**PROCEDURY REAGOWANIA**

**W PRZYPADKU WYSTĄPIENIA W ZESPOLE SZKÓŁ PUBLICZNYCH W MOSTACH IM. LOTNIKÓW POLSKICH**

**ZAGROŻEŃ BEZPIECZEŃSTWA CYFROWEGO**

**CEL/ZASADY OGÓLNE**

Zagrożenia bezpieczeństwa cyfrowego w szkole oraz problemy ucznia w świecie cyfrowym mogą mieć różnorodny charakter. Warto przy tym podkreślić, iż nie istnieje „złota recepta”, którą zastosować można we wszystkich przypadkach wystąpienia zagrożeń spowodowanych przez uczniów.

1. Obligatoryjne działania interwencyjne, będące następstwem wystąpienia zagrożenia.

1) Działania wobec aktu/zdarzenia - opis przypadku, ustalenie okoliczności zdarzenia, zabezpieczenie dowodów oraz monitoring po-interwencyjny.

Działania wobec zdarzenia polegają przede wszystkim na zachowaniu dokumentacji cyfrowej: wiadomości sms, e-maili, nagrań z poczty głosowej telefonu, komentarzy w serwisie społecznościowym, zapisów w blogu i plików filmów wideo. O ile to możliwe, należy także zarchiwizować treść rozmów w komunikatorach oraz linki (konkretne adresy URL) oraz danych o potencjalnym sprawcy. Każde zdarzenie wymaga udokumentowania.

2) Działania wobec uczestników zdarzenia (ofiara – sprawca – świadek – rodzice).

Przez działania na rzecz uczestników zdarzenia rozumie się aktywności podejmowane wobec ofiar (osób poszkodowanych), sprawców i świadków zdarzenia. W szkole osobami poszkodowanymi będą dzieci (nieletni). Dlatego jako kolejną grupę pośrednich uczestników zdarzenia wyróżniamy ich rodziców. Standardowa procedura reakcji w przypadku wystąpienia zagrożenia bezpieczeństwa cyfrowego:

a) rozmowa uczestnika zdarzenia z wychowawcą, pedagogiem/psychologiem,

b) powiadomienie rodziców poszkodowanego,

c) działania wychowawcze i wyciągniecie konsekwencji wobec sprawcy,

d) powiadomienie Policji/sądu rodzinnego w przypadku naruszenia prawa,

e) udzielenie uczestnikom zdarzenia wsparcia psychologiczno-pedagogicznego.

3) Działania wobec instytucji/organizacji/służb pomocowych i współpracujących – Policji, wymiaru sprawiedliwości, służb społecznych.

Działania szkoły adresowane do instytucji i organizacji zewnętrznych są niezbędne w przypadku naruszenia przepisów prawa przez uczniów lub osoby spoza szkoły: Policją i sądami rodzinnymi, służbami społecznymi i placówkami specjalistycznymi oraz dostawcami usług internetowych oraz operatorami telekomunikacyjnymi.

2. Sprawców wszystkich rodzajów zagrożeń bezpieczeństwa cyfrowego w szkole należy objąć, co najmniej poniższymi działaniami:

1) Sprawca musi otrzymać od przedstawicieli szkoły komunikat o braku akceptacji dla działań, jakich dokonał. W trakcie takiej rozmowy uczeń powinien poznać możliwe skutki swojego postępowania, a także konsekwencje, jakie mogą zostać wobec niego wyciągnięte (np. wynikające ze statutu szkoły lub wprowadzonego kontraktu-umowy). W trakcie rozmowy sprawca powinien zostać wezwany do zaprzestania podejmowania podobnych działań w przyszłości, w tym usunięcia skutków swoich działań (np. publikacji w portalu społecznościowym).

2) Sprawca powinien również zostać objęty odpowiednią pomocą psychologiczno- pedagogiczną w celu zrozumienia konsekwencji jego zachowania oraz zmianie postawy i dalszego postępowania. Jeśli sprawców jest więcej, to z każdym z nich należy rozmawiać osobno.

