδομένα, πρέπει να υπάρχει νόμιμος λόγος. Οι πιο συνηθισμένοι λόγοι για τα σχολεία είναι:

Νομική υποχρέωση: επεξεργασία που απαιτείται από την εθνική νομοθεσία για την εκπαίδευση (π.χ. τήρηση αρχείων παρουσίας).

Δημόσιο καθήκον: επεξεργασία που είναι απαραίτητη για την εκτέλεση των δημόσιων καθηκόντων του σχολείου.

Συγκατάθεση: το άτομο έχει συναινέσει στην επεξεργασία (απαιτείται για φωτογραφίες, μη απαραίτητες πλατφόρμες).

Στην επόμενη σελίδα (οριζόντια διάταξη) παρατίθεται ένας ενδεικτικός πίνακας του Μητρώου Αντιστοίχισης Δεδομένων.

Τύπος δεδομένων	Γιατί τα επεξεργαζόμαστε	Νομική βάση	Πού αποθηκεύεται	Ποιός έχει πρόσβαση	Για πόσο καιρό το διατηρούμε	Έχετε κάνει αντίγραφο ασφαλείας;	Κοινοποιήθηκε με
Προσωπικά δεδομένα των μαθητών (όνομα, αριθμός ταυτότητας, διεύθυνση, ημερομηνία γέννησης)	Απαιτείται για τη διοίκηση του σχολείου και τη συμμόρφωση με την εθνική νομοθεσία για την εκπαίδευση	Νομική υποχρέωση	Εθνικό σύστημα πληροφοριών για τα σχολεία (π.χ. MySchool, SIIIR, Unica)	Μόνο διευθυντής και διοικητικό προσωπικό	Σύμφωνα με τις διατάξεις της εθνικής νομοθεσίας	Ναι	Υπουργείο Παιδείας μέσω της εθνικής πλατφόρμας
Ακαδημαϊκά στοιχεία των μαθητών (βαθμοί, παρουσία, αξιολογήσεις)	Απαιτείται για την παρακολούθηση της προόδου των μαθητών και την ενημέρωση των γονέων	Νομική υποχρέωση / Δημόσιο καθήκον	Σύστημα πληροφοριών σχολείου και βαθμολόγιο καθηγητών	Τάξεις, διευθυντής, διοικητικό προσωπικό	Σύμφωνα με τις διατάξεις της εθνικής νομοθεσίας	Ναι	Γονείς (μέσω ασφαλούς καναλιού), Υπουργείο Παιδείας
Πληροφορίες σχετικά με την υγεία των μαθητών (αλλεργίες, αναπηρίες, ιατρικές ανάγκες)	Απαραίτητο για την προστασία της υγείας και της ασφάλειας των μαθητών κατά τη διάρκεια της σχολικής ημέρας	Νομική υποχρέωση / Ζωτικά συμφέροντα	Ασφαλές έντυπο αρχείο ή κρυπτογραφημένο ψηφιακό αρχείο	Μόνο ο διευθυντής, η σχολική νοσοκόμα και οι αρμόδιοι εκπαιδευτικοί	Διάρκεια εγγραφής, καθώς και ό,τι προβλέπεται από τη νομοθεσία	Ναι (κρυπτογραφημένο)	Πάροχοι υγειονομικής περίθαλψης, μόνο όπου είναι απαραίτητο

Τύπος δεδομένων	Γιατί τα επεξεργαζόμαστε	Νομική βάση	Πού αποθηκεύεται	Ποιός έχει πρόσβαση	Για πόσο καιρό το διατηρούμε	Έχετε κάνει αντίγραφο ασφαλείας;	Κοινοποιήθηκε με
Φωτογραφίες και εικόνες μαθητών	Μαθητική ταυτότητα, εκδόσεις, τεκμηρίωση εκδηλώσεων	Συγκατάθεση των γονέων	Διακομιστής του σχολείου ή εγκεκριμένη πλατφόρμα	Διοικητικό προσωπικό, εκπαιδευτικοί με εξουσιοδότηση	Διάρκεια εγγραφής· διαγράφηκε κατόπιν αιτήματος	Ναι	Δεν επιτρέπεται η κοινοποίηση σε τρίτους χωρίς περαιτέρω συγκατάθεση

Παράρτημα VIII: Μητρώο σχολικών πολιτικών και διαδικασιών

Το παρόν μητρώο βοηθά το σχολείο σας να παρακολουθεί τις βασικές πολιτικές ασφάλειας και προστασίας δεδομένων που έχει θεσπίσει. Η ύπαρξη τεκμηριωμένων πολιτικών σε καθέναν από αυτούς τους τομείς αποτελεί σημαντικό δείκτη ότι το σχολείο διαχειρίζεται τις ευθύνες του σε θέματα κυβερνοασφάλειας και προστασίας δεδομένων με οργανωμένο τρόπο.

