

Zasady bezpiecznego korzystania z sieci

§ 1

Zasady ogólne

1. Obowiązkiem szkoły jest takie wykorzystanie sieci, które będzie adekwatne do poziomu dojrzałości poznawczej i emocjonalno-społecznej ucznia oraz nie będzie mu szkodzić ani zagrażać jego rozwojowi psychofizycznemu. Do potencjalnych zagrożeń płynących z użytkowania sieci należy zaliczyć:
 - 1) dostęp do treści niezgodnych z celami wychowania i edukacji (narkotyki, przemoc, pornografia, hazard);
 - 2) działalność innych użytkowników zagrażająca dobru ucznia;
 - 3) oprogramowanie umożliwiające śledzenie i pozyskanie danych osobowych użytkowników szkolnej sieci.

§ 3

Zasady korzystania z urządzeń elektronicznych

1. Zasady używania telefonów komórkowych na terenie **Zespołu** określa Statut. Zasady te służą m.in. ochronie dzieci przed treściami szkodliwymi i zagrożeniami w sieci Internetowej oraz utrwalonymi w innej formie.
2. Uczeń może korzystać z Internetu tylko na komputerze z zainstalowanym programem filtrującym treści. Uczniowie korzystają z komputera pod opieką nauczyciela.
3. Korzystanie z multimediów, Internetu i programów użytkowych służy wyłącznie celom informacyjnym i edukacyjnym.
4. Uczeń obsługuje sprzęt komputerowy zgodnie z zaleceniami nauczyciela
5. Użytkownikowi zabrania się:
 - 1) Instalowania oprogramowania i dokonywania zmian konfiguracji oprogramowania zainstalowanego w systemie
 - 2) usuwania cudzych plików, odinstalowania programów, dekompletowania sprzętu,
 - 3) dotykania elementów z tyłu komputera, kabli zasilających, a także kabli sieciowych.
6. Podstawowe działania zabezpieczające uczniów przed dostępem do treści szkodliwych i zagrożeń z sieci:

Zespół Szkół Publicznych nr 3 w Pleszewie
Załącznik nr 5 do Standardów Ochrony Małoletnich

- 1) monitorowanie działania i aktualizowanie programu antywirusowego, zapory sieciowej;
 - 2) edukacja medialna – dostarczanie uczniom wiedzy i umiejętności dotyczących posługiwania się technologią komunikacyjną;
 - 3) prowadzenie systematycznych działań wychowawczych (integracja zespołu klasowego, budowanie dobrych relacji pomiędzy uczniami, wprowadzanie norm grupowych; uczenie dzieci odróżniania dobra od zła);
 - 4) prowadzenie działań profilaktycznych propagujących zasady bezpiecznego korzystania z sieci oraz uświadamiających zagrożenia płynące z użytkowania różnych technologii komunikacyjnych.
7. Celem tych działań jest:
- 1) poszerzanie wiedzy na temat różnych form cyberprzemocy, prewencji oraz sposobu reagowania w przypadku pojawienia się zagrożenia;
 - 2) ukazanie sposobów bezpiecznego korzystania z sieci, w tym przestrzeganie przed zagrożeniami płynącymi z niewłaściwego użytkowania urządzeń multimedialnych;
 - 3) zapobieganie i ograniczenie lub wyeliminowanie zachowań agresywno przemocowych realizowanych przy użyciu technologii komunikacyjnych w szkole i poza nią;
 - 4) propagowanie zasad dobrego zachowania w Internecie.
 - 5) 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;
 - 6) instalowanie aplikacji filtrujących na urządzeniach, z których korzystają pracownicy i uczniowie oraz aplikacji filtrujących do usług sieciowych, które analizują przepływające dane i są w stanie zablokować dostęp do podejrzanych lokalizacji. Szkoła może także blokować określone domeny, jeżeli jest taka potrzeba, wtedy żadne treści z takiej domeny nie będą wczytane.
8. Podejmowanie interwencji w każdym przypadku ujawnienia lub podejrzenia cyberprzemocy lub ujawnienie niebezpiecznych treści, która obejmuje:
- 1) ustalenie okoliczności zdarzenia;
 - 2) zabezpieczenie dowodów;
 - 3) poinformowanie o sytuacji rodziców/opiekunów uczniów – uczestników zdarzenia;

Zespół Szkół Publicznych nr 3 w Pleszewie
Załącznik nr 5 do Standardów Ochrony Małoletnich

- 4) objęcie pomocą poszkodowanego ucznia;
 - 5) podjęcie działań wobec agresorów, w tym zastosowania środków dyscyplinujących zgodnie z obowiązującym regulaminem szkoły i rodzajem przewinienia;
 - 6) powiadomienie policji, gdy sprawa jest poważna, gdy zostało złamane prawo lub sprawca nie jest uczniem szkoły i jego tożsamość nie jest nikomu znana;
9. W sytuacji znalezienia niebezpiecznych treści na komputerze (lub laptopie) lub zaobserwowanej cyberprzemocy uczniowie bezpośrednio zwracają się do nauczyciela informatyki, bądź innego nauczyciela, którzy w porozumieniu ze szkolnym informatykiem podejmuje odpowiednie kroki chroniące społeczność szkolną i zabezpieczające dostęp do treści zakazanych.
10. Bezpieczne korzystanie z urządzeń elektronicznych z dostępem do sieci Internetowej obejmuje następujące zasady:
- 1) nie podawaj swoich danych osobowych, takich jak: imię, nazwisko, numer telefonu czy adres domowy;
 - 2) dbaj o nierozpowszechnianie swojego wizerunku. W przypadku publikacji zdjęć w sieci należy zadbać, aby dostęp do nich miały wyłącznie osoby znajome. Nie udostępniaj zdjęć nieznanym, w szczególności zdjęć intymnych, czy w niepełnym ubraniu;
 - 3) poinformuj rodziców lub wychowawcę (innego nauczyciela) o każdym przypadku, gdy napotkasz się w sieci na treści, które wydają się nielegalne, czy w jakikolwiek sposób wywołują niepokój;
 - 4) o propozycjach spotkania, jakie otrzymasz od internetowych znajomych zawsze informuj rodziców lub wychowawcę (innego nauczyciela);
 - 5) nie atakuj nikogo w sieci, niezależnie od tego, jakie zdanie on wyraża. Nie pokazuj agresji, nie stosuj gróźb;
 - 6) nie korzystaj z sieci przez zbyt długi czas, bo zbyt długie korzystanie z komputera, tabletu czy smartfona może zaszkodzić Twojemu zdrowiu;
 - 7) pamiętaj, że im dłużej korzystasz z sieci, tym mniej rozmawiasz ze znajomymi twarzą w twarz, a takie kontakty są najbardziej wartościowe