3. Należy zadbać o to, żeby osoba reprezentująca szkołę (pedagog, pedagog specjalny, psycholog, wychowawca) ograniczała się do podjęcia interwencji, a nie wymierzała karę. Decyzję o tym, jaką karę wymierzyć sprawcy, powinna podejmować rada pedagogiczna (po poznaniu wszystkich okoliczności zdarzenia), a przekazywać dyrektor szkoły. Ważne jest zatem oddzielenie osoby pedagoga, nawiązującego relację z uczniem, od organu wymierzającego karę.

1) Celem sankcji wobec sprawcy jest przede wszystkim: zatrzymanie jego działań i zapewnienie poczucia bezpieczeństwa ofierze oraz zmiana postawy sprawcy. Sankcje mają na celu także pokazanie społeczności szkolnej, że działania sprawcy nie będą tolerowane i że szkoła jest w stanie skutecznie zareagować w tego rodzaju sytuacji. Podejmując decyzję o sankcjach, należy wziąć pod uwagę:

a) rozmiar i rangę szkody – np. czy w przypadku cyberprzemocy materiał został upubliczniony w sposób pozwalający na dotarcie do niego wielu osobom (okres oraz rozmiar upokorzenia, jakiego doznaje ofiara), czy trudno jest wycofać materiał z sieci itp.;

b) czas trwania prześladowania – czy było to długotrwałe działanie, czy pojedynczy incydent,

c) świadomość popełnianego czynu – czy działanie było zaplanowane, a sprawca był świadomy, że postąpił nagannie np. czy wie, że wyrządza krzywdę koledze, jak wiele wysiłku włożył w ukrycie swojej tożsamości itp.;

d) motywację sprawcy – należy sprawdzić, czy działanie sprawcy nie jest działaniem odwetowym w odpowiedzi na uprzednie doświadczenia sprawcy.

4. Aktywność wobec sprawcy powinna także obejmować rozmowę z jego rodzicami powinni oni zostać poinformowani o zdarzeniu, zapoznani z materiałami oraz decyzją na temat dalszego postępowania ze sprawcą (np. na temat sankcji). Warto, aby rodzice współpracowali ze szkołą w zakresie rozwiązywania sytuacji kryzysowej, aby stali się jej sojusznikami a nie przeciwnikami. Rodzice sprawcy powinni również zostać poinformowani, że rodzice ofiary mają prawo zgłosić sprawę na Policję.

5. Jeśli sprawca pochodzi spoza szkoły, należy zapewnić bezpieczeństwo ofierze i poinformować ją (jej rodziców) o przysługujących jej prawach (np. zgłoszenie popełnienie przestępstwa na Policję). Jeśli sprawca jest z innej szkoły, należy rozważyć nawiązanie współpracy między placówkami i wspólne rozwiązanie kryzysowej sytuacji.

**PRZEBIEG REALIZACJI/OPIS CZYNNOŚCI**

1. **Cyberprzemoc – procedura reagowania**

Cyberprzemoc – przemoc z użyciem technologii informacyjnych i komunikacyjnych, głównieInternetu oraz telefonów komórkowych. Podstawowe formy zjawiska to nękanie, straszenie,szantażowanie z użyciem sieci, publikowanie lub rozsyłanie ośmieszających,kompromitujących informacji, zdjęć, filmów z użyciem sieci oraz podszywanie się w siecipod kogoś wbrew jego woli. Do działań określanych mianem cyberprzemocywykorzystywane są głównie: poczta elektroniczna, czaty, komunikatory, strony internetowe,logi, serwisy społecznościowe, grupy dyskusyjne, serwisy SMS i MMS.

Telefon Zaufania dla Dzieci i Młodzieży - 116 111

Telefon dla Rodziców i Nauczycieli w sprawie Bezpieczeństwa Dzieci – 800 100 100,

[dyzurnet@dyzurnet.pl](mailto:dyzurnet@dyzurnet.pl) Przyjęcie zgłoszenia i ustalenie okoliczności zdarzenia

1) Przypadek cyberprzemocy może zostać ujawniony przez ofiarę, świadka (np. innego ucznia, nauczyciela, rodzica) lub osobę bliską ofierze (np. rodzice, rodzeństwo, przyjaciele). W każdym przypadku należy ze spokojem wysłuchać osoby zgłaszającej i okazać jej wsparcie. Podziękować za zaufanie i zgłoszenie tej sprawy.