Οι πολιτικές που παρατίθενται παρακάτω είναι αυτές που σχετίζονται περισσότερο με τις συστάσεις της παρούσας Πολιτικής Κυβερνοανθεκτικότητας. Ο κατάλογος είναι ενδεικτικός: το σχολείο σας ενδέχεται να διαθέτει επιπλέον πολιτικές που θα πρέπει επίσης να καταχωρηθούν εδώ. Για κάθε πολιτική, σημειώστε ποιος είναι υπεύθυνος για αυτήν, πότε ενημερώθηκε για τελευταία φορά και πότε προβλέπεται η επόμενη αναθεώρησή της. Σε περίπτωση που δεν υπάρχει ακόμη κάποια πολιτική, καταγράψτε αυτό ως δράση προτεραιότητας.

Διαθέσιμα πρότυπα

Στα παραρτήματα της παρούσας πολιτικής περιλαμβάνονται πρότυπα για αρκετές από τις πολιτικές που αναφέρονται παρακάτω:

- Πολιτική αποδεκτής χρήσης: Παράρτημα III.
- Διαδικασία αντιμετώπισης περιστατικών: Παράρτημα IV.
- Αξιολόγηση επιπτώσεων στην προστασία δεδομένων (DPIA): Παράρτημα V.
- Μητρώο κινδύνων: Παράρτημα VI.
- Μητρώο αντιστοίχισης δεδομένων: Παράρτημα VII.
- Αυτοαξιολόγηση της κυβερνοανθεκτικότητας του σχολείου: Παράρτημα IX

ID	Όνομα πολιτικής	Κύρια θέματα που καλύπτονται	Κάτοχος της ασφάλειας	Τελευταία ενημέρωση	Επόμενη κριτική
1	Πολιτική Αποδεκτής Χρήσης (AUP)	Χρήση σχολικών συστημάτων και συσκευών. Κανόνες για τα κινητά τηλέφωνα. Αναφορά περιστατικών.	Διευθυντής / Συντονιστής Πληροφορικής		
2	Πολιτική ελέγχου πρόσβασης	Ποιος έχει πρόσβαση σε ποια συστήματα και δεδομένα. Κανόνες για τους κωδικούς πρόσβασης. Αφαίρεση των	Συντονιστής Πληροφορικής / Υπεύθυνος Προστασίας		

ID	Όνομα πολιτικής	Κύρια θέματα που καλύπτονται	Κάτοχος της ασφάλειας	Τελευταία ενημέρωση	Επόμενη κριτική
		δικαιωμάτων πρόσβασης όταν ένας υπάλληλος αποχωρεί.	Δεδομένων		
3	Πολιτική προστασίας δεδομένων	Συμμόρφωση με τον ΓΚΠΔ (GDPR). Αρμοδιότητες του Υπεύθυνου Προστασίας Δεδομένων (DPO). Συγκατάθεση των γονέων. Δηλώσεις προστασίας προσωπικών δεδομένων. Αντιμετώπιση παραβιάσεων δεδομένων.	Υπεύθυνος Προστασίας Δεδομένων / Διευθυντής		
4	Πολιτική δημιουργίας αντιγράφων ασφαλείας	Τι αντίγραφα ασφαλείας δημιουργούνται, με ποια συχνότητα, πού αποθηκεύονται και πώς ελέγχεται η διαδικασία ανάκτησης.	Συντονιστής Πληροφορικής		
5	Πολιτική αντιμετώπισης περιστατικών	Πώς αντιδρά το σχολείο σε περιστατικά κυβερνοασφάλειας και παραβιάσεις δεδομένων. Ποιος είναι υπεύθυνος. Πώς γίνεται η ενημέρωση των αρχών.	Διευθυντής / Υπεύθυνος Προστασίας Δεδομένων / Συντονιστής Πληροφορικής		

ID	Όνομα πολιτικής	Κύρια θέματα που καλύπτονται	Κάτοχος της ασφάλειας	Τελευταία ενημέρωση	Επόμενη κριτική
6	Πολιτική κατά του εκφοβισμού (συμπεριλαμβανομένου του διαδικτυακού εκφοβισμού)	Ορισμός του διαδικτυακού εκφοβισμού. Διαδικασία αναφοράς. Πώς ανταποκρίνεται το σχολείο. Εκπαίδευση του προσωπικού. Συμμετοχή των γονέων.	Διευθυντής		
7	Πολιτική για τις κινητές συσκευές	Κανόνες σχετικά με τη χρήση κινητών τηλεφώνων από τους μαθητές, σύμφωνα με την εθνική νομοθεσία. Απαγόρευση της μη εξουσιοδοτημένης καταγραφής.	Διευθυντής		

Παράρτημα IX: Αυτοαξιολόγηση της κυβερνοανθεκτικότητας των σχολείων

Τα σχολεία μπορούν να χρησιμοποιήσουν αυτόν τον κατάλογο ελέγχου για να αποκτήσουν μια βασική εικόνα της τρέχουσας κυβερνοανθεκτικότητάς τους και να εντοπίσουν τα κενά που πρέπει να αντιμετωπιστούν κατά προτεραιότητα. Σημειώστε κάθε στοιχείο ως «Ναι», «Εν μέρει» ή «Όχι». Ο σκοπός δεν είναι η επιτυχία ή η αποτυχία, αλλά ο εντοπισμός των τομέων στους οποίους πρέπει να επικεντρωθούν οι προσπάθειες.

