

POLITYKA BEZPIECZEŃSTWA INTERNETOWEGO W ZESPOLE SZKÓŁ OGÓLNOKSZTAŁCĄCYCH W STRZELINIE

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 (P. A. Ziółkowski),
- 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 Ogólnokształcących w Strzelinie,
- 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) 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. 2. Wyposażenie stanowisk w programów | Administrator ABI, Dyrektor, nauczyciele |

| | | | |
|----|--------------------------------|---|---|
| | | antywirusowe. | |
| 2. | Edukacja uczniów i rodziców | <p>1. Zapoznanie uczniów i rodziców z zagadnieniami:</p> <p>a) ochrony danych osobowych, w tym regulacjami prawnymi wynikającymi z konstytucji RP i Ustawy o ochronie danych;</p> <p>b) cyberprzemoc jako przestępstwo przeciwko prawu, rodzaje zachowań zachowania kwalifikowane jako cyberprzemoc.</p> <p>c) ochrona własnego wizerunku i wizerunku innych osób;</p> <p>d) pojęcie pozornej anonimowości w Internecie;</p> <p>e) prawa autorskie, ochrona praw autorskich;</p> <p>f) co to jest kradzież własności intelektualnej i dzieł chronionych prawami autorskimi;</p> <p>g) co to jest kradzież tożsamości;</p> <p>h) zagrożenia płynące z czatów, komunikatorów internetowych i portali społecznościowych;</p> <p>i) „złośliwe” oprogramowania;</p> <p>j) zorganizowanie Dnia Bezpiecznego Internetu – konkursy, pogadanki, wystawy, prelekcje.</p> <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 z zagrożeniami w Internecie i cyberprzemocy.</p> | <p>Wychowawcy klas,</p> <p>Nauczyciele w trakcie realizacji podstawy programowej kształcenia ogólnego</p> |
| 3. | Zadania dla Rady Pedagogicznej | 1. Zapoznanie Rady Pedagogicznej z Polityką Bezpieczeństwa Internetowego. | Dyrektor, |

