Πολιτική ασφάλειας στο διαδίκτυο

Το 18ο Δ.Σ. Λάρισας εφαρμόζει τις αρχές της πολιτικής ασφάλειας στο διαδίκτυο και υλοποιεί πρακτικές που εναρμονίζονται με τον Γενικό Κανονισμό για την Προστασία Δεδομένων (GDPR). Υπεύθυνοι Προστασίας Δεδομένων και Ασφάλειας στο Διαδίκτυο είναι η διευθύντρια και ο πληροφορικός του σχολείου, ενώ στην εφαρμογή της πολιτικής ασφαλείας συμμετέχει ενεργά το σύνολο του διδακτικού προσωπικού του σχολείου.

➢ *Η αναγκαιότητα σχεδιασμού και εφαρμογής πολιτικής ασφάλειας στο διαδίκτυο*

Η εφαρμογή στο σχολείο μιας πολιτικής ασφάλειας στο διαδίκτυο είναι κρίσιμη για πολλούς λόγους, οι οποίοι περιλαμβάνουν την προστασία των μαθητών, τη διατήρηση της ακεραιότητας του εκπαιδευτικού περιβάλλοντος και τη συμμόρφωση του σχολείου με τον Γενικό Κανονισμό για την Προστασία Δεδομένων (GDPR). Αναλυτικά, οι λόγοι είναι οι εξής:

1. **Προστασία Μαθητών**:
   - **Ασφάλεια από Κακόβουλο Περιεχόμενο**: Η πολιτική ασφάλειας προστατεύει τους μαθητές από την έκθεση σε ακατάλληλο ή βίαιο υλικό.
   - **Αποτροπή Εκφοβισμού (Cyberbullying)**: Εντοπισμός και αποτροπή περιστατικών διαδικτυακού εκφοβισμού, τα οποία μπορούν να επηρεάσουν σοβαρά την ψυχική υγεία των μαθητών.
   - **Προστασία Προσωπικών Δεδομένων**: Διασφάλιση ότι οι προσωπικές πληροφορίες των μαθητών δεν εκτίθενται ή χρησιμοποιούνται με μη εξουσιοδοτημένο τρόπο.

2. **Προστασία Εκπαιδευτικού Περιβάλλοντος**:
   - **Διατήρηση Εστίασης**: Περιορισμός της πρόσβασης σε ιστοσελίδες και εφαρμογές που δεν σχετίζονται με τη μάθηση, βοηθώντας τους μαθητές να παραμένουν συγκεντρωμένοι στις εκπαιδευτικές δραστηριότητες.
   - **Πρόληψη Απωλειών Δεδομένων**: Προστασία των σχολικών δεδομένων από κλοπή ή καταστροφή λόγω κακόβουλου λογισμικού ή διαδικτυακών επιθέσεων.

3. **Συμμόρφωση με Νομοθεσία και Κανονισμούς**:
   - **GDPR και Άλλοι Κανονισμοί**: Συμμόρφωση με τον Γενικό Κανονισμό για την Προστασία Δεδομένων (GDPR) και άλλες τοπικές και διεθνείς νομοθεσίες για την προστασία δεδομένων.
   - **Υποχρεώσεις Αναφοράς**: Εξασφάλιση ότι το σχολείο μπορεί να αναφέρει και να διαχειριστεί σωστά περιστατικά παραβίασης ασφάλειας, όπως απαιτείται από τον νόμο.

4. **Εκπαιδευτική Ευθύνη και Ποιότητα Εκπαίδευσης**:
   - **Ψηφιακή Ιθαγένεια**: Εκπαίδευση των μαθητών σχετικά με την υπεύθυνη και ασφαλή χρήση του διαδικτύου, προετοιμάζοντάς τους για την ψηφιακή κοινωνία.
   - **Διατήρηση Ποιότητας Εκπαίδευσης**: Διασφάλιση ότι οι ψηφιακές πηγές και οι τεχνολογίες που χρησιμοποιούνται στο σχολείο υποστηρίζουν την εκπαιδευτική αποστολή και δεν παρεμποδίζουν τη διαδικασία μάθησης.

5. **Προστασία του Σχολικού Οργανισμού:**
    - **Ασφάλεια Συστήματος**: Προστασία του σχολικού δικτύου και των συστημάτων από επιθέσεις, όπως hacking, phishing και άλλες κακόβουλες δραστηριότητες.

