PROCEDURY DOTYCZĄCE BEZPIECZEŃSTWA W SIECI
w Szkole Podstawowej nr 1 im. Stanisławy Łakomik w Czeladzi

Spis treści

Podstawy prawne stosowania procedur:

1. Ustawa z 14 grudnia 2016 r. Prawo oświatowe /Dz. U. z 2017r. poz. 59 i 949 ze zmianami/
2. Ustawa z dnia 7 września 1991 r. o systemie oświaty (t.j. Dz. U. z 2004 r. Nr 256, poz. 2572 z późn. zm.)
2. Ustawa z dnia 26 października 1982 r. o postępowaniu w sprawach nieletnich (Dz. U. z 1982 r. Nr 35 poz. 228 z p. zm. - tekst jednolity Dz. z 2002 r. Nr 11 poz. 109 z późn. zm.).
3. Zarządzenie Nr 590/03(107) Komendanta Głównego Policji z dnia 24 października 2003r. w sprawie metod i form wykonywania zadań przez policjantów w zakresie przeciwdziałania demoralizacji i przestępczości.
4. Rozporządzenie Ministra Edukacji Narodowej i Sportu z dnia 31 grudnia 2002r. w sprawie bezpieczeństwa i higieny w publicznych i niepublicznych szkołach i placówkach (Dz. U. z 2003 r. Nr 6, poz. 69, zm. Dz. U. z 2009r. Nr 139, poz. 1130).

1. Procedura zapewnienia bezpieczeństwa dziecka w sieci

1. Wszystkie komputery, z których korzystają uczniowie są zabezpieczone odpowiednim oprogramowaniem uniemożliwiającym uczniom dostęp do treści niepożądanych.
2. Nauczyciele mają prawo kontrolować czynności wykonywane przez ucznia przy komputerze.
3. Uczniowie mogą korzystać z Internetu wyłącznie pod kontrolą nauczyciela i tylko ze stron przez niego wskazanych.
4. Zabronione jest korzystanie bez zgody nauczyciela z komunikatorów, poczty elektronicznej, portali społecznościowych, stron internetowych niewiadomego pochodzenia.
5. Na stronach wymagających logowania nie włączamy opcji „zapamiętaj hasło”
6. Nie należy otwierać maili niewiadomego pochodzenia.
7. Nie wolno ściągać załączników, pobierać zawartości stron www bez zgody i nadzoru nauczyciela.
8. Nie wolno dodawać wyjątków do certyfikatów bezpieczeństwa bez zgody i nadzoru nauczyciela.
9. Nie wolno wyrażać zgody na żadne z żądań pojawiających się w oknach pop-up bez zgody i nadzoru nauczyciela.
10. W razie pojawienia się niewłaściwych i szkodliwych treści należy niezwłocznie powiadomić o tym fakcie nauczyciela.
11. Niestosowanie się przez uczniów do powyższych zasad i narażanie się na niebezpieczeństwa płynące z sieci skutkuje poinformowaniem o zaistniałej sytuacji wychowawcy klasy i rodziców.

2. Cyberprzemoc – charakterystyka zjawiska.

Zapewnienie uczniom bezpieczeństwa w szkole jest jednym z najważniejszych zadań placówki oświatowej. Ujawnienie zjawiska cyberprzemocy wymaga podjęcia w szkole konkretnych działań interwencyjnych.

Cyberprzemoc to inaczej przemoc z użyciem mediów elektronicznych – przede wszystkim Internetu i telefonów komórkowych.

Do działań określanych, jako cyberprzemoc zalicza się m.in:

1. Wyzywanie, straszenie poniżanie kogoś w Internecie lub przy użyciu telefonu,

2. Robienie komuś zdjęć lub rejestrowanie filmów bez jego zgody,

3. Publikowanie w Internecie lub rozsyłanie telefonem zdjęć, filmów lub tekstów, które kogoś obrażają lub ośmieszają,

4. Podszywanie się pod kogoś w sieci.

a. Cyberprzemoc - postanowienia ogólne.