Τα σχολεία ενθαρρύνονται να επαναλαμβάνουν αυτή την αυτοαξιολόγηση τουλάχιστον μία φορά το χρόνο. Η παρακολούθηση των αποτελεσμάτων με την πάροδο του χρόνου βοηθά στην παρακολούθηση της προόδου και υποστηρίζει μια κουλτούρα συνεχούς βελτίωσης.

Τα στοιχεία που αναφέρονται είναι ενδεικτικά. Προσαρμόστε τα ώστε να αντανακλούν το συγκεκριμένο πλαίσιο του σχολείου σας, τις εθνικές απαιτήσεις και τις συγκεκριμένες περιστάσεις.

Τομέας	Τι πρέπει να ελέγξετε	Ναι / Εν μέρει / Όχι
Διακυβέρνηση	Το σχολείο διαθέτει έναν ειδικά ορισμένο συντονιστή για θέματα κυβερνοασφάλειας ή ψηφιακής ασφάλειας.	
Διακυβέρνηση	Το σχολείο διαθέτει γραπτή Πολιτική Αποδεκτής Χρήσης, η οποία αναθεωρήθηκε τα τελευταία 2 χρόνια.	
Διακυβέρνηση	Το σχολείο διαθέτει μια τεκμηριωμένη διαδικασία αντιμετώπισης περιστατικών, η οποία είναι γνωστή στο προσωπικό.	
Ευαισθητοποίηση και κατάρτιση	Το προσωπικό παρακολουθεί τουλάχιστον μία φορά το χρόνο εκπαίδευση σε θέματα κυβερνοασφάλειας και ασφάλειας στο διαδίκτυο.	
Ευαισθητοποίηση και κατάρτιση	Οι μαθητές λαμβάνουν εκπαίδευση σε θέματα ψηφιακής πολιτειότητας και ασφάλειας στο διαδίκτυο, κατάλληλη για την ηλικία τους.	
Ευαισθητοποίηση και κατάρτιση	Οι γονείς και οι κηδεμόνες ενημερώνονται για τους ψηφιακούς κινδύνους τουλάχιστον μία φορά ανά σχολικό έτος.	
Ευημερία και Πρόληψη	Το σχολείο διαθέτει ένα συγκεκριμένο, ονομασμένο πρωτόκολλο για την αντιμετώπιση του διαδικτυακού εκφοβισμού.	
Ευημερία και Πρόληψη	Οι μαθητές γνωρίζουν πώς και σε ποιον να αναφέρουν εμπιστευτικά τα περιστατικά που συμβαίνουν στο διαδίκτυο.	
Ευημερία και Πρόληψη	Οι δράσεις πρόληψης απευθύνονται ρητά σε διαφορετικές και ευάλωτες ομάδες.	
Δεδομένα και προστασία της ιδιωτικής ζωής	Το σχολείο τηρεί κατάλογο των πλατφορμών και των εργαλείων που επεξεργάζονται τα δεδομένα των μαθητών.	
Δεδομένα και προστασία της ιδιωτικής ζωής	Όπου απαιτείται από το νόμο, λαμβάνεται η συγκατάθεση των γονέων πριν από την εγγραφή των μαθητών σε ψηφιακές πλατφόρμες.	
Τεχνικά μέτρα	Οι συσκευές και τα δίκτυα των σχολείων χρησιμοποιούν ενημερωμένο λογισμικό	

Τομέας	Τι πρέπει να ελέγξετε	Ναι / Εν μέρει / Όχι
	προστασίας και μηχανισμούς ελέγχου πρόσβασης.	
Τεχνικά μέτρα	Τα αντίγραφα ασφαλείας των κρίσιμων σχολικών δεδομένων δημιουργούνται τακτικά και ελέγχονται.	

Πώς να ερμηνεύσετε τη βαθμολογία σας

Μετρήστε τις απαντήσεις «Ναι» (1 βαθμός) και τις απαντήσεις «Εν μέρει» (0,5 βαθμοί). Διαιρέστε το αποτέλεσμα με το 13 και πολλαπλασιάστε το με το 100 για να βρείτε το ποσοστό. Αντιστοιχίστε το αποτέλεσμα στα παρακάτω επίπεδα ωριμότητας.