2) Jeśli zgłaszającym jest ofiara cyberprzemocy, podejmując działania przede wszystkim należy okazać wsparcie, z zachowaniem jej podmiotowości poszanowaniem jej uczuć . Potwierdzić , że ujawnienie przemocy jest dobrą decyzją. Taką rozmowę należy przeprowadzić w miejscu bezpiecznym, zapewniającym ofierze intymność. Nie należy podejmować kroków, które mogłyby prowadzić do powtórnej wiktymizacji czy wzbudzić podejrzenia sprawcy (np. wywoływać ucznia z lekcji do dyrekcji).

3) Jeśli osobą zgłaszającą nie jest ofiara, na początku prosimy o opis sytuacji, także z zachowaniem podmiotowości i poszanowaniem uczuć osoby zgłaszającej (np. strach przed byciem donosicielem, obawa o własne bezpieczeństwo).

4) W każdej sytuacji w trakcie ustalania okoliczności trzeba ustalić charakter zdarzenia (rozmiar i rangę szkody, jednorazowość /powtarzalność). Realizując procedurę należy unikać działań, które mogłyby wtórnie stygmatyzować ofiarę lub sprawcę, np.: wywoływanie uczniów z lekcji, konfrontowanie ofiary i sprawcy, niewspółmierna kara, wytykanie palcami, etc. Trzeba dokonać oceny, czy zdarzenie wyczerpuje znamiona cyberprzemocy, czy jest np. niezbyt udanym żartem (wtedy trzeba podjąć działania profilaktyczne mające na celu niedopuszczenie do eskalacji tego typu zachowań w stronę cyberprzemocy).

5) Należy zabezpieczyć wszystkie dowody związane z aktem cyberprzemocy (np. zrobić kopię materiałów, zanotować datę i czas otrzymania materiałów, dane nadawcy, adresy stron www, historię połączeń, etc.). W trakcie zbierania materiałów należy zadbać o bezpieczeństwo osób zaangażowanych w problem.

6) Identyfikacja sprawcy(ów) często jest możliwa dzięki zebranym materiałom – wynikom rozmów z osobą zgłaszającą, z ofiarą, analizie zebranych materiałów. Ofiara często domyśla się, kto stosuje wobec niego cyberprzemoc.

7) Jeśli ustalenie sprawcy nie jest możliwe, a w ocenie kadry pedagogicznej jest to konieczne, należy skontaktować się z Policją. Bezwzględnie należy zgłosić rozpowszechnianie nagich zdjęć osób poniżej 18 roku życia (art. 202 par. 3 KK)

8) Gdy sprawca cyberprzemocy jest znany i jest on uczniem szkoły, pedagog/psycholog szkolny powinien przeprowadzić z nim rozmowę o jego zachowaniu. Rozmowa taka ma służyć ustaleniu okoliczności zdarzenia, jego wspólnej analizie (w tym np. przyjrzeniu się przyczynom), a także próbie rozwiązania sytuacji konfliktowej (w tym sposobów zadość uczynienia ofiarom cyberprzemocy).

9) Cyberprzemoc powinna podlegać sankcjom określonym w wewnętrznych przepisach szkoły (m. in. w statucie, kontrakcie, regulaminie). Szkoła może tu stosować konsekwencje przewidziane dla sytuacji „tradycyjnej” przemocy. Warto jednak rozszerzyć repertuar dostępnych środków, np. o czasowy zakaz korzystania ze szkolnej pracowni komputerowej w czasie wolnym i przynoszenia do szkoły akcesoriów elektronicznych (PSP, mp3) itp.

10) W pierwszej kolejności należy udzielić wsparcia ofierze. Musi się ona czuć bezpieczna i zaopiekowana przez dorosłych. Na poczucie bezpieczeństwa dziecka wpływa fakt, że wie ono, iż szkoła podejmuje kroki w celu rozwiązania problemu.

11) Podczas rozmowy z uczniem – ofiarą cyberprzemocy – należy zapewnić go, że nie jest winny zaistniałej sytuacji oraz że nikt nie ma prawa zachowywać się w ten sposób wobec niego, a także podkreślić , że dobrze zrobił ujawniając sytuację. Należy okazać zrozumienie dla jego uczuć, w tym trudności z ujawnieniem okoliczności wydarzenia, strachu, wstydu. Trzeba podkreślić, że szkoła nie toleruje przemocy i że zostaną podjęte odpowiednie procedury interwencyjne. Należy poinformować ucznia o krokach, jakie może podjąć szkoła i sposobach, w jaki może zapewnić mu bezpieczeństwo.