1. Szkoła prowadzi działania profilaktyczne uświadamiające całej społeczności szkolnej (uczniom, rodzicom, nauczycielom i innym pracownikom szkoły) zasady korzystania i zagrożenia płynące z użytkowania różnych technologii komunikacyjnych.
2. W szkole podejmuje się interwencję w każdym przypadku ujawnienia lub podejrzenia cyberprzemocy.
3. Niniejsze procedury zawierają zasady postępowania nauczycieli i innych pracowników szkoły w sytuacji podejrzenia lub ujawnienia cyberprzemocy.
4. Procedury reagowania na cyberprzemoc w szkole muszą dotyczyć zachowań i działań wobec:
   - ofiary,
   - sprawcy,
   - świadka.

b. Reagowanie szkoły na ujawnienie cyberprzemocy

1. Ujawnienie przypadku cyberprzemocy.

   Informacja o tym, że w szkole miała miejsce cyberprzemoc może pochodzić z różnych źródeł. Osobą zgłaszającą fakt prześladowania może być poszkodowany uczeń, jego rodzice, inni uczniowie — świadkowie zdarzenia, nauczyciele.

2. Ustalenie okoliczności zdarzenia.

1). Wszystkie przypadki przemocy, a więc także przemocy z wykorzystaniem mediów elektronicznych powinny zostać właściwie zbadane, zarejestrowane i udokumentowane.
2). Jeśli wiedzę o zajściu posiada nauczyciel niebędący wychowawcą, powinien przekazać informację wychowawcy klasy, który informuje o fakcie pedagoga/ psychologa szkolnego i dyrektora.
3). Pedagog/ psycholog szkolny i dyrektor wspólnie z wychowawcą powinni dokonać analizy zdarzenia i zaplanować dalsze postępowanie.
4). Do zadań szkoły należy także ustalenie okoliczności zdarzenia i ewentualnych świadków.
5). Nauczyciel informatyki w procedurze interwencyjnej, o ile to możliwe, zabezpiecza dowody i ustala tożsamość sprawcy cyberprzemocy.

3. Zabezpieczenie dowodów:

1). Wszelkie dowody cyberprzemocy powinny zostać zabezpieczone i zarejestrowane. Należy zanotować datę i czas otrzymania materiału, treść wiadomości oraz, jeśli to możliwe, dane nadawcy (nazwę użytkownika, adres e-mail, numer telefonu komórkowego, itp.) lub adres strony WWW, na której pojawiły się szkodliwe treści czy profil.

2). Zabezpieczenie dowodów nie tylko ułatwi dalsze postępowanie dostawcy usługi (odnalezienie sprawcy, usunięcie szkodliwych treści z serwisu), ale również stanowi materiał, z którym powinny się zapoznać wszystkie zaangażowane w sprawę osoby: dyrektor i pedagog szkolny, rodzice, a wreszcie policja, jeśli doszło do złamania prawa.

4. Jak można zarejestrować dowody cyberprzemocy?

- telefon komórkowy (nie wolno kasować wiadomości, trzeba zapisywać zarówno te tekstowe jak też zdjęcia, nagrania z dyktafonu czy filmy)
- komunikatory (w niektórych serwisach jest możliwość zapisywania rozmów w tzw. archiwach. Jeżeli nie ma takiej możliwości, można rozmowę skopiować do edytora tekstowego i wydrukować).
- strona WWW (można zapisać widok strony przez naciśnięcie klawisza PrintScreen, a następnie wykonać operację Wklej w dokumencie Word lub Paint.
- e-mail (trzeba zapisać wiadomość i to nie tylko treść, ale całą wiadomość, ponieważ może to pomóc w ustaleniu pochodzenia wiadomości)

5. Identyfikacja sprawcy:

1). Szkoła podejmuje działania mające na celu identyfikację sprawcy cyberprzemocy
2). W sytuacji, kiedy ustalenie sprawcy nie jest możliwe, należy skontaktować się z dostawcą usługi w celu usunięcia z Sieci kompromitujących lub krzywdzących materiałów. Do podjęcia takiego działania zobowiązuje administratora serwisu art. 14 Ustawy z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną.
3). W przypadku, gdy zostało złamane prawo, a tożsamości sprawcy nie udało się ustalić należy bezwzględnie skontaktować się z policją.

