

POLITYKA BEZPIECZEŃSTWA INTERNETOWEGO W Szkole Podstawowej im. Jana Pawła II w Lubatowej

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:

- 1) *administratorze bezpieczeństwa informacji* – rozumie się przez to osobę, której dyrektor szkoły powierzył pełnienie obowiązków administratora bezpieczeństwa informacji,
- 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 im. Jana Pawła II w Lubatowej,
- 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) zwiększenia 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 uczniowskich stanowisk komputerowych	1. Zainstalowanie bramek przed dostępem do niepożądanych treści i portali. 2. Wyposażenie stanowisk w programów antywirusowe.	Administrator ABI, Dyrektor, nauczyciele

2.	Edukacja uczniów i rodziców	<p>1. Zapoznanie uczniów i rodziców z zagadnieniami:</p> <ul style="list-style-type: none"> 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 autorskich; 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. <p>2. Poinformowanie uczniów i rodziców o sposobach radzenia z zachowaniami przemocy elektronicznej, rozpoznawaniu cyberprzemocy oraz postępowania w przypadku jej wystąpienia.</p> <p>3. Przygotowanie gablotki z informacjami o zagrożeniach w Internecie i cyberprzemocy.</p>	<p>Wychowawcy klas, Nauczyciele w trakcie realizacji podstawy programowej kształcenia ogólnego</p>
3.	Zadania dla Rady Pedagogicznej	<p>1. Zapoznanie Rady Pedagogicznej z Polityką Bezpieczeństwa Internetowego.</p> <p>2. Realizacja na zajęciach z wychowawcą w ramach Programu Profilaktyki tematyki cyberprzemocy i jej skutków.</p> <p>3. Uświadamianie rodzicom potrzeby kontroli dostępu do Internetu oraz innych nośników elektronicznych używanych przez ich dzieci.</p> <p>4. Zaplanować szeroką działalność</p>	<p>Dyrektor, nauczyciele pedagog</p>

		informacyjną o sposobach pomocy dzieciom, które doznały cyberprzemocy.	
4.	Reakcja na zjawisko cyberprzemocy	<ol style="list-style-type: none"> 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

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 1 września 2014 roku.

.....
(podpis dyrektora)