Επίπεδο	Βαθμολογία	Περιγραφή
1 - Αρχικό	0 έως 20%	Υπάρχουν ελάχιστες ή καθόλου επίσημες διαδικασίες διακυβέρνησης, εκπαίδευσης ή αντιμετώπισης περιστατικών.
2 - Αναπτυσσόμενο	21 έως 45%	Υπάρχουν βασικές πολιτικές, αλλά δεν εφαρμόζονται, δεν αναθεωρούνται και δεν κοινοποιούνται με συνέπεια.
3 - Καθιερωμένο	46 έως 70%	Τα βασικά στοιχεία διακυβέρνησης, εκπαίδευσης και αντιμετώπισης περιστατικών έχουν τεθεί σε εφαρμογή και είναι γνωστά στο προσωπικό.
4 - Προχωρημένο	71 έως 90%	Οι ολοκληρωμένες πολιτικές, οι οποίες αναθεωρούνται τακτικά, καθώς και τα προγράμματα κατάρτισης απευθύνονται στο προσωπικό, τους μαθητές και τους γονείς.
5 - Ανθεκτικό	91 έως 100%	Η ανθεκτικότητα στον κυβερνοχώρο είναι ενσωματωμένη στην σχολική κουλτούρα μέσω της συνεχούς κατάρτισης και της προληπτικής δράσης χωρίς αποκλεισμούς.

Τα επίπεδα αυτά αποτελούν απλώς ένα εργαλείο αυτοαξιολόγησης και δεν συνιστούν επίσημη πιστοποίηση ή αξιολόγηση συμμόρφωσης.

Παραπομπές

Νομοθεσία της Ευρωπαϊκής Ένωσης

Τα ακόλουθα νομικά κείμενα της Ευρωπαϊκής Ένωσης αποτελούν το κοινό νομικό πλαίσιο στο οποίο βασίζεται η παρούσα Πολιτική. Καθορίζουν τις βασικές απαιτήσεις για την προστασία των δεδομένων, την κυβερνοασφάλεια, την τεχνητή νοημοσύνη, τις ψηφιακές υπηρεσίες, τις ηλεκτρονικές επικοινωνίες και την ψηφιακή εκπαίδευση σε όλα τα κράτη μέλη της ΕΕ.

- Ευρωπαϊκή Ένωση, Κανονισμός (ΕΕ) 2016/679 (Γενικός Κανονισμός για την Προστασία Δεδομένων – GDPR), Επίσημη Εφημερίδα της Ευρωπαϊκής Ένωσης. Διαθέσιμο στη διεύθυνση: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679
- Ευρωπαϊκή Ένωση, Οδηγία (ΕΕ) 2022/2555 (Οδηγία NIS 2), Επίσημη Εφημερίδα της Ευρωπαϊκής Ένωσης. Διαθέσιμη στη διεύθυνση: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022L2555
- Ευρωπαϊκή Ένωση, Κανονισμός (ΕΕ) 2024/1689 (Νόμος για την Τεχνητή Νοημοσύνη), Επίσημη Εφημερίδα της Ευρωπαϊκής Ένωσης. Διαθέσιμο στη διεύθυνση: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L_202401689

- Ευρωπαϊκή Ένωση, Κανονισμός (ΕΕ) 2022/2065 (Νόμος για τις Ψηφιακές Υπηρεσίες), Επίσημη Εφημερίδα της Ευρωπαϊκής Ένωσης. Διαθέσιμο στη διεύθυνση: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022R2065

- Ευρωπαϊκή Ένωση, Οδηγία 2002/58/ΕΚ (Οδηγία για την ηλεκτρονική ιδιωτικότητα), Επίσημη Εφημερίδα των Ευρωπαϊκών Κοινοτήτων. Διαθέσιμη στη διεύθυνση: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32002L0058 Ευρωπαϊκή Ένωση, Κανονισμός (ΕΕ) 2019/881 (Νόμος για την Κυβερνοασφάλεια), Επίσημη Εφημερίδα της Ευρωπαϊκής Ένωσης. Διαθέσιμο στη διεύθυνση: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019R0881

Εθνικά νομοθετικά κείμενα

Για την εκπόνηση του Μέρους 2 της παρούσας πολιτικής χρησιμοποιήθηκαν τα ακόλουθα εθνικά νομοθετικά κείμενα και επίσημες πηγές. Παρατίθενται ανά χώρα, σύμφωνα με την καθιερωμένη πρακτική αναφοράς για τα έργα που χρηματοδοτούνται από την Ευρωπαϊκή Ένωση.

