

Załącznik nr 12. Zasady ochrony dzieci przed treściami szkodliwymi i zagrożeniami z sieci

1 Pod pojęciem „treści szkodliwe i zagrożenia z sieci” rozumiane są:

- ✓ treści szkodliwe, niedozwolone, nielegalne i niebezpieczne dla zdrowia (pornografia, treści obrazujące przemoc, promujące działania szkodliwe dla zdrowia i życia dzieci, popularyzujące szkodliwą ideologię i działalność niezgodną z prawem, nawołujące do samookaleczeń i samobójstw, korzystania z narkotyków;
- ✓ 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 dzieci przed dostępem do treści szkodliwych i zagrożeń z sieci:

- a) monitorowanie działania i aktualizowanie programu antywirusowego, zapory sieciowej; stosowanie filtrów antyspamowych;
- b) edukacja medialna – dostarczanie dzieciom wiedzy i umiejętności dotyczących posługiwania się technologią komunikacyjną;
- c) prowadzenie systematycznych działań wychowawczych (integracja dzieci w grupie, budowanie dobrych relacji pomiędzy dziećmi wprowadzanie norm grupowych; uczenie dzieci odróżniania dobra od zła);
- d) prowadzenie działań profilaktycznych propagujących zasady bezpiecznego korzystania z sieci oraz uświadamiających zagrożenia płynące z użytkowania różnych technologii komunikacyjnych. Celem tych działań jest:
 - ✓ poszerzanie wiedzy na temat różnych form cyberprzemocy, prewencji oraz sposobu reagowania w przypadku pojawienia się zagrożenia,
 - ✓ ukazanie sposobów bezpiecznego korzystania z sieci, w tym przestrzeganie przed zagrożeniami płynącymi z niewłaściwego użytkowania urządzeń multimedialnych,
 - ✓ zapobieganie i ograniczenie lub wyeliminowanie zachowań agresywnych lub przemocowych realizowanych przy użyciu technologii komunikacyjnych w szkole i poza nią,
 - ✓ propagowanie zasad dobrego zachowania w Internecie;

- e) włączenie rodziców dzieci w działania przedszkola na rzecz zapobiegania cyberprzemocy – 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;
- f) instalowanie aplikacji filtrujących na każdym komputerze, z których korzystają pracownicy i dzieci oraz aplikacji filtrujących do usług sieciowych, które analizują przepływające dane i są w stanie zablokować dostęp do podejrzanych lokalizacji niezależnie od tego, czy przyłączony komputer wyposażono w odpowiednie narzędzie, czy też nie;
- g) podejmowanie interwencji w każdym przypadku ujawnienia lub podejrzenia cyberprzemocy lub ujawnienie niebezpiecznych treści,
- h) określenie procedury wskazującej osoby w Przedszkolu, do których należy się zwrócić oraz działania, które należy podjąć w sytuacji znalezienia niebezpiecznych treści na komputerze lub zjawiska doświadczonej/zaobserwowanej cyberprzemocy.-