POLITYKA BEZPIECZEŃSTWA INTERNETOWEGO
W ZESPOLE SZKÓŁ Zawodowych nr 3 im. Kardynała Stefana Wyszyńskiego

w Ostrołęce

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 Zespół Szkół Zawodowych nr 3 im. Kardynała Stefana Wyszyńskiego Nr 3 w Ostrołęce
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	1. Zainstalowanie bramek przed dostępem do	Administrator

	uczniowskich stanowisk komputerowych	niepożądanych treści i portali. 2. Wyposażenie stanowisk w programów antywirusowe.	ABI, Dyrektor, nauczyciele
2.	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 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. 2. Poinformowanie uczniów i rodziców o sposobach radzenia z zachowaniami przemocy elektronicznej, rozpoznawaniu cyberprzemocy oraz postępowania w przypadku jej wystąpienia. 3. Przygotowanie gablotki z informacjami z zagrożeniach w Internecie i cyberprzemocy.	Wychowawcy klas, Nauczyciele w trakcie realizacji podstawy programowej kształcenia ogólnego i zawodowego

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. Uświadamianie rodzicom potrzeby kontroli dostępu do Internetu oraz innych nośników elektronicznych używanych przez ich dzieci. 4. Zaplanować szeroką działalność informacyjną o sposobach pomocy dzieciom, które doznały cyberprzemocy.	Dyrektor, nauczyciele 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 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 **15 września 2016 roku**