Ελλάδα

- Ελληνική Δημοκρατία (2018). Νόμος 4577/2018 περί ασφάλειας δικτύων και συστημάτων πληροφοριών. Εφημερίδα της Κυβερνήσεως Α΄ 199/03.12.2018. Διαθέσιμο στη διεύθυνση: https://www.mindigital.gr/wp-content/uploads/2019/09/N.4577_2018.pdf
- Ελληνική Δημοκρατία (2019). Νόμος 4624/2019 για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα (εφαρμογή του ΓΚΠΔ). Εφημερίδα της Κυβερνήσεως Α' 137/29.08.2019. Διαθέσιμο στη διεύθυνση: https://www.dpa.gr/sites/default/files/2020-08/LAW%204624_2019_EN_TRANSLATED%20BY%20THE%20HDPA.PDF
- Ελληνική Δημοκρατία (2020). Νόμος 4727/2020 περί Ψηφιακής Διακυβέρνησης και Ηλεκτρονικών Επικοινωνιών. Εφημερίδα της Κυβερνήσεως Α΄ 184/23.09.2020. Διαθέσιμο στη διεύθυνση: https://adae.gov.gr/images/nomothetiko-plaisio/Nomos_4727_2020_01.pdf
- Ελληνική Δημοκρατία (2022). Νόμος 4961/2022 περί αναδυόμενων τεχνολογιών και ψηφιακής διακυβέρνησης. Εφημερίδα της Κυβερνήσεως Α΄ 146/27.07.2022. Διαθέσιμο στη διεύθυνση: https://www.mindigital.gr/wp-content/uploads/2024/02/N-4961.pdf
- Ελληνική Δημοκρατία (2023). Νόμος 5029/2023 για την πρόληψη και τη διαχείριση της σχολικής βίας και του διαδικτυακού εκφοβισμού. Εφημερίδα της Κυβερνήσεως Α'

55/10.03.2023. Διαθέσιμο στη διεύθυνση: https://www.iep.edu.gr/wp-content/uploads/2025/01/2024-08-02_N_5029-2023.pdf

- Ελληνική Δημοκρατία (2024). Νόμος 5160/2024 περί Κυβερνοασφάλειας (μεταφορά της οδηγίας NIS2). Εφημερίδα της Κυβερνήσεως Α΄ 195/27.11.2024. Διαθέσιμο στη διεύθυνση: https://search.et.gr/el/fek/?fekId=774154
- Υπουργείο Ψηφιακής Διακυβέρνησης, Ελληνική Δημοκρατία (2025). Υπουργική Απόφαση 1689/2025 σχετικά με τις απαιτήσεις κυβερνοασφάλειας για φορείς του δημόσιου τομέα. Εφημερίδα της Κυβέρνησης Β' 2186/06.05.2025. Διαθέσιμο στη διεύθυνση: https://cyber.gov.gr/wp-content/uploads/2025/05/20250202186.pdf
- Υπουργείο Ψηφιακής Διακυβέρνησης, Ελληνική Δημοκρατία (2025). Υπουργική Απόφαση 1899/2025 σχετικά με τη Διακυβέρνηση της Ασφάλειας των Πληροφοριών για τους Δημόσιους Φορείς. Εφημερίδα της Κυβέρνησης Β΄ 4250/05.08.2025. Διαθέσιμο στη διεύθυνση: https://cyber.gov.gr/wp-content/uploads/2025/03/KYA_APOFASI_10-Feb-2025_FEK-463_DEFTERO-TEFHOS.pdf

Ιταλία

- Ιταλική Δημοκρατία (2003). Νομοθετικό διάταγμα αριθ. 196/2003 — Κώδικας Προστασίας Προσωπικών Δεδομένων, όπως τροποποιήθηκε με το νομοθετικό διάταγμα αριθ. 101/2018. Διαθέσιμο στη διεύθυνση: https://www.garanteprivacy.it/documents/10160/0/Codice+in+materia+di+protezione+dei+dati+personali.pdf
- Ιταλική Δημοκρατία (2021). Νόμος αριθ. 109/2021 για τη μετατροπή του νομοθετικού διατάγματος αριθ. 82/2021 — Ίδρυση της Εθνικής Υπηρεσίας Κυβερνοασφάλειας (ACN). Επίσημη Εφημερίδα, 04.08.2021. Διαθέσιμο στη διεύθυνση: https://www.gazzettaufficiale.it/atto/serie_generale/caricaDettaglioAtto/originario?atto.codiceRedazionale=21A04841
- Ιταλική Δημοκρατία (2024). Νομοθετικό διάταγμα αριθ. 138/2024 — Μεταφορά της οδηγίας NIS2. Επίσημη Εφημερίδα, 01.10.2024. Διαθέσιμο στη διεύθυνση: https://www.gazzettaufficiale.it/eli/id/2024/10/01/24G00155/SG
- Υπουργείο Παιδείας της Ιταλικής Δημοκρατίας (2020). Υπουργική απόφαση αριθ. 89/2020 — Κατευθυντήριες γραμμές για την Ψηφιακή Ολοκληρωμένη Διδασκαλία (DDI). Διαθέσιμο στη διεύθυνση: https://www.mim.gov.it/documents/20182/0/Decreto.pdf
- Υπουργείο Παιδείας της Ιταλικής Δημοκρατίας (2024). Εγκύκλιος MIM αριθ. 5274/2024 — Περιορισμοί στη χρήση smartphone στα σχολεία. Διαθέσιμο στη διεύθυνση: https://www.mim.gov.it/-/nota-n-5274-dell-11-luglio-2024
- Υπουργείο Παιδείας της Ιταλικής Δημοκρατίας (2025). Εγκύκλιος MIM αριθ. 3392/2025 — Περιορισμοί στη χρήση κινητών τηλεφώνων στα σχολεία. Διαθέσιμο στη διεύθυνση: https://www.mim.gov.it/-/circolare-n-3392-del-16-giugno-2025
- Υπουργείο Παιδείας της Ιταλικής Δημοκρατίας (2025). Υπουργική απόφαση αριθ. 166/2025 — Κατευθυντήριες γραμμές για την υπεύθυνη χρήση της τεχνητής νοημοσύνης στα σχολεία. Διαθέσιμο στη διεύθυνση: https://www.mim.gov.it/-/decreto-ministeriale-n-166-del-9-agosto-2025

