*załącznik nr 1/2016/2017*
*do Programu Wychowawczego*

# POLITYKA BEZPIECZEŃSTWA INTERNETOWEGO
# w Zespole Szkół nr 4 im. Generała Stefana ,,Grota" Roweckiego w Mrągowie

## 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.** Ilekroć 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 Zespół Szkół nr 4 im. Generała Stefana ,,Grota" Roweckiego
5) *użytkowniku* – 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 uczniowskich stanowisk komputerowych | 1. Zainstalowanie bramek przed dostępem do niepożądanych treści i portali.<br>2. Wyposażenie stanowisk w programy antywirusowe. | Administrator ABI,<br>Dyrektor, nauczyciele |

| | | | |
|---|---|---|---|
| 2. | Edukacja uczniów i rodziców | 1. Zapoznawanie uczniów i rodziców z zagadnieniami:<br>a) ochrony danych osobowych, w tym regulacjami prawnymi wynikającymi z konstytucji RP i Ustawy o ochronie danych;<br>b) cyberprzemoc jako przestępstwo przeciwko prawu, rodzaje zachowań zachowania kwalifikowane jako cyberprzemoc.<br>c) ochrona własnego wizerunku i wizerunku innych osób;<br>d) pojęcie pozornej anonimowości w Internecie;<br>e) prawa autorskie, ochrona praw autor-skich;<br>f) co to jest kradzież własności intelektualnej i dzieł chronionych prawami autorskimi;<br>g) co to jest kradzież tożsamości;<br>h) zagrożenia płynące z czatów, komunikatorów internetowych i portali społecznościowych;<br>i) „ złośliwe” oprogramowania;<br>j) zorganizowanie Dnia Bezpiecznego Internetu – konkursy, pogadanki, wystawy, prelekcje.<br><br>2. Poinformowanie uczniów i rodziców o sposobach radzenia z zachowaniami przemocy elektronicznej, rozpoznawaniu cyberprzemocy oraz postępowania w przypadku jej wystąpienia.<br><br>3. Przygotowanie gablotki z informacjami z zagrożeniach w Internecie i cyberprzemocy. | Wychowawcy klas,<br><br>Nauczyciele w trakcie realizacji podstawy programowej kształcenia ogólnego |
| 3. | Zadania dla Rady Pedagogicznej | 1. Zapoznanie Rady Pedagogicznej z Polityką Bezpieczeństwa Internetowego.<br><br>2. Realizacja na zajęciach z wychowawcą w ramach Programu Profilaktyki tematyki cyberprzemocy i jej skutków.<br><br>3. Uświadamianie rodzicom potrzeby kontroli dostępu do Internetu oraz innych nośników elektronicznych używanych przez ich dzieci.<br><br>4. Zaplanować szeroką działalność informacyjną o sposobach pomocy | Dyrektor,<br><br>nauczyciele<br><br>pedagog |

| | | | |
|---|---|---|---|
| | | dzieciom, które doznały cyberprzemocy. | |
| 4. | Reakcja na zjawisko cyberprzemocy | 1. Opracowanie procedur reagowania w szkole na zjawiska cyberprzemocy.<br><br>2.Podejmowanie interwencji w każdym przypadku ujawnienia lub podejrzenia cyberprzemocy.<br><br>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 14.XI.2016r.

Mrągowo, 14.XI.2016r.

*mgr Edward Suchan*
/ podpis dyrektora/