6. **Εμπιστοσύνη και Φήμη**:
    - **Δημιουργία Αξιοπιστίας**: Ενίσχυση της εμπιστοσύνης των γονέων και της κοινότητας στο σχολείο, αποδεικνύοντας ότι λαμβάνει σοβαρά την ασφάλεια και την προστασία των μαθητών.
    - **Φήμη του Σχολείου**: Προστασία της φήμης του σχολείου από τις αρνητικές συνέπειες που μπορεί να έχουν περιστατικά παραβίασης ασφάλειας ή διαρροής ευαίσθητων δεδομένων.

Η εφαρμογή μιας πολιτικής ασφάλειας στο διαδίκτυο βοηθά στην επίτευξη ενός ασφαλούς και παραγωγικού εκπαιδευτικού περιβάλλοντος, εξασφαλίζοντας ότι οι μαθητές μπορούν να επωφεληθούν από τις τεχνολογικές δυνατότητες με ασφάλεια και υπευθυνότητα.

➢ ***Ποιες είναι στα πλαίσια του σχολείου οι αρμοδιότητες του Υπεύθυνου Προστασίας Δεδομένων και Ασφάλειας στο διαδίκτυο;***

Ο Υπεύθυνος Προστασίας Δεδομένων και Ασφάλειας στο διαδίκτυο σε ένα σχολείο έχει κρίσιμο ρόλο στη διασφάλιση της ψηφιακής ασφάλειας και της προστασίας των προσωπικών δεδομένων των μαθητών, του προσωπικού και των γονέων. Οι κύριες αρμοδιότητές του περιλαμβάνουν:

1. **Συμμόρφωση με Κανονισμούς**:
    - Παρακολούθηση της συμμόρφωσης του σχολείου με την ισχύουσα νομοθεσία για την προστασία δεδομένων, όπως ο GDPR.
    - Παροχή συμβουλών και καθοδήγησης στη διοίκηση και το προσωπικό του σχολείου σχετικά με τις υποχρεώσεις τους σύμφωνα με τους κανονισμούς προστασίας δεδομένων.

2. **Ανάπτυξη Πολιτικών και Διαδικασιών**:
    - Σχεδιασμός, ανάπτυξη και εφαρμογή πολιτικών και διαδικασιών για την προστασία δεδομένων και την ασφάλεια στο διαδίκτυο.
    - Καθορισμός των μέτρων ασφαλείας για την προστασία των προσωπικών δεδομένων και την αποτροπή παραβιάσεων ασφαλείας.

3. **Εκπαίδευση και Ευαισθητοποίηση**:
    - Οργάνωση εκπαιδευτικών προγραμμάτων και σεμιναρίων για το προσωπικό, τους μαθητές και τους γονείς σχετικά με την ασφάλεια στο διαδίκτυο και την προστασία δεδομένων.
    - Δημιουργία και διανομή υλικού ευαισθητοποίησης σχετικά με τις βέλτιστες πρακτικές για την ασφάλεια στο διαδίκτυο.

4. **Διαχείριση Πρόσβασης και Δικτύου**:
    - Εφαρμογή και διαχείριση των πολιτικών πρόσβασης για μαθητές, προσωπικό και άλλους χρήστες του σχολικού δικτύου.
    - Παρακολούθηση και διαχείριση των συστημάτων ασφαλείας του σχολικού δικτύου, όπως firewall, antivirus, και συστήματα ανίχνευσης εισβολών.

5. **Προστασία και Διαχείριση Δεδομένων**:
    - Διασφάλιση της προστασίας των προσωπικών δεδομένων των μαθητών, του προσωπικού και των γονέων από μη εξουσιοδοτημένη πρόσβαση, αλλοίωση ή διαρροή.
    - Εφαρμογή τεχνικών και οργανωτικών μέτρων για την ασφάλεια των δεδομένων, όπως κρυπτογράφηση και τακτικά αντίγραφα ασφαλείας.

6. **Αντιμετώπιση Περιστατικών Ασφαλείας**:
    - Δημιουργία και εφαρμογή διαδικασιών για την αναγνώριση, αναφορά και αντιμετώπιση περιστατικών παραβίασης ασφαλείας.
    - Συντονισμός της ανταπόκρισης σε περιστατικά παραβίασης δεδομένων και αποκατάσταση της κανονικότητας.

7. **Συνεργασία με Αρχές και Φορείς**:
    - Συνεργασία με τις αρμόδιες εποπτικές αρχές και άλλους εξωτερικούς φορείς για θέματα προστασίας δεδομένων και ασφάλειας στο διαδίκτυο.
    - Αναφορά παραβιάσεων δεδομένων στις αρμόδιες αρχές και ενημέρωση των ενδιαφερομένων μερών.