3. Działania wobec sprawcy cyberprzemocy

1. W przypadku, gdy sprawca cyberprzemocy jest znany i jest on uczniem szkoły, pedagog/ psycholog szkolny powinien podjąć następujące działania:
   - przeprowadzić rozmowę z uczniem, której celem jest ustalenie okoliczności zajścia, wspólnie zastanowić się nad jego przyczynami i poszukać rozwiązania sytuacji konfliktowej;
   - omówić z uczniem skutki jego postępowania i poinformować o konsekwencjach regulaminowych, które zostaną wobec niego zastosowane;
   - zobowiązać sprawcę do zaprzestania swojego działania i usunięcia z Sieci szkodliwych materiałów;
   - ustalić ze sprawcą sposób zadośćuczynienia wobec ofiary cyberprzemocy.
2. Jeśli w zdarzeniu brała udział większa grupa uczniów, należy rozmawiać z każdym z nich z osobna, zaczynając od lidera grupy.
3. Nie należy konfrontować sprawcy i ofiary cyberprzemocy.
4. Rodzice sprawcy zostają poinformowani o przebiegu zdarzenia i zapoznani z materiałem dowodowym, a także z decyzją w sprawie dalszego postępowania i podjętych przez szkołę środkach dyscyplinarnych wobec ich dziecka.
5. We współpracy z rodzicami należy opracować projekt kontraktu dla dziecka, określającego zobowiązania ucznia, rodziców i przedstawiciela szkoły oraz konsekwencje nieprzestrzegania przyjętych wymagań i terminy realizacji zadań zawartych w umowie.

4. Zastosowanie środków dyscyplinarnych wobec sprawcy cyberprzemocy.

1. Wobec sprawcy cyberprzemocy szkoła stosuje kary zawarte w statucie szkoły, takie same, jak w przypadku każdego rodzaju przemocy.

2. Dodatkowo uczeń-sprawca może mieć czasowy zakaz korzystania ze szkolnej pracowni multimedialnej w czasie wolnym lub przynoszenia do szkoły akcesoriów (zgodnie z regulaminem korzystania z telefonów komórkowych lub innych urządzeń elektronicznych).

3. Podejmując decyzję o rodzaju kary należy wziąć pod uwagę:
   - rozmiar i rangę szkody — czy materiał został upubliczniony w sposób pozwalający na dotarcie do niego wielu osobom (określa to rozmiar upokorzenia, jakiego doznaje ofiara), czy trudno jest wycofać materiał z Sieci, itp.; -
   - czas trwania prześladowania — czy było to długotrwałe działanie, czy pojedynczy incydent; - świadomość popełnianego czynu — czy działanie było zaplanowane, a sprawca był świadomy, że wyrządza krzywdę koledze oraz jak wiele wysiłku włożył w ukrycie swojej tożsamości, itp.;
   - motywację sprawcy — należy sprawdzić, czy działanie sprawcy nie jest działaniem odwetowym w odpowiedzi na uprzednio doświadczone prześladowanie;
   - rodzaj rozpowszechnianego materiału.

5. Działania wobec ofiary cyberprzemocy.

1. Ofiara cyberprzemocy otrzymuje w szkole pomoc psychologiczno-pedagogiczną udzielaną przez pedagoga/ psychologa szkolnego.
2. W strategii działań pomocowych uczeń-ofiara powinien otrzymać wsparcie psychiczne oraz poradę, jak ma się zachować, aby zapewnić sobie poczucie bezpieczeństwa i nie doprowadzić do eskalacji prześladowania: nie utrzymywać kontaktów ze sprawcą, nie kasować dowodów tj. e-maili, SMS-ów, MMS-ów, zdjęć, filmów. Ważna jest też zmiana danych kontaktowych np. na komunikatorze, zmiana adresu e-mail, a nawet w szczególnie trudnych sytuacjach numeru telefonu (oczywiście robią to rodzice).
3. Po zakończeniu interwencji wychowawca wraz z osobą udzielającą pomocy monitorują sytuację ucznia sprawdzając, czy nie są wobec niego podejmowane dalsze działania przemocy bądź odwetowe ze strony sprawcy.
4. Rodzice dziecka będącego ofiarą cyberprzemocy zostają poinformowani o problemie, podjętych działaniach szkoły i, w miarę potrzeb, otrzymują wsparcie i pomoc specjalistów.