Πορτογαλία

- Πορτογαλική Δημοκρατία (2018). Νόμος αριθ. 46/2018 — Νομικό πλαίσιο για την ασφάλεια στον κυβερνοχώρο (RFSC). Diário da República, 13.08.2018. Διαθέσιμο στη διεύθυνση: https://diariodarepublica.pt/dr/detalhe/lei/46-2018-116029384

- Πορτογαλική Δημοκρατία (2019). Νόμος αριθ. 58/2019 — Πορτογαλικός νόμος περί προστασίας δεδομένων (εφαρμογή του ΓΚΠΔ). Diário da República, 08.08.2019. Διαθέσιμο στη διεύθυνση: https://diariodarepublica.pt/dr/detalhe/lei/58-2019-123815982
- Συμβούλιο Υπουργών της Πορτογαλικής Δημοκρατίας (2020). Ψήφισμα αριθ. 30/2020 — Σχέδιο Δράσης για την Ψηφιακή Μετάβαση (PATD). Diário da República, 2020. Διαθέσιμο στη διεύθυνση: https://diariodarepublica.pt/dr/detalhe/resolucao-conselho-ministros/30-2020-132133788
- Πορτογαλική Δημοκρατία (2025). Νομοθετικό διάταγμα αριθ. 95/2025 — Απαγόρευση της χρήσης smartphone στα σχολεία (1η–6η τάξη). Diário da República, 03.07.2025.
- Πορτογαλική Δημοκρατία (2025). Νομοθετικό διάταγμα αριθ. 125/2025 — Μεταφορά του NIS2 (σε ισχύ από τις 3 Απριλίου 2026). Diário da República, 04.12.2025. Διαθέσιμο στη διεύθυνση: Decreto-Lei n.º 125/2025, de 4 de dezembro | DR
- Γενική Διεύθυνση Εκπαίδευσης (DGE), Πορτογαλία. PADDE — Πλαίσιο Σχεδίου Δράσης για την Ψηφιακή Ανάπτυξη των Σχολείων. Διαθέσιμο στη διεύθυνση: https://www.dge.mec.pt
- Εθνικό Κέντρο Κυβερνοασφάλειας (CNCS) / DGE, Πορτογαλία. SeguraNet — Πόροι για την ψηφιακή ασφάλεια και την κυβερνοασφάλεια στα σχολεία. Διαθέσιμο στη διεύθυνση: https://www.seguranet.pt
- Εθνικό Κέντρο Κυβερνοασφάλειας (CNCS), Πορτογαλία. CERT.PT — Εθνική Ομάδα Αντιμετώπισης Έκτακτων Περιστατικών Πληροφορικής. Διαθέσιμο στη διεύθυνση: https://www.cncs.gov.pt/pt/certpt/

Ρουμανία

- Δημοκρατία της Ρουμανίας (2018). Νόμος αριθ. 190/2018 — Προστασία δεδομένων προσωπικού χαρακτήρα (εφαρμογή του ΓΚΠΔ). Εφημερίδα της Κυβερνήσεως της Ρουμανίας αριθ. 651/26.07.2018. Διαθέσιμο στη διεύθυνση: https://portal.just.ro/101/Documents/LEGE__190_2018_date_cu_caracter_personal.pdf
- Δημοκρατία της Ρουμανίας (2023). Νόμος αριθ. 58/2023 σχετικά με τις υποχρεώσεις στον τομέα της κυβερνοασφάλειας για τους διαχειριστές δικτύων και συστημάτων πληροφοριών. Εφημερίδα της Κυβερνήσεως της Ρουμανίας αριθ. 214/15.03.2023. Διαθέσιμο στη διεύθυνση: https://legislatie.just.ro/Public/DetaliiDocument/265677
- Δημοκρατία της Ρουμανίας (2023). Νόμος αριθ. 198/2023 — Νόμος περί προπανεπιστημιακής εκπαίδευσης. Επίσημη Εφημερίδα της Ρουμανίας αριθ. 613/05.07.2023. Διαθέσιμο στη διεύθυνση: https://edu.ro/sites/default/files/_fisiere/Minister/2023/Legi_educatie_Romania_educata/legi_monitor/Legea_invatamantului_preuniversitar_nr_198.pdf
- Κυβέρνηση της Ρουμανίας (2024). Έκτακτη Διαταγή (OUG) αριθ. 155/2024 — Μεταφορά του NIS2 (εγκρίθηκε με τον Νόμο αριθ. 124/2025). Εφημερίδα της Κυβερνήσεως της Ρουμανίας αριθ. 1332/31.12.2024. Διαθέσιμο στη διεύθυνση: https://legislatie.just.ro/Public/DetaliiDocumentAfis/293121
- Υπουργείο Παιδείας της Ρουμανίας (2024). Απόφαση αριθ. 5707/2024 — Κανονισμός Φοιτητών. Επίσημη Εφημερίδα της Ρουμανίας αριθ. 795/12.08.2024. Διαθέσιμο στη διεύθυνση: https://www.edu.ro/sites/default/files/_fisiere/Legislatie/2024/OM_5707_2024_Statut_elev.pdf
- Υπουργείο Παιδείας της Ρουμανίας (2025). OMEC 6055-6058 — ROFUIP 2025-2026: Κανονισμός-πλαίσιο για την οργάνωση και τη λειτουργία των προπανεπιστημιακών εκπαιδευτικών μονάδων. Εφημερίδα της Κυβερνήσεως της Ρουμανίας αριθ. 819/04.09.2025. Διαθέσιμο στη διεύθυνση: https://www.edu.ro/ROFUIP