8. **Διατήρηση Αρχείων και Τεκμηρίωση**:
    - Τήρηση και ενημέρωση αρχείων σχετικά με τις δραστηριότητες επεξεργασίας δεδομένων και την ασφάλεια στο διαδίκτυο.
    - Τεκμηρίωση των πολιτικών και των διαδικασιών ασφαλείας και προστασίας δεδομένων.

9. **Συνεχής Βελτίωση και Αναθεώρηση**:
    - Τακτική αξιολόγηση και αναθεώρηση των πολιτικών και των μέτρων ασφάλειας για την προσαρμογή σε νέες απειλές και τεχνολογικές εξελίξεις.
    - Συλλογή ανατροφοδότησης και προτάσεων βελτίωσης από το προσωπικό και τους μαθητές.

10. **Υποστήριξη στη Διοίκηση**:
    - Παροχή συμβουλών και υποστήριξης στη διοίκηση του σχολείου για θέματα ασφάλειας στο διαδίκτυο και προστασίας δεδομένων.
    - Συνεισφορά στη λήψη αποφάσεων που σχετίζονται με την ασφάλεια και την προστασία των δεδομένων στο σχολείο.

Ο ρόλος του Υπεύθυνου Προστασίας Δεδομένων και Ασφάλειας στο διαδίκτυο είναι θεμελιώδης για την εξασφάλιση ενός ασφαλούς και συμμορφούμενου εκπαιδευτικού περιβάλλοντος, όπου προστατεύονται τα προσωπικά δεδομένα και προάγεται η ασφαλής χρήση του διαδικτύου.

➢ *Το σύνολο των κανόνων και πρακτικών της Πολιτικής Ασφάλειας στο διαδίκτυο*

Η πολιτική ασφάλειας στο διαδίκτυο που εφαρμόζεται στο 18ο Δημοτικό Σχολείο Λάρισας περιλαμβάνει **ένα σύνολο κανόνων και πρακτικών** που στοχεύουν στην προστασία των μαθητών, του προσωπικού και των δεδομένων τους από διαδικτυακές απειλές. Αυτή η πολιτική αποσκοπεί στην ασφαλή χρήση του διαδικτύου και περιλαμβάνει τα εξής μέτρα:

1. **Εκπαίδευση και Ευαισθητοποίηση**:

   - Εκπαίδευση των μαθητών, στα πλαίσια του μαθήματος «Τεχνολογίες της Πληροφορικής και της Επικοινωνίας (Τ.Π.Ε)», σχετικά με την ασφαλή χρήση του διαδικτύου, τις διαδικτυακές απειλές και την αναγνώριση κακόβουλων ενεργειών.
   - **Οργάνωση σεμιναρίων** για το διδακτικό προσωπικό του σχολείου (**ενδοσχολική επιμόρφωση**) και παρουσίαση σχετικού υλικού με πρακτικές ασκήσεις (π.χ. Οδηγός για την Κυβερνοασφάλεια)
   - **Ενημερωτικές καμπάνιες** και δημιουργία υλικού (**βίντεο, φυλλάδια, αφίσες**) που ενημερώνει για την ασφάλεια στο διαδίκτυο.
   - Συμμετοχή του σχολείου σε εκπαιδευτικά προγράμματα (π.χ. **etwinning**) με στόχο την ενημέρωση σε θέματα διαδικτυακής ασφάλειας
   - Συμμετοχή στην Κοινότητα eSafety Label και στη διαδικασία πιστοποίησης σχολείων με την ετικέτα ψηφιακής ασφάλειας eSafety Label. Μέσω της αυτοαξιολόγησης ενισχύουμε περαιτέρω την ασφαλή χρήση του Διαδίκτυο στο σχολείου μας.
   - Συμμετοχή στις δράσεις της Ημέρας Ασφαλούς Διαδικτύου – Safer Internet Day **(SID)** με σκοπό την προώθηση της ασφαλής και θετικής χρήσης της ψηφιακής τεχνολογίας, ιδιαίτερα ανάμεσα σε παιδιά και νέους ανθρώπους.

