Procedury reagowania w przypadku wystąpienia w szkole zagrożeń bezpieczeństwa cyfrowego.

Wstęp

Czym jest zagrożenie bezpieczeństwa cyfrowego?

To 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)

Cyberprzemoc – to we współczesnym świecie jedno z najczęściej stosowanych zagrożeń, to przemoc z użyciem technologii informacyjnych i komunikacyjnych, głównie Internetu oraz telefonów komórkowych.

Podstawowe formy zjawiska cyberprzemocy 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, media społecznościowe, grupy dyskusyjne, SMS- y i MMS- y.

Niniejszy dokument zawiera dziewięć podstawowych zagrożeń bezpieczeństwa cyfrowego w środowisku szkolnym, którym przypisano opracowane według jednego standardu opisu procedury reagowania:

1. Dostęp do treści szkodliwych, niepożądanych, nielegalnych
2. Cyberprzemoc
3. Naruszenia prywatności dotyczące nieodpowiedniego lub niezgodnego z prawem wykorzystania danych osobowych lub wizerunku dziecka i pracownika szkoły
4. Zagrożenia dla zdrowia dzieci w związku z nadmiernym korzystaniem z Internetu
5. Nawiązywanie niebezpiecznych kontaktów w Internecie - uwodzenie, zagrożenie pedofilią.
6. Seksting, prowokacyjne zachowania i aktywność seksualna jako źródło dochodu osób nieletnich.

7. Bezkrytyczna wiara w treści zamieszczone w Internecie, nieumiejętność odróżnienia treści prawdziwych od nieprawdziwych, szkodliwość reklam
8. Łamanie prawa autorskiego
9. Zagrożenia bezpieczeństwa technicznego sieci, komputerów i zasobów.

Pkt 1

Dostęp do treści szkodliwych, niepożądanych, nielegalnych - procedura reagowania.

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)

W przypadku gdy:

szkoła pozyska wiedzę o wystąpieniu zagrożenia musi ustalić czy:

- treści te można bezpośrednio powiązać z uczniami szkoły
- treści nielegalne lub szkodliwe nie mają związku z uczniami szkoły, lecz wymagają kontaktu szkoły z odpowiednimi służbami.
- W przypadku ustalenia, że niebezpieczne treści można powiązać z uczniami szkoły, należy:
  - Zabezpieczyć dowody - pedagog, wychowawca lub nauczyciel informatyk, w obecności dyrektora szkoły powinien zabezpieczyć zgłoszone dowody w formie elektronicznej tj. wszystkie pliki z niedozwolonymi treściami, zapisy rozmów w komunikatorach, e-maile, zrzuty ekranu.
- W przypadku zaistnienia przypadku zagrożenia poza szkołą, zabezpieczenie dowodów jest zadaniem rodziców lub opiekunów prawnych ucznia.

W obydwu przypadkach należy rozważyć dwa rozwiązania tj:

- wewnętrzne szkolne – rozmowy dyscyplinujące, zaproszenie i poinformowanie o sytuacji rodziców, przedstawienie informacji dotyczących konsekwencji prawnych (wychowawca, pedagog), zajęcia wychowawcze

- zewnętrzne – poinformowanie policji o zaistniałej sytuacji przy pełnym, bezpośrednim kontakcie z rodzicami ucznia (w przypadku rozpowszechniania pornografii)

Działania szkoły wobec sprawców zdarzenia:

- W przypadku udostępniania przez ucznia niedozwolonych treści, wychowawca, pedagog/ psycholog dyrektor szkoły, przeprowadza z uczniem rozmowę dyscyplinującą i uświadamiającą szkodliwość działania.
- W przypadku upowszechniania przez sprawców treści nielegalnych (np. pornografii dziecięcej lub prób uwiedzenia małoletniego w wieku do 15 lat przez osobę dorosłą), dyrektor szkoły zobowiązany jest złożyć zawiadomienie o zdarzeniu na Policję.

