Załącznik do zarządzenia nr 16/12/2019/2020
z dnia 18.12.2019 r.

PROCEDURY REAGOWANIA

w przypadku wystąpienia w szkole zagrożeń bezpieczeństwa cyfrowego

Będzin, grudzień 2019 r.

1. *Ustawa z dnia 7 września 1991 r. o systemie oświaty* (Dz. U. z 2004r. nr 256 poz. 2572 z zm.)
2. Ustawa z dnia 14 grudnia 2016 r. Prawo oświatowe (Dz. U. z 20017r. poz. 59, 949 i 2203)
3. *Ustawa z dnia 26 października 1982 r. o postępowaniu w sprawach nieletnich (Dz. U. z 1982 r. nr 35 poz. 228 z późn. zm. - tekst jednolity Dz. U. z 2010 r. nr 33 poz. 178 oraz przepisy wykonawcze w związku z ustawą).*
4. *Ustawa z dnia 26 października 1982 r. o wychowaniu w trzeźwości i przeciwdziałaniu alkoholizmowi (Dz. U. z 2002 r., Nr 147 poz. 1231).*
5. *Zarządzenie Komendanta Głównego Policji nr 1619 z dnia 3 listopada 2012 r. w sprawie form i metod działań policji w zakresie zapobiegania i zwalczania demoralizacji i przestępczości nieletnich.*
6. *Ustawa z dnia 6 kwietnia 1990 r. o Policji (Dz. U. nr 30 poz. 179 z p. zm.).*
7. *Ustawa z dnia 9 listopada 1995 roku o ochronie zdrowia przed następstwami używania tytoniu i wyrobów tytoniowych (Dz. U. z 1996 r., Nr 10 poz. 55).*
8. *Ustawa z dnia 29 lipca 2005 r. o przeciwdziałaniu narkomanii (Dz. U. z 2005 r., Nr 179 poz. 1485 ze zm. , tekst jednolity ustawy z dnia 10 stycznia 2012 r.)*
9. *Rozporządzenie MEN i S z dnia 31 stycznia 2003 r. w sprawie szczegółowych form działalności wychowawczej i zapobiegawczej wśród dzieci i młodzieży zagrożonej uzależnieniem (Dz. U. z 2003 r., Nr 26 poz. 226)*
10. Rozporządzenie MENiS z dnia 31 grudnia 2002 r. w sprawie bezpieczeństwa i higieny w publicznych i niepublicznych szkołach i placówkach (Dz. U nr 6, poz 69 z 2003 z póź. zm).
11. Ustawa z dnia 10 czerwca 2016 r. o działaniach antyterrorystycznych (Dz. U. z 2019 r. poz.796).
12. *Statut CKZiU w Będzinie, ul. 11 Listopada 3*

Podstawowe działania na rzecz bezpieczeństwa cyfrowego w szkole.

W przypadkach wystąpienia incydentu naruszenia bezpieczeństwa, zwłaszcza wobec naruszenia prawa, działania szkoły cechuje otwartość w działaniu, szybka identyfikacja problemu - określenie szkodliwych lub niezgodnych z prawem zachowań - i jego rozwiązywanie adekwatnie do poziomu zagrożenia, jakie wywołało w szkole.

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.

Opis procedury reagowania 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/ prawi opiekunowie, inni uczniowie — świadkowie zdarzenia, nauczyciele
2. .**Ustalenie okoliczności zdarzenia**
   a. Wszystkie przypadki przemocy, a więc także przemocy z wykorzystaniem mediów elektronicznych powinny zostać właściwie zbadane, zarejestrowane i udokumentowane.
   b. Jeśli wiedzę o zajściu posiada nauczyciel nie będący wychowawcą, przekazuje informację wychowawcy klasy, który informuje o fakcie pedagoga szkolnego i dyrektora.
   c. Pedagog szkolny i dyrektor wspólnie z wychowawcą dokonują analizy zdarzenia i planują dalsze postępowanie. Ustalają okoliczności zdarzenia i ewentualnych świadków.
   d. Nauczyciel informatyki, o ile to możliwe, zabezpiecza dowody i ustala tożsamość sprawcy cyberprzemocy.
3. **Zabezpieczenie dowodów**
   a. 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 email, numer telefonu komórkowego, itp.) lub adres strony www, na której pojawiły się szkodliwe treści czy profil.
   b. 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/prawni opiekunowie, a także policja, jeśli doszło do złamania prawa.
4. **Identyfikacja sprawcy**
   a. Szkoła podejmuje działania mające na celu identyfikację sprawcy cyberprzemocy.
   b. W sytuacji kiedy ustalenie sprawcy nie jest możliwe, dyrektor szkoły kontaktuje 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.

c. W przypadku, gdy zostało złamane prawo, a tożsamości sprawcy nie udało się ustalić dyrektor zgłasza sprawę policji.