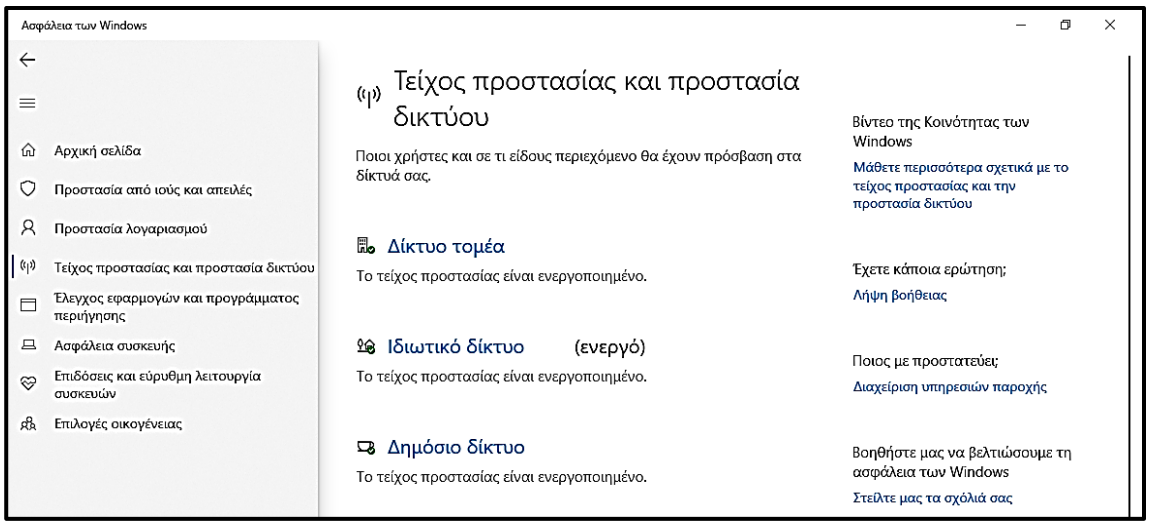
2. **Έλεγχος Πρόσβασης**:

   - Το Πανελλήνιο Σχολικό Δίκτυο (ΠΣΔ) **εφαρμόζει έλεγχο πρόσβασης μέσω φίλτρων περιεχομένου και λογισμικού ελέγχου για την αποτροπή πρόσβασης σε ακατάλληλο ή επικίνδυνο περιεχόμενο**. Στόχος είναι η θέσπιση ενός ασφαλούς περιβάλλοντος εργασίας που θα αποθαρρύνει ή θα αποτρέπει την πρόσβαση σε περιεχόμενο που συγκρούεται με θεμελιώδεις αρχές της ανθρώπινης αξιοπρέπειας. Χωρίς λογοκρισία και ασφυκτικούς περιορισμούς, στοχεύουμε στην εύρεση τρόπων διασφάλισης της αποκλειστικής χρήσης του Διαδικτύου στο σχολείο για εκπαιδευτικούς σκοπούς με αποτροπή πρόσβασης σε ακατάλληλο υλικό.

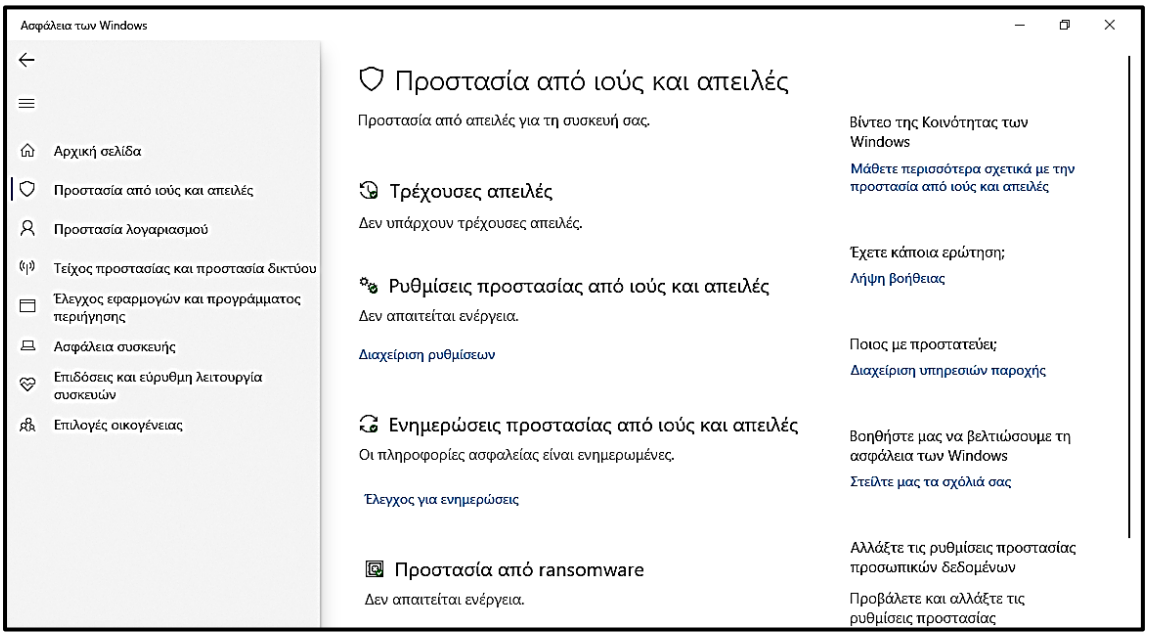
- Καθορισμός και εφαρμογή πολιτικών πρόσβασης που περιορίζουν την πρόσβαση σε συγκεκριμένους ιστοτόπους και διαδικτυακές υπηρεσίες, χωρίς όμως να αχρηστευτούν οι δυνατότητες του Διαδικτύου που μπορούν να χρησιμοποιηθούν για να διευκολύνουν την επικοινωνία, την ανταλλαγή απόψεων, την συνεργατικότητα και τη μαθησιακή διαδικασία.