Działania szkoły wobec ofiar zdarzenia:

- Ofiary i świadków zdarzenia - na terenie szkoły- należy otoczyć opieką psychologiczno-pedagogiczną.
- Rozmowę z uczniem przeprowadza pedagog i psycholog szkolny. Rozmowa z uczniem 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.
- Szkoła musi koniecznie powiadomić rodziców lub opiekunów prawnych o zaistniałym zdarzeniu, uzgodnić podejmowane działania i formy wsparcia ucznia. Działania szkoły w takich przypadkach powinna cechować poufność i empatia w kontaktach z wszystkimi uczestnikami zdarzenia oraz udzielającymi wsparcia.
- W przypadku kontaktu ucznia z treściami szkodliwymi należy dokładnie zbadać sposób, w jaki nastąpił kontakt ucznia z nimi (poszukiwanie 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).
- W przypadku, gdy informacja na temat zdarzenia dotrze do środowiska rówieśniczego ofiary, wychowawca, pedagog, psycholog szkolny zobowiązani są do podjęcia działań edukacyjnych i wychowawczych (spotkania z uczniami, zajęcia wychowawcze, doraźne spotkania wg potrzeb)

Współpraca ze służbami i placówkami specjalistycznymi:

- 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 ucznia.
- Pedagog szkolny/ psycholog szkolny powinien przygotować wykaz instytucji pomocowych w tym zakresie.

Pkt 2

Cyberprzemoc

Zagrożenie to dotyczy przemocy 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, media społecznościowe, grupy dyskusyjne, SMS i MMS

Przypadek cyberprzemocy może zostać ujawniony przez ofiarę, świadka (np. innego ucznia, nauczyciela, rodzica) lub osobę bliską ofierze (np. rodzice, rodzeństwo, przyjaciele).

W przypadku gdy:

- 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 wzbudzić podejrzenia sprawcy (np. wywoływać ucznia z lekcji do dyrektora)
- Jeśli osobą zgłaszającą nie jest ofiara, prowadzący rozmowę – pedagog/ psycholog, nauczyciel/ wychowawca prosi o opis sytuacji, także z zachowaniem podmiotowości i poszanowaniem uczuć osoby zgłaszającej (np. strach, 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).

Szkoła powinna:

- 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 zadbać o bezpieczeństwo osób zaangażowanych w problem.
- Przeprowadzić rozmowę z ofiarą, która najczęściej domyśla się, kto stosuje wobec niego cyberprzemoc.
- Jeśli ustalenie sprawcy nie jest możliwe, a w ocenie kadry pedagogicznej jest to konieczne, dyrektor szkoły kontaktuje się z Policją. Bezwzględnie należy zgłosić rozpowszechnianie nagich zdjęć osób poniżej 18 roku życia (art. 202 par. 3 KK)

Działania szkoły wobec sprawcy zdarzenia:

- Gdy sprawca cyberprzemocy jest znany i jest on uczniem szkoły, pedagog/ psycholog szkolny powinien przeprowadzić z nim rozmowę dyscyplinującą. Rozmowa taka ma również służyć ustaleniu okoliczności zdarzenia, jego wspólnej analizie (w tym np. przyjrzeniu się przyczynom), a także próbie rozwiązania sytuacji konfliktowej (w tym sposobów zadośćuczynienia ofiarom cyberprzemocy).
- Uczeń / sprawca cyberprzemocy powinien podlegać również sankcjom przewidzianym w zapisach wewnętrznych dokumentów szkolnych np. Statucie Szkoły.
- Pedagog/ psycholog szkolny spisuje z uczniem kontrakt, z którego jest terminowo rozliczany.

Działania szkoły wobec ofiary zdarzenia:

- W przypadku ujawnienia ofiary zdarzenia szkoła powinna udzielić wsparcia ofierze. Musi się Ona czuć bezpieczna i zaopiekowana przez pracowników szkoły. Na poczucie

bezpieczeństwa ofiary/ ucznia musi wpływać poczucie, iż szkoła podejmuje kroki w celu rozwiązania Jego problemu.

- Należy poinformować ucznia o krokach, jakie może podjąć szkoła i sposobach, w jaki może zapewnić mu bezpieczeństwo.
- Należy skontaktować się rodzicami /opiekunami 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 uczeń nie wyraża zgody, należy omówić z nim jego obawy, a jeśli to nie pomaga powołać się na obowiązujące szkołę zasady i przekazać informację rodzicom.
- W trakcie rozmowy z uczniem i/lub jego rodzicami/opiekunami -jeśli jest to wskazane- szkoła powinna zaproponować pomoc specjalistów zewnętrznych
- W trakcie rozmowy z rodzicami / prawnymi opiekunami ofiary, szkoła winna przekazać informację o możliwości i zasadach zgłoszenia sprawy Policji.
- Po zakończeniu działań, szkoła jeszcze powinna monitorować sytuację, Pedagog/ psycholog, wychowawca powinni „czuwać" nad bezpieczeństwem ofiary, zwracać uwagę czy nie są podejmowane wobec niej dalsze działania przemocowe, obserwować, jak uczeń radzi sobie w grupie po ujawnionym incydencie cyberprzemocy.

