2. Procedury na wypadek wystąpienia zagrożeń bezpieczeństwa cyfrowego.

2.2 Cyberprzemoc – procedura reagowania

2.2 CYBERPRZEMOC

Podstawy prawne uruchomienia procedury zawiera Kodeks Karny, Statut szkoły, Regulamin szkoły. Rodzaj zagrożenia objętego procedurą Cyberprzemoc — przemoc z użyciem technologii informacyjnych i komunikacyjnych, głównie Internetu 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 sieci pod kogoś wbrew jego woli. Do działań określanych mianem cyberprzemocy wykorzystywane są głównie: poczta elektroniczna, czaty, komunikatory, strony internetowe, blogi, serwisy społecznościowe, grupy dyskusyjne, serwisy SMS i MMS.

Telefony alarmowe krajowe i lokalne:

Telefon Zaufania dla Dzieci i Młodzieży -- 116 111

Telefon dla Rodziców i Nauczycieli w sprawie Bezpieczeństwa Dzieci — 800 100 100.

Przyjęcie zgłoszenia i ustalenie okoliczności zdarzenia

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.

Jeśli zgłaszającym jest ofiara cyberprzemocy, podejmując działania przede wszystkim należy okazać wsparcie, z zachowaniem jej podmiotowości i 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). 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 kapusiem, obawa o własne bezpieczeństwo). 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 nie dopuszczenie do eskalacji tego typu zachowań w stronę cyberprzemocy).

Opis okoliczności, analiza, zabezpieczenie dowodów.

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. Identyfikacja sprawcy(--ów) Identyfikacja sprawcy(o w) 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. 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)

Aktywności wobec sprawców zdarzenia ze szkoły/ spoza szkoły

Gdy sprawca cyberprzemocy jest znany i jest on uczniem szkoły, pedagog 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). 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. Aktywności wobec ofiar zdarzenia W pierwszej kolejności należy udzielić wsparcia ofierze. Musi się ona czuć bezpieczna i chroniona przez dorosłych. Na poczucie bezpieczeństwa dziecka wpływa fakt, z e wie ono, iż szkoła podejmuje kroki w celu rozwiązania problemu. 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 z e zostaną podjęte odpowiednie procedury interwencyjne. Należy poinformować ucznia o krokach, jakie może podjąć szkoła i sposobach, w jaki może zapewnić mu bezpieczeństwo. 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 etc.). Pomoc ofierze nie może kończyć się w momencie zakończenia procedury. Warto monitorować sytuację, „czuwając " 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. W działania wobec ofiary należy także włączyć rodziców/opiekunów 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 wyraz a zgody, należy omówić z nim jego obawy, a jeśli to nie pomaga powołać się na obowiązujące nas zasady i przekazać informację rodzicom. 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 możliwości zgłoszenia sprawy Policji.

Aktywności wobec świadków .

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. Współpraca z Policją i sądami rodzinnymi 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). 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.

Współpraca z dostawcami Internetu i operatorami telekomunikacyjnymi.

Kontakt z dostawcą usługi może być wskazany w celu usunięcia z sieci kompromitujących lub krzywdzących materiałów. Do podjęcia takiego działania stymuluje administratora serwisu art. 14 Ustawy z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną.

Opracował

Piotr Lisiak