

POLITYKA BEZPIECZEŃSTWA INTERNETOWEGO W SZKOLE PODSTAWOWEJ NR 5 Z ODDZIAŁAMI INTEGRACYJNYMI W KĘTRZYNIE

I. Postanowienia wstępne.

1. „Polityka bezpieczeństwa internetowego” wskazuje działania, które są podejmowane w szkole w celu zapewnienia bezpieczeństwa uczniom korzystającym z nowych technologii informatycznych zarówno w szkole, jak i poza nią oraz zapobieganiu cyberprzemocy wśród uczniów.

2. Ilekcioć w dokumencie jest mowa o:

- 1) *Administrator* – rozumie się przez to osobę/osoby wyznaczoną przez Dyrektora szkoły do zarządzania systemami informatycznymi,
- 2) *sieci publicznej* - rozumie się przez to sieć telekomunikacyjną, wykorzystywaną głównie do świadczenia publicznie dostępnych usług telekomunikacyjnych,
- 3) *systemie informatycznym* - rozumie się przez to zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych,
- 4) *szkole* - rozumie się przez to Szkołę Podstawową Nr 5 z Oddziałami Integracyjnymi im. Macieja Kalenkiewicza „Kotwiczka” w Kętrzynie
- 5) *użytkownika* - rozumie się przez to uczniów i nauczycieli korzystających z dostępnych w szkole sieci internetowych;
- 6) *cyberprzemocy (agresja elektroniczna)* - rozumie się przez to stosowanie przemocy poprzez: prześladowane, zastraszanie, nękanie, wyśmiewanie innych osób z wykorzystaniem Internetu i narzędzi typu elektronicznego takich jak sms, witryny internetowe, fora dyskusyjne w Internecie i inne

3. „Polityka bezpieczeństwa internetowego” określa zbiór działań podejmowanych w szkole w celu:

- 1) zadbania o ochronę uczniowskich stanowisk komputerowych;
- 2) zwiększenie świadomości społeczności szkolnej na temat zagrożeń, jakie niosą ze sobą technologie komputerowe i informacyjne;
- 3) kształtowanie odpowiedniej postawy w zakresie korzystania z nowoczesnych technologii informacyjnych

II. Zadania do realizacji:

L.p.	Zadanie	Sposób realizacji	Odpowiedzialni
1.	Zabezpieczenie	1. Zainstalowanie bramek przed dostępem do	Administrator

	uczniowskich stanowisk komputerowych	niepożądanych treści i portali. 2. Wyposażenie stanowisk w oprogramowanie antywirusowe.	Dyrektor, nauczyciele
2.	Edukacja uczniów i rodziców	1. Zapoznavanie uczniów i rodziców z zagadnieniami: ochrony danych osobowych, w tym regulacjami prawnymi wynikającymi z konstytucji RP i Ustawy o ochronie danych; cyberprzemoc jako przestępstwo przeciwko prawu, rodzaje zachowań zachowania kwalifikowane jako cyberprzemoc. ochrona własnego wizerunku i wizerunku innych osób; pojęcie pozornej anonimowości w Internecie; prawa autorskie, ochrona praw autorskich; co to jest kradzież własności intelektualnej i dzieł chronionych prawami autorskimi; co to jest kradzież tożsamości; zagrożenia płynące z czatów, komunikatorów internetowych i portali społecznościowych; „złośliwe” oprogramowania; zorganizowanie Dnia Bezpiecznego Internetu - konkursy, pogadanki, wystawy, prelekcje (czas realizacji - ms. Luty). 2. Poinformowanie uczniów i rodziców o sposobach radzenia z zachowaniami przemocy elektronicznej, rozpoznawaniu cyberprzemocy oraz postępowania w przypadku jej wystąpienia. 3. Przygotowanie gablotki lub slajdów z informacjami z zagrożeniach w Internecie i cyberprzemocy.	Wychowawcy klas, Nauczyciele w trakcie realizacji podstawy programowej kształcenia ogólnego

3.	Zadania dla Rady Pedagogicznej	Zapoznanie Rady Pedagogicznej z Polityką Bezpieczeństwa Internetowego. Realizacja na zajęciach z wychowawcą w ramach Programu Profilaktyki tematyki cyberprzemocy i jej skutków. Informowanie rodziców o potrzebie kontroli dostępu do Internetu oraz innych nośników elektronicznych używanych przez ich dzieci. Zaplanować szeroką działalność informacyjną o sposobach pomocy dzieciom, które doznały cyberprzemocy.	Dyrektor, nauczyciele pedagog
4.	Reakcja na zjawisko cyberprzemocy	Pracowanie procedur reagowania w szkole na zjawiska cyberprzemocy. Podjęcie interwencji w każdym przypadku ujawnienia lub podejrzenia cyberprzemocy. Przekazanie uczniom i rodzicom informacji o możliwości i potrzebie poinformowania Dyrektora szkoły, pedagoga lub wychowawcy o zastosowaniu wobec niego przemocy.	Dyrektor, nauczyciele

III. Postanowienia końcowe.

1. Każdy pracownik szkoły jest zobowiązany do przestrzegania Polityki Bezpieczeństwa Internetowego.
2. Niezastosowanie się do postanowień niniejszego dokumentu i naruszenie procedur zapewniania bezpieczeństwa internetowego dla uczniów jest traktowane jako ciężkie naruszenie obowiązków służbowych, skutkujące poważnymi konsekwencjami prawnymi.
3. Polityka bezpieczeństwa, wchodzi w życie z dniem 30 sierpnia 2016r.