3. **Ασφάλεια Δικτύου**:

- Χρήση **τείχους προστασίας** (Firewall) και λογισμικού ανίχνευσης και πρόληψης εισβολών (IDS/IPS) για την προστασία του σχολικού δικτύου από εξωτερικές απειλές.

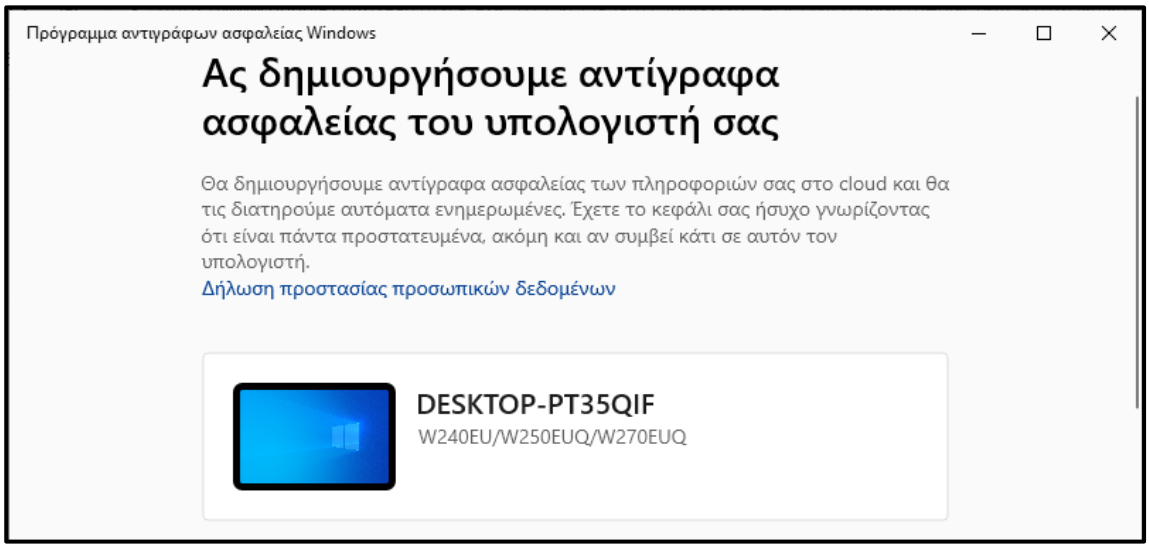


- Εγκατάσταση και τακτική ενημέρωση **λογισμικού προστασίας από ιούς** και κακόβουλο λογισμικό (Antivirus).



4. **Προστασία Δεδομένων**:

- Κρυπτογράφηση ευαίσθητων δεδομένων κατά την αποθήκευση και μετάδοση.
- Τακτική δημιουργία αντιγράφων ασφαλείας (Backup) των δεδομένων και ασφαλής αποθήκευσή τους σε **εξωτερικό σκληρό δίσκο (**External Hard Disk Drive**).**



