Polityka Bezpieczeństwa Internetowego

Zespołu Szkół w Goleniowie

załącznik do Programu Wychowawczego

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:
   - *Administratorze bezpieczeństwa informacji* – rozumie się przez to osobę, której dyrektor szkoły powierzył pełnienie obowiązków administratora bezpieczeństwa informacji,
   - *Sieci publicznej* – rozumie się przez to sieć telekomunikacyjną, wykorzystywaną głównie do świadczenia publicznie dostępnych usług telekomunikacyjnych,
   - *Systemie informatycznym* – rozumie się przez to zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych,
   - *Szkole* – rozumie się przez to Zespół Szkół w Goleniowie,
   - *Użytkowniku* – rozumie się przez to uczniów i nauczycieli korzystających z dostępnych w szkole sieci internetowych,
   - *Cyberprzemocy (agresja elektroniczna)* – rozumie się przez to stosowanie przemocy poprzez: prześladowanie, 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:
   - Zadbania o ochronę uczniowskich stanowisk komputerowych,
   - Zwiększenia świadomości społeczności szkolnej na temat zagrożeń, jakie niosą ze sobą technologie komputerowe i informacyjne,
   - Kształtowania odpowiedniej postawy w zakresie korzystania z nowoczesnych technologii informacyjnych.

II **Zadania do realizacji:**

Lp.	Zadanie	Sposób realizacji	Odpowiedzialni
1.	Zabezpieczenie uczniowskich stanowisk	1.Zainstalowanie bramek przed dostępem do niepożądanych treści i portali	Administrator

	komputerowych	2.Wyposażenie stanowisk w programy antywirusowe	Dyrektor, nauczyciele
2.	Edukacja uczniów i rodziców	1.Zapoznanie uczniów i rodziców z zAgadnieniami: - ochrona danych osobowych, w tym regulacje prawne wynikające z Konstytucji RP i Ustawy o ochronie danych; -cyberprzemoc jako przestępstwo przeciwko prawu, rodzaje zachowań 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 Bezpieczeństwa Internetowego – konkursy, pogadanki, wystawy, prelekcje; 2.Poinformowanie uczniów i rodziców o sposobach radzenia z zachowaniami przemocy elektronicznej, rozpoznawaniu cyberprzemocy oraz postępowania w przypadku jej wystąpienia.	Wychowawcy klas Nauczyciele w trakcie realizacji podstawy programowej kształcenia ogólnego

		3.Przygotowanie gazetki z informacjami o zagrożeniach w Internecie i cyberprzemocy.	
3.	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.Uświadomienie rodzicom potrzeby kontroli dostępu do Internetu oraz innych nośników elektronicznych używanych przez ich dzieci. 4.Zaplanowanie działalności informacyjnej o sposobach pomocy dzieciom, które doznały cyberprzemocy	Dyrektor Wychowawcy Wychowawcy Pedagog
4.	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 pedagoga lub wychowawcy o zastosowaniu wobec niego cyberprzemocy.	Pedagog Pedagog Wychowawcy

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 konsekwencjami prawnymi.

3. Przedstawiono Radzie Rodziców dnia 16 lutego 2016 r.

4. Rada Rodziców pozytywnie zaopiniowała Politykę Bezpieczeństwa Internetowego (protokół RR ..... 2016) .

5. Przedstawiono Radzie Pedagogicznej dnia 23 lutego 2016 r.

6. Rada Pedagogiczna pozytywnie zaopiniowała Politykę Bezpieczeństwa Internetowego (protokół RP ..... 2015/2016) .

……

Podpis dyrektora