Zespół Szkół im. Lotników Polskich
w Płocicznie-Tartak

Polityka bezpieczeństwa internetowego

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. Ilektoć w dokumencie jest mowa o:
   a) *administratorze bezpieczeństwa informacji* – rozumie się przez to osobę, której dyrektor szkoły powierzył pełnienie obowiązków administratora bezpieczeństwa informacji,
   b) *sieci publicznej* – rozumie się przez to sieć telekomunikacyjną, wykorzystywaną głównie do świadczenia publicznie dostępnych usług telekomunikacyjnych,
   c) *systemie informatycznym* – rozumie się przez to zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych,
   d) *szkole* – rozumie się przez to Zespół Szkół im. Lotników Polskich w Płocicznie-Tartak,
   e) *użytkowniku* – rozumie się przez to uczniów i nauczycieli korzystających z dostępnych w szkole sieci internetowych;
   f) *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:
   a) zadbania o ochronę uczniowskich stanowisk komputerowych;
   b) zwiększenie świadomości społeczności szkolnej na temat zagrożeń, jakie niosą ze sobą technologie komputerowe i informacyjne;
   c) kształtowanie odpowiedniej postawy w zakresie korzystania z nowoczesnych technologii informacyjnych

II. Zadania do realizacji:

Zadanie	Sposób realizacji	Odpowiedzialni
Zabezpieczenie uczniowskich stanowisk komputerowych	1. Zainstalowanie bramek przed dostępem do niepożądanych treści i portali. 2. Wyposażenie stanowisk w programów antywirusowe.	Administrator ABI Dyrektor, nauczyciele
Zadania dla Rady Pedagogicznej	1. Zapoznanie Rady Pedagogicznej z Polityką Bezpieczeństwa Internetowego. 2. Realizacja na zajęciach z wychowawcą w ramach Programu Profilaktyki tematyki cyberprzemocy i jej skutków. 3. Uświadamianie rodzicom potrzeby kontroli dostępu do Internetu oraz innych nośników elektronicznych używanych przez ich dzieci. 4. Zaplanowanie szerokiej działalności informacyjnej o sposobach pomocy dzieciom, które doznały cyberprzemocy: a) konsekwentne reagowanie na zgłaszane problemy oraz zaistniałe incydenty. b) przeszkolenie Rady Pedagogicznej dotyczące cyberprzemocy c) zachęcanie do poruszania tematyki bezpieczeństwa dzieci w sieci, oraz włączania tej problematyki do programów zajęć	Dyrektor Wychowawcy Pedagog Wychowawcy Pedagog
Reakcja na zjawisko cyberprzemocy	1. Opracowanie procedur reagowania w szkole na zjawiska cyberprzemocy. 2. Podejmowanie interwencji w każdym przypadku ujawnienia lub podejrzenia cyberprzemocy. 3. Przekazanie uczniom i rodzicom informacji o możliwości i potrzebie poinformowania Dyrektora szkoły, pedagoga lub wychowawcy o zastosowaniu wobec niego przemocy .	Dyrektor, nauczyciele Dyrektor, nauczyciele Wychowawcy, nauczyciele

Edukacja uczniów i rodziców	1. Zapoznawanie uczniów i rodziców z zagadnieniami: a) ochrony danych osobowych, w tym regulacjami prawnymi wynikającymi z konstytucji RP i Ustawy o ochronie danych; b) cyberprzemoc jako przestępstwo przeciwko prawu, rodzaje zachowań zachowania kwalifikowane jako cyberprzemoc. c) ochrona własnego wizerunku i wizerunku innych osób; d) pojęcie pozornej anonimowości w Internecie; e) prawa autorskie, ochrona praw autor-skich; f) co to jest kradzież własności intelektualnej i dzieł chronionych prawami autorskimi; g) co to jest kradzież tożsamości; h) zagrożenia płynące z czatów, komunikatorów internetowych i portali społecznościowych; i) złośliwe" oprogramowania; j) zorganizowanie Dnia Bezpiecznego Internetu – konkursy, pogadanki, wystawy, prelekcje.	Wychowawcy klas, nauczyciele w trakcie realizacji podstawy programowej kształcenia ogólnego
	2. Poinformowanie uczniów i rodziców o sposobach radzenia z zachowaniami przemocy elektronicznej, rozpoznawaniu cyberprzemocy oraz postępowania w przypadku jej wystąpienia.	Pedagog Wychowawcy klas
	3. Aktywne włączanie rodziców we wszystkie działania podejmowane przez szkołę	Pedagog
	4. Organizacja szkoleń, spotkań informacyjnych dotyczących tematu bezpieczeństwa internetowego.	Pedagog Wychowawcy klas

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 internetowego wchodzi w życie z dniem 1 września 2014 roku