5. Działania wobec sprawcy cyberprzemocy

a. W przypadku, gdy sprawca cyberprzemocy jest znany i jest on uczniem szkoły, pedagog szkolny podejmuje następujące działania:
   - ✓ przeprowadza rozmowę z uczniem, której celem jest ustalenie okoliczności zajścia, jego przyczynami i szuka rozwiązania sytuacji konfliktowej,
   - ✓ omawia z uczniem skutki jego postępowania i informuje go o konsekwencjach regulaminowych, które zostaną wobec niego zastosowane - zobowiązuje sprawcę do zaprzestania swojego działania i usunięcia z Sieci szkodliwych materiałów.

b. Jeśli w zdarzeniu brała udział większa grupa uczniów, pedagog rozmawia z każdym z nich z osobna, zaczynając od lidera grupy.

c. Nie konfrontuje się sprawcy i ofiary cyberprzemocy.

d. Rodzice/prawni opiekunowie 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.

6. Zastosowanie środków dyscyplinarnych wobec sprawcy cyberprzemocy

a. Wobec sprawcy cyberprzemocy szkoła stosuje kary zawarte w Statucie szkoły.

b. Dodatkowo uczeń - sprawca może mieć czasowy zakaz korzystania ze szkolnej pracowni multimedialnej w czasie wolnym lub przynoszenia do szkoły akcesoriów elektronicznych.

c. Na decyzję o rodzaju kary wpływa:
   - ✓ 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.;
   - ✓ motywacja sprawcy - czy działanie sprawcy nie jest np. działaniem odwetowym w odpowiedzi na uprzednio doświadczone prześladowanie;
   - ✓ rodzaj rozpowszechnianego materiału.

7. Działania wobec ofiary cyberprzemocy

a. Ofiara cyberprzemocy otrzymuje w szkole pomoc psychologiczno-pedagogiczną udzielaną przez pedagoga.

b. W strategii działań pomocowych uczeń - ofiara otrzymuje wsparcie psychiczne oraz poradę, jak ma się zachować, aby zapewnić sobie poczucie bezpieczeństwa i nie doprowadzić do eskalacji prześladowania.

c. Po zakończeniu interwencji wychowawca wraz z pedagogiem monitorują sytuację ucznia sprawdzając, czy nie są wobec niego podejmowane dalsze działania przemocowe bądź odwetowe ze strony sprawcy.

d. Rodzice/prawni opiekunowie ucznia będącego ofiarą cyberprzemocy zostają poinformowani o problemie, podjętych działaniach szkoły, otrzymują wsparcie i pomoc specjalistów.

8. Ochrona świadków zgłaszających zdarzenie

a. Opieką psychologiczno - pedagogiczną szkoła otacza także świadków zdarzenia uczestniczących w ustalaniu przebiegu zajścia.
b. Osoba, której uczeń zaufał informując o cyberprzemocy ma obowiązek postępować tak, by swoim zachowaniem i działaniem nie narazić świadka zgłaszającego problem.

9. Sporządzenie dokumentacji z zajścia

a. Pedagog szkolny sporządza notatkę służbową z rozmów ze sprawcą, poszkodowanym, ich rodzicami/prawnymi opiekunami oraz świadkami zdarzenia. Dokument zawiera datę i miejsce rozmowy, personalia osób biorących w niej udział i opis ustalonego przebiegu wydarzeń.
b. Jeśli rozmowa przebiegała w obecności świadka (np. wychowawcy) podpisuje on notatkę po jej sporządzeniu.
c. Jeśli zostały zabezpieczone dowody cyberprzemocy, włącza się je do dokumentacji pedagogicznej (wydruki, opis, itp.).

10. Powiadomienie sądu rodzinnego

a. Jeśli rodzice/prawni opiekunowie sprawcy cyberprzemocy odmawiają współpracy lub nie stawiają się do szkoły, a uczeń nie zaniechał dotychczasowego postępowania dyrektor szkoły powiadamia o zaistniałej sytuacji sąd rodzinny, szczególnie jeśli do szkoły napływają informacje o innych przejawach demoralizacji dziecka.
b. W sytuacji, gdy szkoła wykorzysta wszystkie dostępne jej środki wychowawcze (rozmowa z rodzicami/prawnymi opiekunami, konsekwencje regulaminowe wobec ucznia, spotkania z pedagogiem, itp.), a ich zastosowanie nie przynosi pożądanych rezultatów, dyrektor zwraca się do sądu rodzinnego z zawiadomieniem o podjęcie odpowiednich środków wynikających z ustawy o postępowaniu w sprawach nieletnich.
c. W przypadku szczególnie drastycznych aktów agresji z naruszeniem prawa, dyrektor szkoły zgłasza te fakty policji.