Współpraca szkoły ze służbami i placówkami specjalistycznymi:

Wystąpienie zjawiska cyberprzemocy nie jest jednoznaczne z koniecznością zaangażowania Policji i Sądu Rodzinnego dlatego:

- Szkoła winna umożliwiać rozwiązania sytuacji problemowych na poziomie pracy wychowawczej.
- Szkoła powinna powiadomić odpowiednie służby tylko w przypadku, gdy wykorzysta wszystkie dostępne środki wychowawcze, a ich zastosowanie nie przyniosło pożądanych rezultatów
- Kontaktu z Policją winny wymagać wszystkie sytuacje, w których zostało naruszone prawo (np. groźby karalne, świadome publikowanie nielegalnych treści, rozpowszechnianie nagich zdjęć z udziałem małoletnich, treści pornograficzne). Za zgłoszenie powinien odpowiadać dyrektor szkoły.

Pkt 3

Naruszenia prywatności dotyczące nieodpowiedniego lub niezgodnego z prawem wykorzystania danych osobowych lub wizerunku dziecka i pracownika szkoły

Zagrożenie to polega na naruszeniu prywatności ucznia lub pracownika szkoły poprzez nieodpowiednie lub niezgodne z prawem wykorzystanie danych osobowych lub wizerunku. Najczęstszymi formami wyłudzenia lub kradzieży danych jest przejęcie profilu na portalu społecznościowym w celu dyskredytacji lub naruszenia dobrego wizerunku ofiary (np. publikacja zdjęć intymnych) szantażu, dokonania zakupów i innych transakcji finansowych. Często naruszenia prywatności łączy się z cyberprzemocą.

W przypadku gdy:

- Sprawcą jest uczeń - kolega ofiary ze szkoły czy klasy, uczniowie lub rodzice winni skontaktować się z dyrektorem szkoły, wychowawcą lub pedagogiem/ psychologiem szkolnym
- W przypadku, gdy do naruszenia prywatności poprzez kradzież, wyłudzenie danych osobowych wykorzystanie wizerunku ucznia dochodzi ze strony dorosłych osób trzecich, rodzice winni skontaktować się bezpośrednio z Policją i powiadomić o tym szkołę (zgodnie z Kodeksem Karnym ściganie następuje tu na wniosek pokrzywdzonego).
- W przypadku zgłoszenia zdarzenia w szkole, należy zabezpieczyć dowody nieodpowiedniego lub niezgodnego z prawem działania - w formie elektronicznej (e-mail, zrzut ekranu, konwersacja w komunikatorze lub sms). Należy dokonać zmian tych danych identyfikujących, które zależą od ofiary, tj. haseł i loginów lub kodów dostępu do platform i portali internetowych, tak aby uniemożliwić kontynuację procederu naruszania prywatności - w działaniu tym ucznia powinna wspierać osoba dorosła (nauczyciel, pedagog, psycholog, wychowawca)
- Jeśli wykradzione dane zostały wykorzystane w celu naruszenia dobrego wizerunku ofiary, bądź w innych celach niezgodnych z prawem, szkoła powinna dążyć do wyjaśnienia tych działań i usunięcia ich skutków, także tych widocznych w Internecie.
- Likwidacja stron internetowych czy profili w portalach społecznościowych, która wymagać będzie interwencji w zebrane dowody musi odbywać się za zgodą Policji (o ile została powiadomiona).

- Szczególnej uwagi wymagają incydenty kradzieży tożsamości w celu posłużenia się nią np. podczas zakupu towarów *online* lub dokonania transakcji finansowych. W tym przypadku ofiara powinna skontaktować się ze sklepem lub pożyczkodawcą i wyjaśnić charakter zdarzenia.
- W przypadku znanego sprawcy (ucznia, pracownika szkoły) szkoła powinna dążyć do rozwiązania problemu w ramach wewnętrznych procedur i działań wychowawczo – profilaktycznych.
- O wszystkich czynach niezgodnych z prawem należy powiadomić Policję.

