Załącznik nr 6.

do Polityki ochrony dzieci przed krzywdzeniem w Sz. P. im. F. Świebockiego w Barcicach

Zasady bezpiecznego korzystania z Internetu i mediów elektronicznych

I. Potencjalne zagrożenia

1. Do potencjalnych zagrożeń płynących z użytkowania sieci w szkole należy zaliczyć:
   a) dostęp do treści niezgodnych z celami wychowania i edukacji (narkotyki, przemoc, pornografia, hazard),
   b) działalność innych użytkowników zagrażająca dobru uczniów,
   c) oprogramowanie umożliwiające śledzenie i pozyskanie danych osobowych użytkowników szkolnej sieci.

II. Zasady korzystania z urządzeń elektronicznych z dostępem do Internetu

1. Infrastruktura sieciowa szkoły umożliwia dostęp do Internetu, zarówno personelowi, jak i uczniom w czasie zajęć.
2. Rozwiązania organizacyjne na poziomie szkoły bazują na aktualnych standardach bezpieczeństwa.
3. Na wszystkich komputerach z dostępem do Internetu na terenie szkoły monitorowany jest ruch sieciowy.
4. W szkole wyznaczony jest pracownik odpowiedzialny za bezpieczeństwo sieci.
5. Do obowiązków pracownika, o którym mowa w pkt. 4 należą:
   a) zabezpieczenie sieci internetowej przed niebezpiecznymi treściami;
   b) monitorowanie ruchu sieciowego;
   c) zgłaszanie nieetycznych incydentów do CERT.
6. Na terenie szkoły dostęp ucznia do internetu możliwy jest pod nadzorem nauczyciela na zajęciach lekcyjnych z dostępem do komputera.

7. Nauczyciel ma obowiązek informowania dzieci o zasadach bezpiecznego korzystania z internetu. Personel placówki czuwa także nad bezpieczeństwem korzystania z internetu przez dzieci podczas lekcji.
8. Korzystanie z multimediów, internetu i programów użytkowych podczas zajęć lekcyjnych służy wyłącznie celom informacyjnym i edukacyjnym.
9. Uczeń obsługuje sprzęt komputerowy zgodnie z zaleceniami nauczyciela, z obowiązującym regulaminem pracowni informatycznej.
10. Użytkownikowi komputera zabrania się:

a) instalowania oprogramowania oraz dokonywania zmian w konfiguracji oprogramowania zainstalowanego w systemie,
b) usuwania cudzych plików, odinstalowania programów, dekompletowania sprzętu, dotykania kabli, montażu i demontażu elementów komputera, drukarek, i innych urządzeń znajdujących się w pracowni komputerowej.

III. Zasady postępowania na wypadek znalezienia niebezpiecznych treści na komputerach szkolnych

1. Wyznaczony nauczyciel, o którym mowa w pkt. 4 kilka razy w roku sprawdza, czy na komputerach ze swobodnym dostępem, podłączonych do internetu nie znajdują się niebezpieczne treści. W przypadku znalezienia niebezpiecznych treści, wyznaczony nauczyciel stara się ustalić, kto korzystał z komputera w czasie ich wprowadzenia.
2. Informację o dziecku, które korzystało z komputera w czasie wprowadzenia niebezpiecznych treści, wyznaczony członek personelu przekazuje kierownictwu placówki, które aranżuje dla dziecka rozmowę z psychologiem lub pedagogiem.
3. Pedagog/psycholog przeprowadza z dzieckiem, o którym mowa w punktach poprzedzających, rozmowę na temat bezpieczeństwa w internecie.
4. Jeżeli w wyniku przeprowadzonej rozmowy pedagog/psycholog uzyska informację, że dziecko jest krzywdzone, podejmuje działania opisane w Standardach ochrony małoletnich i dotyczących procedur interwencji w przypadku podejrzenia krzywdzenia dziecka.

IV. Zasady ochrony uczniów przed treściami szkodliwymi i zagrożeniami z sieci.

1. Pod pojęciem „treści szkodliwe i zagrożenia z sieci” rozumiane są:
   a) treści szkodliwe, niedozwolone, nielegalne i niebezpieczne dla zdrowia (pornografia, treści obrazujące przemoc, promujące działania szkodliwe dla zdrowia i życia, popularyzujące ideologię faszystowską i działalność niezgodną z prawem, nawołujące do samookaleczeń i samobójstw, korzystania z narkotyków);
   b) treści stwarzające niebezpieczeństwo werbunku uczniów do organizacji nielegalnych;
   c) różne formy cyberprzemocy, np. nękanie, straszenie, szantażowanie z użyciem sieci, publikowanie lub rozsyłanie ośmieszających, kompromitujących informacji, zdjęć, filmów z użyciem sieci oraz podszywanie się w sieci pod kogoś wbrew jego woli.
2. Podstawowe działania zabezpieczające uczniów przed dostępem do treści szkodliwych i zagrożeń z sieci:
   a) monitorowanie działania sieci szkolnej;
   b) edukacja medialna – dostarczanie uczniom wiedzy i umiejętności dotyczących posługiwania się technologią komunikacyjną, prowadzenie działań profilaktycznych propagujących zasady bezpiecznego korzystania z sieci oraz uświadamiających zagrożenia płynące z użytkowania różnych technologii komunikacyjnych.
   c) prowadzenie systematycznych działań wychowawczych (integracja zespołu klasowego, budowanie dobrych relacji pomiędzy uczniami, wprowadzanie norm grupowych; uczenie uczniów odróżniania dobra od zła);
   d) włączenie rodziców uczniów w działania szkoły na rzecz zapobiegania cyberprzemocy – poinformowanie ich o polityce szkoły w zakresie reagowania na cyberprzemoc; edukacja na temat cyberprzemocy i zagrożeń z sieci: warsztaty, szkolenia dla rodziców, udostępnianie materiałów i publikacji, w tym polecanie i wskazywanie sposobów instalowania ochrony rodzicielskiej;
   e) podejmowanie interwencji w każdym przypadku ujawnienia lub podejrzenia cyberprzemocy lub ujawnienie niebezpiecznych treści, która obejmuje:

- ustalenie okoliczności zdarzenia;
- zabezpieczenie dowodów;
- poinformowanie o sytuacji opiekunów uczniów będących uczestnikami zdarzenia;
- objęcie pomocą poszkodowanego ucznia;
- podjęcie działań wobec agresorów, w tym zastosowanie środków dyscyplinujących zgodnie ze Statutem Szkoły i rodzajem przewinienia;
- powiadomienie policji, gdy sprawa jest poważna, zostało złamane prawo lub sprawca nie jest uczniem szkoły i jego tożsamość nie jest nikomu znana;
- jeśli mimo zastosowanych działań, niepożądane zachowania nadal mają miejsce, przekazanie informacji do sądu rodzinnego z podejrzeniem demoralizacji małoletniego.