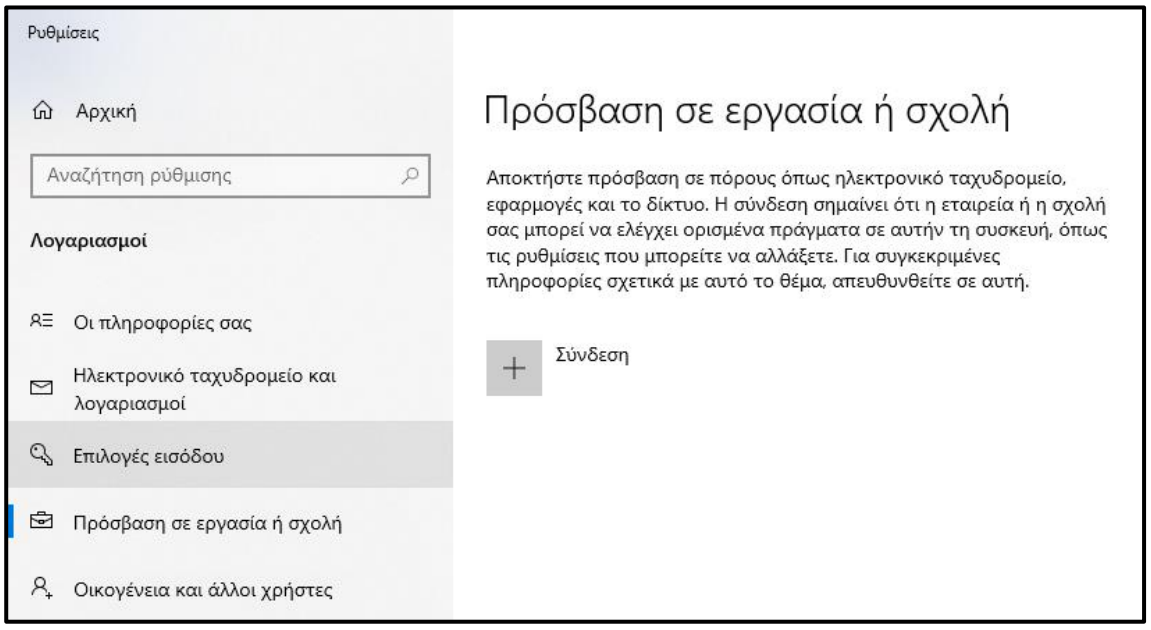
5. **Διαχείριση Κωδικών Πρόσβασης:**

- Εφαρμογή πολιτικών ισχυρών κωδικών πρόσβασης και τακτική αλλαγή τους.
- Εκπαίδευση των χρηστών στη δημιουργία και διαχείριση ασφαλών κωδικών πρόσβασης.
- Δημιουργία κωδικού που να περιέχει τουλάχιστον 8 (οκτώ) χαρακτήρες και να αποτελείται από γράμματα, αριθμούς, σύμβολα και σημεία στίξης.

- Εάν πρέπει να γράψετε τον κωδικό σας κάπου, αυτός θα πρέπει να φυλάσσεται μακριά από την συσκευή που δίνει πρόσβαση και να μην είναι σε ένα μεμονωμένο χαρτάκι.

6. Διαχείριση Λογαριασμών Χρηστών:

- Κάθε υπολογιστής του σχολείου διαθέτει ένα κύριο λογαριασμό **Διαχειριστή** και (τουλάχιστον) ένα απλό λογαριασμό **Χρήστη**, οι οποίοι προστατεύονται με κωδικούς πρόσβασης.
- Ο Διαχειριστής παρέχει **δικαιώματα πρόσβασης** στους απλούς Χρήστες και δεν επιτρέπει την εγκατάσταση πειρατικού ή επικίνδυνου λογισμικού, ενισχύοντας έτσι την ασφάλεια των υπολογιστών του σχολείου.



7. Χρήση αφαιρούμενων συσκευών

- Επιτρέπεται η χρήση αφαιρούμενων συσκευών (κάρτες μνήμης flash, φορητοί σκληροί δίσκοι, CD, DVD και USB sticks) μόνο όταν είναι απαραίτητο για τις εργασίες του σχολείου. (Σχετικές οδηγίες χρήσης δίνονται στους μαθητές κατά την ώρα του σχετικού μαθήματος πληροφορικής)
- Τα αφαιρούμενα μέσα πρέπει να ελέγχονται από λογισμικό προστασίας για ιούς (antivirus) για να αποφευχθεί η μόλυνση του συγκεκριμένου υπολογιστή ή ακόμα και του τοπικού δικτύου.