Σλοβακία

- Σλοβακική Δημοκρατία (2003). Νόμος αριθ. 596/2003 Coll. περί κρατικής διοίκησης στην εκπαίδευση και της σχολικής αυτοδιοίκησης (Νόμος περί σχολείων και σχολικών εγκαταστάσεων), όπως τροποποιήθηκε. Διαθέσιμο στη διεύθυνση: https://www.slov-lex.sk
- Σλοβακική Δημοκρατία (2008). Νόμος αριθ. 245/2008 Coll. περί εκπαίδευσης και κατάρτισης (Νόμος για τα σχολεία), όπως τροποποιήθηκε με τον Νόμο αριθ. 323/2025 Coll. που τέθηκε σε ισχύ την 1η Ιανουαρίου 2025 (περιορισμοί στη χρήση κινητών τηλεφώνων). Διαθέσιμο στη διεύθυνση: https://www.slov-lex.sk/ezbierky/pravne-predpisy/SK/ZZ/2008/245/
- Σλοβακική Δημοκρατία (2018). Νόμος αριθ. 18/2018 Coll. σχετικά με την προστασία των δεδομένων προσωπικού χαρακτήρα (εφαρμογή του ΓΚΠΔ). Διαθέσιμο στη διεύθυνση: https://www.slov-lex.sk/ezbierky/pravne-predpisy/SK/ZZ/2018/18
- Σλοβακική Δημοκρατία (2018). Νόμος αριθ. 69/2018 Coll. περί κυβερνοασφάλειας. Διαθέσιμο στη διεύθυνση: https://www.zakonypreludi.sk/zz/2018-69
- Σλοβακική Δημοκρατία (2024). Νόμος αριθ. 366/2024 Coll. περί κυβερνοασφάλειας (μεταφορά της οδηγίας NIS2), που τέθηκε σε ισχύ την 1η Ιανουαρίου 2025. Διαθέσιμο στη διεύθυνση: https://www.slov-lex.sk/ezbierky/pravne-predpisy/SK/ZZ/2018/18/
- Υπουργείο Παιδείας της Σλοβακικής Δημοκρατίας (2025). Κατευθυντήρια οδηγία αριθ. 1/2025 για την πρόληψη και την αντιμετώπιση του διαδικτυακού εκφοβισμού στα σχολεία και τις εκπαιδευτικές εγκαταστάσεις. Διαθέσιμο στη διεύθυνση: https://www.minedu.sk/data/att/d76/32441.fb1a83.pdf
- Υπουργείο Παιδείας, Σλοβακική Δημοκρατία (2025). Σχέδιο για την υπεύθυνη χρήση της τεχνητής νοημοσύνης στην εκπαίδευση 2025-2027. Διαθέσιμο στη διεύθυνση: https://ai.iedu.sk/

Πρότυπα ISO

Τα ακόλουθα διεθνώς αναγνωρισμένα πρότυπα αποτέλεσαν τη βάση για την εκπόνηση των πρακτικών συστάσεων και των μέτρων διακυβέρνησης που παρουσιάζονται στην παρούσα Πολιτική.