6. Rozmowa z uczniem – ofiarą cyberprzemocy.

1. Podczas rozmowy z uczniem – ofiarą cyberpzemocy:
   - Należy zapewnić go, że dobrze zrobił, mówiąc o tym, co się stało.
   - Mówimy, że widzimy i rozumiemy, że jest mu trudno ujawnić to, co go spotkało.
   - Informujemy go, że nikt nie ma prawa tak się zachowywać wobec niego.
   - Zapewniamy go, że szkoła nie toleruje żadnej formy przemocy i że postara się mu pomóc, uruchamiając odpowiednie procedury interwencyjne.
   - Jesteśmy uważni na pozawerbalne przejawy uczuć dziecka – zażenowanie, skrępowanie, wstyd, lęk, przerażenie, smutek, poczucie winy.

7. Ochrona świadków zgłaszających zdarzenie.

1. Szkoła otacza świadków zdarzenia uczestniczących w ustalaniu przebiegu zajścia opieką psychologiczno-pedagogiczną.
2. Osoba, której uczeń zaufał informując, o cyberprzemocy ma obowiązek postępować tak, by swoim zachowaniem i działaniem nie narazić świadka zgłaszającego problem.
3. Niedopuszczalne jest konfrontowanie świadka ze sprawcą, jako metoda wyjaśniania sprawy.
4. Świadkowie powinni być objęci profesjonalną ochroną, a wszystkie działania powinny być tak prowadzone, aby zapewniały bezpieczeństwo nie tylko ofierze, ale i świadkom cyberprzemocy. Ważne jest, by w wyniku interwencji nie narażać świadka na groźby i zdarzenia ze strony sprawcy. Całe postępowanie powinno być prowadzone w sposób bardzo dyskretny i poufny. Jeżeli tak nie będzie, to dziecko może bać się, że wobec niego też może wystąpić takie zdarzenie i zostanie nazwany „donosicielem". Dlatego podczas takiej rozmowy należy wzbudzić swoim zachowaniem zaufanie oraz poczucie bezpieczeństwa, wykazać zrozumienie i empatię, powiedzieć uczniowi, że postąpił właściwie, że wymagało to od niego odwagi. Należy zapewnić go o dyskrecji i nie ujawniać jego danych osobowych (chyba, że jest to na prośbę policji).

8. Sporządzenie dokumentacji z zajścia.

1. Pedagog/ psycholog szkolny zobowiązany jest do sporządzenia notatki służbowej z rozmów ze sprawcą, poszkodowanym, ich rodzicami oraz świadkami zdarzenia. Dokument powinien zawierać datę i miejsce rozmowy, personalia osób biorących w niej udział i opis ustalonego przebiegu wydarzeń
2. Jeśli rozmowa przebiegała w obecności świadka (np. wychowawcy) powinien on podpisać notatkę po jej sporządzeniu.
3. Jeśli zostały zabezpieczone dowody cyberprzemocy, należy je również włączyć do dokumentacji pedagogicznej (wydruki, opis, itp.).

9. Powiadomienie sądu rodzinnego

1. Jeśli rodzice sprawcy cyberprzemocy odmawiają współpracy lub nie stawiają się do szkoły, a uczeń nie zaniechał dotychczasowego postępowania dyrektor szkoły powinien pisemnie powiadomić o zaistniałej sytuacji sąd rodzinny, szczególnie, jeśli do szkoły napływają informacje o innych przejawach demoralizacji dziecka.
2. W sytuacji, gdy szkoła wykorzysta wszystkie dostępne jej środki wychowawcze (rozmowa z rodzicami, konsekwencje regulaminowe wobec ucznia, spotkania z pedagogiem, itp.), a ich zastosowanie nie przynosi pożądanych rezultatów, dyrektor powinien zwrócić się do sądu rodzinnego z zawiadomieniem o podjęcie odpowiednich środków wynikających z ustawy o postępowaniu w sprawach nieletnich.
3. W przypadku szczególnie drastycznych aktów agresji z naruszeniem prawa, dyrektor szkoły zobowiązany jest zgłosić te fakty policji i do sądu rodzinnego.