8. Προστασία ευαίσθητων δεδομένων:

- Οι κωδικοί του ηλεκτρονικού ταχυδρομείου είναι αυστηρά προσωπικοί και δεν διανέμονται μεταξύ μαθητών.
- Κατά την χρησιμοποίηση των διαδικτυακών εργαλείων Web 2.0 οι μαθητές πρέπει να κάνουν έξοδο ή αποσύνδεση (sign out) μετά το πέρας του μαθήματος ή της εργασίας τους

9. Αντιμετώπιση Απειλών και Περιστατικών:

- Δημιουργία και εφαρμογή σχεδίων δράσης για την αντιμετώπιση περιστατικών ασφάλειας, όπως παραβιάσεις δεδομένων ή επιθέσεις κακόβουλου λογισμικού.
- Ενημέρωση των αρμόδιων αρχών και των ενδιαφερόμενων μερών σε περίπτωση σοβαρού περιστατικού ασφάλειας.
- Στις περιπτώσεις που θα κάνετε χρήση του προσωπικού σας ηλεκτρονικού ταχυδρομείου, αν χρειαστεί να κατεβάσετε κάποιο αρχείο οποιασδήποτε μορφής
- Εάν εντοπίσετε κάποιο παράξενο αρχείο στο ηλεκτρονικό σας ταχυδρομείο να ενημερώσετε πρώτα τον υπεύθυνο της τάξης που βρίσκεστε θα πρέπει, πριν το ανοίξετε, να το ελέγξετε με το πρόγραμμα προστασίας από ιούς.

10. Χρήση των κινητών τηλεφώνων:

- Το ασύρματο δίκτυο (Wi-Fi) του σχολείου μας είναι απενεργοποιημένο και συνεπώς μη προσβάσιμο για κινητά τηλέφωνα. Η Πολιτική Ορθής Χρήσης παρέχει ένα αυστηρό πρωτόκολλο για τη χρήση των κινητών τηλεφώνων στο σχολείο βάσει και των οδηγιών του Υπουργείου και περιέχει ξεκάθαρες κατευθυντήριες οδηγίες για την κατοχή, τη χρήση κινητών τηλεφώνων στο σχολείο και τις συνέπειες παραβίασής της.
- Οι εκπαιδευτικοί δεν κάνουν χρήση των κινητών τους τηλεφώνων κατά τη διάρκεια της εκπαιδευτικής διαδικασίας εκτός εάν παραστεί ανάγκη ή η χρήση τους σχετίζεται με την υλοποίηση κάποιας δράσης.
- Δεν επιτρέπεται η κατοχή και χρήση κινητών τηλεφώνων στο σχολείο καθώς και κατά τη διάρκεια σχολικών εκδρομών και εορτών

11. Λήψη και δημοσίευση φωτογραφιών και βίντεο

- Υπάρχει ξεκάθαρη πολιτική με συγκεκριμένες κατευθυντήριες γραμμές από το Υπουργείο παιδείας για τις φωτογραφίες και τις εικόνες. Οι εκπαιδευτικοί, οι γονείς, οι μαθητές και η ευρύτερη σχολική κοινότητα είναι ενημερωμένοι και η πολιτική του σχολείου τους υπενθυμίζεται τακτικά με τη χρήση και της σχετικής Υπεύθυνης Δήλωσης Γονικής Συγκατάθεσης από το Πανελλήνιο Σχολικό Δίκτυο.
- μαθητές και εκπαιδευτικοί είναι ενήμεροι σχετικά με τις φωτογραφίες και τη χρήση των μέσων κοινωνικής δικτύωσης ενώ κανένας εκπαιδευτικός δεν διατηρεί στα προφίλ του επαφές με τους εν ενεργεία μαθητές του σχολείου μας.
- Ο εκπαιδευτικός που υλοποιεί προγράμματα (σχολικών δραστηριοτήτων, Erasmus+, eTwinning) είναι υποχρεωμένος να διανείμει στους μαθητές το σχετικό από το Πανελλήνιο Σχολικό Δίκτυο έντυπο γονικής συγκατάθεσης για τη λήψη και δημοσίευση φωτογραφιών και βίντεο
- Σε περίπτωση που οι γονείς δε συναινούν στη λήψη και δημοσίευση φωτογραφιών και βίντεο των παιδιών τους, ο εκπαιδευτικός είναι υποχρεωμένος να το λάβει υπόψη του κατά την υλοποίηση των σχετικών προγραμμάτων

12. Συμμετοχή στα Μέσα Κοινωνικής Δικτύωσης:

- Κανένας εκπαιδευτικός του σχολείου δεν επιτρέπεται να διατηρεί στα προφίλ του στα μέσα κοινωνικής δικτύωσης επαφές με τους εν ενεργεία μαθητές του σχολείου μας
- Συστήνεται στους εκπαιδευτικούς να μην εμπλέκονται σε συζητήσεις στα μέσα κοινωνικής δικτύωσης σε θέματα που αφορούν στη λειτουργία του σχολείου και διασύρουν τη φήμη του σχολείου
- Οι μαθητές δεν επιτρέπεται να χρησιμοποιούν στο χώρο του σχολείου λογαριασμούς τους στα μέσα κοινωνικής δικτύωσης
- Οι μαθητές δεν επιτρέπεται να αναπαράγουν υλικό που έχει δημιουργηθεί στο σχολείο στα μέσα κοινωνικής δικτύωσης
- Σε περίπτωση που κάποιος μαθητής υποστεί διαδικτυακή απειλή ή προσβολή καλείται να ενημερώσει τον εκπαιδευτικό της τάξης ή τους υπευθύνους της ομάδας Πολιτικής ασφάλειας του σχολείου

13. Πνευματικά δικαιώματα:

- Μαθητές και εκπαιδευτικοί είναι ενήμεροι για την πολιτική χρήσης εικόνων, μουσικής και βίντεο από το διαδίκτυο
- Οι μαθητές χρησιμοποιούν φωτογραφίες, μουσική και βίντεο από το διαδίκτυο που δεν υπόκεινται σε πνευματικά δικαιώματα

14. Ενσωμάτωση της ψηφιακής ασφάλειας στο σχολικό πρόγραμμα

- Η ψηφιακή ασφάλεια διδάσκεται στο σχολείο μας κατά τη διάρκεια του μαθήματος της Πληροφορικής, κατά τη διάρκεια υλοποίησης προγραμμάτων (σχολικών δραστηριοτήτων, Erasmus+, eTwinning) καθώς και αφορμής δοθείσης με την εξέταση κάποιας σχετικής ενότητας από τα σχολικά εγχειρίδια.
- Αρκετοί από τους εκπαιδευτικούς του σχολείου μας λαμβάνουν τακτική επιμόρφωση στην ψηφιακή ασφάλεια, ενώ οι μαθητές μας λαμβάνουν ειδική καθοδήγηση με την εξέταση κάποιου σχετικού θέματος.
- Η συνεχής επαγγελματική ανάπτυξη των εκπαιδευτικών είναι σχετική και αντιμετωπίζει τρέχοντα θέματα και τάσεις για την ψηφιακή ασφάλεια, ενώ η εκπαίδευση στην ψηφιακή ασφάλεια παρέχεται από αναγνωρισμένο φορέα στον τομέα της Ασφάλειας στο Διαδίκτυο. (EUN Academy, SaferInternet)

15. Ενημέρωση κηδεμόνων και γονέων

- Υλικό σχετικό με την ψηφιακή ασφάλεια είναι αναρτημένη στην **ιστοσελίδα του σχολείου,** ενώ οι γονείς καλούνται να αναλάβουν ενεργό ρόλο για την ψηφιακή ασφάλεια του σχολείου μέσω συστάσεων προς τα παιδιά τους
- Οι γονείς ενημερώνονται σε θέματα ψηφιακής ασφάλειας με την αποστολή της **έγγραφης δήλωσης γονικής συγκατάθεσης** σχετικά με τη δημοσίευση φωτογραφιών ή βίντεο στην ιστοσελίδα του σχολείου

16. Συνεχής Παρακολούθηση και Αξιολόγηση:

- Συνεχής παρακολούθηση του δικτύου και των συστημάτων για ύποπτες δραστηριότητες ή παραβιάσεις.
- Τακτική αξιολόγηση των πολιτικών και των μέτρων ασφάλειας για την προσαρμογή σε νέες απειλές και τεχνολογίες.
- Εξασφάλιση ότι η πολιτική ασφάλειας στο διαδίκτυο συμμορφώνεται με τις νομοθεσίες και τους κανονισμούς.

Αυτά τα μέτρα αποτελούν τη βάση της ολοκληρωμένης πολιτικής ασφάλειας στο διαδίκτυο στο 18ο Δ.Σ Λάρισας, εξασφαλίζοντας ένα ασφαλές εκπαιδευτικό περιβάλλον για όλους τους εμπλεκόμενους.

Πηγές - ιστότοποι:

- https://saferinternet4kids.gr/
- https://www.saferinternet.gr/
- https://internet-safety.sch.gr/
- https://www.safeline.gr/
- https://www.cyberkid.gov.gr/
- https://www.saferinternetday.org/