- Διεθνής Οργανισμός Τυποποίησης (ISO), ISO/IEC 27001:2022, Ασφάλεια πληροφοριών, κυβερνοασφάλεια και προστασία της ιδιωτικής ζωής – Συστήματα διαχείρισης ασφάλειας πληροφοριών – Απαιτήσεις. Διαθέσιμο στη διεύθυνση: https://www.iso.org/standard/27001
- Διεθνής Οργανισμός Τυποποίησης (ISO), ISO/IEC 27002:2022, Ασφάλεια πληροφοριών, κυβερνοασφάλεια και προστασία της ιδιωτικής ζωής – Μέτρα ελέγχου ασφάλειας πληροφοριών. Διαθέσιμο στη διεύθυνση: https://www.iso.org/standard/75652.html
- Διεθνής Οργανισμός Τυποποίησης (ISO), ISO/IEC 27701:2025, Τεχνικές ασφάλειας — Επέκταση των προτύπων ISO/IEC 27001 και ISO/IEC 27002 για τη διαχείριση πληροφοριών σχετικά με την προστασία της ιδιωτικής ζωής — Απαιτήσεις και κατευθυντήριες γραμμές. Διαθέσιμο στη διεύθυνση: https://www.iso.org/standard/27701
- Διεθνής Οργανισμός Τυποποίησης (ISO), ISO 22301:2019, Ασφάλεια και ανθεκτικότητα – Συστήματα διαχείρισης επιχειρησιακής συνέχειας – Απαιτήσεις. Διαθέσιμο στη διεύθυνση: https://www.iso.org/standard/75106.html
- Διεθνής Οργανισμός Τυποποίησης (ISO), ISO 31000:2018, Διαχείριση κινδύνων – Κατευθυντήριες οδηγίες. Διαθέσιμο στη διεύθυνση: https://www.iso.org/standard/65694.html

Έρευνα και στοιχεία

Για την εκπόνηση του Μέρους 4 της παρούσας πολιτικής χρησιμοποιήθηκαν οι ακόλουθες ερευνητικές πηγές και δημοσιεύσεις.

- Ευρωπαϊκή Επιτροπή (2025). Οι απόψεις των παιδιών για τον διαδικτυακό εκφοβισμό: Διαβούλευση με παιδιά ηλικίας 12-17 ετών. Διαθέσιμο στη διεύθυνση: https://eu-for-children.europa.eu/cyberbullying_en
- Ευρωπαϊκή Επιτροπή (2025). Κατευθυντήριες γραμμές σχετικά με μέτρα για τη διασφάλιση υψηλού επιπέδου ιδιωτικότητας, ασφάλειας και προστασίας των ανηλίκων στο διαδίκτυο. Διαθέσιμο στη διεύθυνση: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:C_202505519
- Ευρωπαϊκή Επιτροπή / «Καλύτερο Διαδίκτυο για τα Παιδιά» (BIK+) / Δίκτυο Insafe (2025-2026). BIK Policy Monitor και στατιστικά στοιχεία της γραμμής βοήθειας. Διαθέσιμο στη διεύθυνση: https://better-internet-for-kids.europa.eu/en
- Οργανισμός της Ευρωπαϊκής Ένωσης για την Κυβερνοασφάλεια (ENISA) (2022). Πρωτοβουλίες εκπαίδευσης στον τομέα της κυβερνοασφάλειας στα κράτη μέλη της ΕΕ. Διαθέσιμο στη διεύθυνση: https://www.enisa.europa.eu/publications/cybersecurity-education-initiatives-in-the-eu-member-states
- ΟΟΣΑ (2025). Πώς είναι η ζωή των παιδιών στην ψηφιακή εποχή; Διαθέσιμο στη διεύθυνση: 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., κ.ά. (2021). Συστηματική ανασκόπηση και μετα-ανάλυση παρεμβάσεων για τη μείωση της διάπραξης και της θυματοποίησης από διαδικτυακό εκφοβισμό. Prevention Science. Διαθέσιμο στη διεύθυνση: https://link.springer.com/article/10.1007/s11121-021-01259-y
- Torgal, C. και Aksoy, C. (2022). Μια μετα-ανάλυση της επίδρασης των σχολικών προγραμμάτων πρόληψης του διαδικτυακού εκφοβισμού στη συμπεριφορά των διαδικτυακών παρευρισκομένων. School Psychology Review, 52(2). Διαθέσιμο στη διεύθυνση: https://www.tandfonline.com/doi/full/10.1080/2372966X.2021.1913037
- Περιφερειακό Γραφείο της Ευρώπης του Παγκόσμιου Οργανισμού Υγείας (2024). Συμπεριφορά Υγείας σε Παιδιά Σχολικής Ηλικίας (HBSC): Ευρήματα σχετικά με τον εκφοβισμό και τον διαδικτυακό εκφοβισμό. Διαθέσιμο στη διεύθυνση: https://www.who.int/europe/initiatives/health-behaviour-in-school-aged-children-(hbsc)-study
- Κυβερνοεκφοβισμός και νέοι της LGBTQ κοινότητας: Συστηματική ανασκόπηση της βιβλιογραφίας και συστάσεις για την πρόληψη και την παρέμβαση (2018). Διαθέσιμο στη διεύθυνση: https://pmc.ncbi.nlm.nih.gov/articles/PMC7163911/
- Συσχετίσεις μεταξύ του εθισμού στα μέσα κοινωνικής δικτύωσης και του άγχους, της κατάθλιψης, του FoMO, της μοναξιάς και της αυτοεκτίμησης στους φοιτητές: Μια συστηματική ανασκόπηση και μετα-ανάλυση (2025). PLOS ONE. Διαθέσιμο στη διεύθυνση: https://journals.plos.org/plosone/article?id=10.1371/journal.pone.0329466