

POLITYKA BEZPIECZEŃSTWA CYFROWEGO W SZKOLE PODSTAWOWEJ NR 1 Z ODDZIAŁAMI INTEGRACYJNYMI IM. M.SKŁODOWSKIEJ- CURIE W LUBINIE

1. Wstęp

Celem niniejszej polityki jest zapewnienie bezpiecznego, odpowiedzialnego i zgodnego z prawem korzystania z technologii cyfrowych w szkole przez uczniów, nauczycieli oraz pracowników obsługi i administracji. Dokument określa zasady ochrony danych, bezpieczeństwa informacji oraz właściwego zachowania w środowisku cyfrowym.

2. Zakres polityki

Polityka dotyczy:

- wszystkich uczniów,
- nauczycieli i pracowników szkoły,
- osób korzystających z infrastruktury IT szkoły (np. gości),
- wszystkich urządzeń szkolnych oraz prywatnych używanych na terenie szkoły.

3. Zasady ogólne

1. Korzystanie z zasobów cyfrowych szkoły powinno odbywać się wyłącznie w celach edukacyjnych.
2. Każdy użytkownik jest odpowiedzialny za swoje działania w sieci.
3. Zabrania się podejmowania działań mogących naruszyć bezpieczeństwo systemów informatycznych.
4. Należy szanować prywatność innych użytkowników.

4. Bezpieczeństwo danych

1. Dane osobowe muszą być chronione zgodnie z obowiązującymi przepisami prawa.
2. Użytkownicy powinni:
 - stosować silne hasła i nie udostępniać ich innym,
 - regularnie zmieniać hasła,
 - wylogowywać się po zakończeniu pracy.
3. Zabrania się kopiowania i udostępniania danych bez zgody uprawnionych osób.

Bezpieczeństwo danych w szkole to również kontrola dostępu:

- Każdy uczeń i pracownik powinien mieć własne konto (login + hasło)
- Dostęp do danych (np. dziennika elektronicznego) tylko dla uprawnionych osób
- Regularne usuwanie lub blokowanie nieaktywnych kont
- Wymaganie silnych haseł (min. 10–12 znaków)
- Obowiązkowa zmiana haseł co określony czas
- Wdrożenie uwierzytelniania dwuskładnikowego
- Komputery zabezpieczone hasłem
- Automatyczne blokowanie ekranu
- Instalacja tylko zatwierdzonego oprogramowania
- Program antywirusowy i zaporę sieciową
- Sieć Wi-Fi zabezpieczona hasłem (nie publiczna)
- Oddzielna sieć dla uczniów i pracowników
- Filtrowanie treści (blokowanie niebezpiecznych stron)
- Przestrzeganie zasad RODO
- Przechowywanie danych uczniów tylko tam, gdzie to konieczne
- Ograniczony dostęp do dokumentów (np. ocen, danych kontaktowych)
- Szkolenia dla uczniów i nauczycieli

- Nieotwieranie podejrzanych wiadomości
- Regularne tworzenie backupów danych szkoły
- Przechowywanie kopii w bezpiecznym miejscu (np. chmura lub serwer offline)
- Lekcje o bezpieczeństwie cyfrowym
- Nauka:
 - ochrony haseł
 - rozpoznawania zagrożeń
 - odpowiedzialnego korzystania z Internetu

Regularne aktualizacje systemów i oprogramowania

Stały nadzór administratora IT

Monitorowanie sieci (wykrywanie zagrożeń)

5. Korzystanie z Internetu

1. Dostęp do Internetu w szkole służy wyłącznie celom edukacyjnym.
2. Zabrania się:
 - odwiedzania stron o treściach nieodpowiednich (np. przemoc, pornografia),
 - pobierania nielegalnego oprogramowania,
 - rozpowszechniania nieprawdziwych informacji.
3. Szkoła może monitorować aktywność w sieci w celu zapewnienia bezpieczeństwa.

6. Cyberprzemoc i zachowania niepożądane

1. Zakazane są wszelkie formy cyberprzemocy, w tym:
 - obrażanie innych użytkowników,
 - publikowanie kompromitujących materiałów,
 - nękanie w sieci.
2. Każdy przypadek naruszenia należy zgłosić nauczycielowi lub dyrekcji.
3. Szkoła podejmuje działania wychowawcze i dyscyplinarne wobec sprawców.

7. Urządzenia cyfrowe

1. Uczniowie mogą korzystać z własnych urządzeń tylko za zgodą nauczyciela.
2. Urządzenia muszą być zabezpieczone (np. hasłem, aktualnym oprogramowaniem).
3. Zabrania się instalowania nieautoryzowanego oprogramowania na sprzęcie szkolnym.

8. Ochrona przed zagrożeniami

1. Należy zachować ostrożność przy:
 - otwieraniu wiadomości e-mail od nieznanych nadawców,
 - klikaniu w podejrzaną linki,
 - pobieraniu plików z Internetu.
2. W przypadku podejrzenia zagrożenia należy niezwłocznie zgłosić problem administratorowi IT.

9. Szkolenia i edukacja

1. Szkoła zapewnia regularne szkolenia z zakresu bezpieczeństwa cyfrowego.
2. Uczniowie są edukowani w zakresie:
 - ochrony danych osobowych,
 - bezpiecznego korzystania z Internetu,
 - rozpoznawania zagrożeń cyfrowych.

10. Odpowiedzialność i konsekwencje

1. Naruszenie zasad polityki może skutkować:
 - ograniczeniem dostępu do zasobów cyfrowych,
 - konsekwencjami wychowawczymi,
 - odpowiedzialnością prawną.
2. Każdy użytkownik zobowiązany jest do zapoznania się z dokumentem i jego przestrzegania.

11. Postanowienia końcowe

1. Polityka wchodzi w życie z dniem zatwierdzenia przez dyrekcję szkoły.
2. Wszelkie zmiany wymagają zatwierdzenia przez dyrekcję.
3. Każdy pracownik szkoły jest zobowiązany do przestrzegania Polityki Bezpieczeństwa Cyfrowego.
4. Niezastosowanie się do postanowień niniejszego dokumentu i naruszenie procedur zapewniania bezpieczeństwa internetowego dla uczniów jest traktowane jako naruszenie obowiązków służbowych, skutkujące konsekwencjami prawnymi.

Podpis dyrektora:

DYREKTOR SZKOŁY

mgr Iwona Kędzierska