12) Należy pomóc ofierze (rodzicom ofiary) w zabezpieczeniu dowodów (to może być dla niej zadanie trudne zarówno ze względów technicznych, jak i emocjonalnych), zerwaniu kontaktu ze sprawcą, zadbaniu o podstawowe zasady bezpieczeństwa on-line (np. nieudostępnianie swoich danych kontaktowych, kształtowanie swojego wizerunku, itd.).

13) Pomoc ofierze nie może kończyć się w momencie zakończenia procedury. Warto monitorować sytuację, „czuwać ” nad jej bezpieczeństwem, np. zwracać uwagę czy nie są podejmowane wobec niej dalsze działania przemocowe, obserwować, jak sobie radzi w grupie po ujawnionym incydencie cyberprzemocy.

14) W działania wobec ofiary należy także włączyć rodziców ofiary – trzeba na bieżąco ich informować o sytuacji, pamiętając przy tym o podmiotowym traktowaniu dziecka – mówiąc mu o tym i starając się uzyskać jego akceptację dla udziału rodziców. Jeśli dziecko nie wyraża zgody, należy omówić z nim jego obawy, a jeśli to nie pomaga powołać się na obowiązujące nas zasady i przekazać informację rodzicom.

15) W trakcie rozmowy z dzieckiem i/lub jego rodzicami/opiekunami, jeśli jest to wskazane, można zaproponować pomoc specjalisty (np. psycholog szkolny, poradnia psychologiczno-pedagogiczna) oraz przekazać informację o możliwość zgłoszenia sprawy Policji.

16) Należy zadbać o bezpieczeństwo świadków zdarzenia, zwłaszcza, jeśli byli oni osobami ujawniającymi cyberprzemoc. W trakcie rozmowy ze świadkami należy okazać zrozumienie i empatię dla ich uczuć – obawy przed przypięciem łatki „donosiciela”, strachu przed staniem się kolejną ofiarą sprawcy itp.

17) Samo wystąpienie zjawiska cyberprzemocy nie jest jednoznaczne z koniecznością zaangażowania Policji i sądu rodzinnego – procedura powinna umożliwiać rozwiązanie sytuacji problemowej na poziomie pracy wychowawczej szkoły. Szkoła powinna powiadomić odpowiednie służby (np. sąd rodzinny), gdy wykorzysta wszystkie dostępne jej środki wychowawcze (rozmowa z rodzicami, konsekwencje z statutu i/lub regulaminu wobec ucznia) i interwencje pedagogiczne, a ich zastosowanie nie przynosi pożądanych rezultatów (np. nie ma zmian postawy ucznia).

18) Kontaktu z Policją wymagają wszelkie sytuacje, w których zostało naruszone prawo (np. groźby karalne, świadome publikowanie nielegalnych treści, rozpowszechnianie nagich zdjęć z udziałem małoletnich). Za zgłoszenie powinien odpowiadać dyrektor szkoły.

19) Kontakt z dostawcą usługi może być wskazany w celu usunięcia z sieci kompromitujących lub krzywdzących materiałów.

**2. Dostęp do treści szkodliwych, niepożądanych i nielegalnych – procedura reagowania**

1) Zagrożenie łatwym dostępem do treści szkodliwych, niedozwolonych, nielegalnych i niebezpiecznych dla zdrowia (pornografia, treści obrazujące przemoc i promujące działania szkodliwe dla zdrowia i życia dzieci, popularyzujące ideologię faszystowską i działalność niezgodną z prawem, nawoływanie do samookaleczeń i samobójstw, korzystania z narkotyków; niebezpieczeństwo werbunku dzieci i młodzieży do organizacji nielegalnych i terrorystycznych).

2) Zgłaszanie nielegalnych treści: dyzurnet@dyzurnet.pl, tel. 801 615 005, Policja 997.

