**PROCEDURY OCHRONY DZIECI PRZED TREŚCIAMI SZKODLIWYMI I ZAGROŻENIAMI W INTERNECIE ORAZ UTRWALONYMI W INNEJ FORMIE**

1. Szkoła ma obowiązek podejmować działania zabezpieczające dzieci przed łatwym dostępem do tych treści z sieci, które mogą zagrażać ich prawidłowemu rozwojowi.
2. Pod pojęciem „treści szkodliwe i zagrożenia z sieci” rozumiane są:
3. treści szkodliwe, niedozwolone, nielegalne i niebezpieczne dla zdrowa (pornografia, treści obrazujące przemoc, promujące działania szkodliwe dla zdrowia i życia dzieci, popularyzujące ideologię faszystowską i działalność niezgodną z prawem, nawołujące do samookaleczeń i samobójstw, korzystania z narkotyków);
4. treści stwarzające niebezpieczeństwo werbunku dzieci do organizacji nielegalnych i terrorystycznych;
5. formy cyberprzemocy, np. : nękanie, straszenie, szantażowanie, publikowanie lub rozsyłanie ośmieszających, kompromitujących informacji, zdjęć, filmów, podszywanie się pod kogoś wbrew jego woli
6. Podstawowe działania zabezpieczające dzieci przed dostępem do treści szkodliwych i zagrożeń z sieci:
7. monitorowanie działania i aktualizowanie programu antywirusowego;
8. instalowanie aplikacji filtrujących na każdym komputerze, z których korzystają pracownicy i uczniowie;
9. edukacja medialna – dostarczanie dzieciom wiedzy i umiejętności dotyczących po-sługiwania się technologią komunikacyjną,
10. prowadzenie systematycznych działań wychowawczych (integracja zespołu klasowego, budowanie dobrych relacji pomiędzy uczniami, wprowadzanie norm grupowych; odróżnianie dobra od zła),
11. prowadzenie działań profilaktycznych propagujących zasady bezpiecznego korzystania z sieci oraz uświadamiających zagrożenia płynące z użytkowania różnych technologii komunikacyjnych,
12. 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: szkolenia dla rodziców, udostępnianie materiałów i publikacji, w tym polecanie i wskazywanie sposobów instalowania ochrony rodzicielskiej;
13. podejmowanie interwencji w każdym przypadku ujawnienia lub podejrzenia cyberprzemocy lub ujawnienie niebezpiecznych treści,
14. określenie procedury wskazującej osoby w szkole, do których należy się zwrócić oraz działania, które należy podjąć w sytuacji znalezienia niebezpiecznych treści na komputerze lub zjawiska doświadczonej/ zaobserwowanej cyberprzemocy.