3) Reakcja szkoły w przypadku pozyskania wiedzy o wystąpieniu zagrożenia będzie zależna od tego, czy:

a) treści te można bezpośrednio powiązać z uczniami danej szkoły, czy też nie,

b) treści nielegalne lub szkodliwe nie mają związku z uczniami danej szkoły, lecz wymagają kontaktu szkoły z odpowiednimi służbami.

4) W pierwszej kolejności należy zabezpieczyć dowody w formie elektronicznej (pliki z treściami niedozwolonymi, zapisy rozmów w komunikatorach, e-maile, zrzuty ekranu), znalezione w Internecie lub w komputerze dziecka. Zabezpieczenie dowodów jest zadaniem rodziców lub opiekunów prawnych dziecka, w czynnościach tych może wspomagać ich przedstawiciel szkoły posiadający odpowiednie kompetencje techniczne. W przypadku sytuacji a) rozwiązanie leży po stronie szkoły, zaś b) należy rozważyć zgłoszenie incydentu na Policję oraz zgłosić go do serwisu Dyżurnet (dyzurnet.pl).

5) W identyfikacji sprawców kluczowe znaczenie odgrywać będą zgromadzone dowody. W procesie udostępniania nielegalnych i szkodliwych treści małoletnim występują na ogół: twórca treści (np. pornografii) oraz osoby, która udostępniły je dziecku. Często osobami tymi są rówieśnicy – uczniowie tej samej szkoły czy klasy, dzieci sąsiadów. Konieczne jest poinformowanie wszystkich rodziców lub opiekunów dzieci uczestniczących w zdarzeniu o sytuacji i roli ich dzieci.

6) W przypadku udostępniania (dzielenia się) treści opisanych wcześniej jako szkodliwych/niedozwolonych/nielegalnych i niebezpiecznych dla zdrowia przez ucznia należy przeprowadzić z nim rozmowę na temat jego postępowania i w jej trakcie uzmysłowić mu szkodliwość prowadzonych przez niego działania. Działania szkoły powinny koncentrować się jednak na aktywnościach wychowawczych. W przypadku upowszechniania przez sprawców treści nielegalnych należy złożyć zawiadomienie o zdarzeniu na Policję.

7) Dzieci - ofiary i świadków zdarzenia – należy od pierwszego etapu interwencji – otoczyć opieką psychologiczno-pedagogiczną. Rozmowa z dzieckiem powinna się odbywać w warunkach jego komfortu psychicznego, z poszanowaniem poufności i podmiotowości ucznia ze względu na fakt, iż kontakt z treściami nielegalnymi może mieć bardzo szkodliwy wpływ na jego psychikę. W jej trakcie należy ustalić okoliczności uzyskania przez ofiarę dostępu do w/w treści.

8) Należy koniecznie powiadomić ich rodziców lub opiekunów prawnych o zdarzeniu i uzgodnić z nimi podejmowane działania i formy wsparcia dziecka. Działania szkoły w takich przypadkach powinna cechować poufność i empatia w kontaktach ze wszystkimi uczestnikami zdarzenia oraz udzielającymi wsparcia.

9) W przypadku kontaktu dziecka z treściami szkodliwymi należy dokładnie zbadać sposób, w jaki nastąpił kontakt dziecka z nimi. Poszukiwanie przez dziecko tego typu treści w sieci lub podsuwanie ich dziecku przez innych może być oznaką niepokojących incydentów ze świata rzeczywistego np. kontakty z osobami handlującymi narkotykami czy proces rekrutacji do sekty lub innej niebezpiecznej grupy.

10) W przypadku, gdy informacja na temat zdarzenia dotrze do środowiska rówieśniczego ofiary – w klasie, czy szkole, wskazane jest podjęcie działań edukacyjnych i wychowawczych.

11) W przypadku naruszenia prawa np. rozpowszechniania materiałów pornograficznych z udziałem nieletniego lub prób uwiedzenia małoletniego w wieku do 15 lat przez osobę dorosłą należy – w porozumieniu z rodzicami dziecka – niezwłocznie powiadomić Policję.

12) Kontakt z treściami szkodliwymi lub niebezpiecznymi może wywołać potrzebę skorzystania przez ofiarę ze specjalistycznej opieki psychologicznej. Decyzja o takim kontakcie i skierowaniu na terapię musi zostać podjęta w porozumieniu z rodzicami/opiekunami prawnymi dziecka.