Działania szkoły wobec ofiary:

- Nieletnią ofiarę incydentów należy otoczyć – w porozumieniu z rodzicami/opiekunami prawnymi - opieką pedagogiczno-psychologiczną i powiadomić o działaniach podjętych w celu usunięcia skutków działania sprawcy (np. usunięcie z Internetu intymnych zdjęć ofiary, zablokowanie dostępu do konta w portalu społecznościowym).
- Jeśli kradzież tożsamości, bądź naruszenie dobrego wizerunku ofiary jest znane tylko jej i rodzicom, szkoła winna zapewnić poufność działań, tak aby informacje narażające ofiarę na naruszenie wizerunku nie były rozpowszechniane.
- W przypadku, gdy do naruszenia prywatności poprzez kradzież, wyłudzenie danych osobowych wykorzystanie wizerunku ucznia dochodzi ze strony dorosłych osób trzecich, rodzice winni skontaktować się bezpośrednio z Policją i powiadomić o tym szkołę (zgodnie z Kodeksem Karnym ściganie następuje tu na wniosek pokrzywdzonego).

Działania szkoły wobec sprawcy:

- Gdy sprawcą incydentu jest uczeń szkoły, należy wobec niego – w porozumieniu z rodzicami – podjąć działania profilaktyczne, zmierzające do uświadomienia nieodpowiedniego i nielegalnego charakteru czynów, jakich dokonał.
- Dyrekcja szkoły winna podjąć decyzje w sprawie powiadomienia o incydencie Policji, biorąc pod uwagę rodzaj czynu oraz wiek sprawcy, jego dotychczasowe zachowanie, postawę po odkryciu incydentu , opinie wychowawcy i pedagoga.

Współpraca ze służbami i instytucjami zewnętrznymi

- Gdy naruszenie prywatności, czy wyłudzenie lub kradzież tożsamości skutkują wyrządzeniem ofierze szkody majątkowej lub osobistej, rodzice ucznia winni o tym powiadomić Policję.
- W przypadku konieczności podejmowania dalszych działań pomocowych wobec ofiary, można skierować ucznia, za zgodą i we współpracy z rodzicami/opiekunami prawnymi, do placówki specjalistycznej, np. terapeutycznej.

Pkt 4

Zagrożenia dla zdrowia dzieci w związku z nadmiernym korzystaniem z Internetu

Procedura dotyczy problemu infoholizmu (siecioholizmu) czyli nadmiernego, obejmującego niekiedy niemal całą dobę korzystania z zasobów Internetu i gier komputerowych (najczęściej sieciowych) i portali społecznościowych. Jego negatywne efekty polegają na pogarszaniu się stanu zdrowia fizycznego (np. choroby oczu, padaczka ekranowa, choroby kręgosłupa) i psychicznego (irytacja, rozdrażnienie, spadek sprawności psychofizycznej, a nawet depresja), zaniedbywaniu codziennych czynności, oraz osłabianiu relacji rodzinnych i społecznych.

W przypadku gdy:

- Nauczyciel/ wychowawca zauważy, iż uczeń przejawia cechy infoholizmu koniecznie podejmuje działania pomocowe – przeprowadza rozmowę z uczniem, informuje o problemie pedagoga / psychologa, informuje o zaistniałej sytuacji rodziców – prawnych opiekunów ucznia.
- Osoba, której problem dotyczy, powinna zostać otoczona zindywidualizowaną opieką pedagoga/psychologa szkolnego.

Działania szkoły wobec ucznia

- Wychowawca, pedagog / psycholog zaprasza na rozmowę ucznia, informuje o problemie rodziców/ opiekunów. Próbuje zdiagnozować poziom zagrożenia, określić przyczyny popadnięcia w nałóg (np. problemy domowe, brak sukcesów, edukacyjnych, izolacja w środowisku rówieśniczym).
- W przypadku nadmiernego infoholizmu i widocznych skutków ubocznych zdrowotnych i psychicznych tj. brak snu, brak chęci do posiłków, rezygnacja

z dawnych zainteresowań, gorsze oceny, zaburzenie relacji rodzinnych, zaburzenie relacji rówieśniczych, izolacja), wychowawca lub pedagog przedstawia rodzicom możliwości pomocy min. skierowania ucznia (za zgodą i we współpracy z rodzicami / opiekunami) do placówki specjalistycznej, np. terapeutycznej.

- Jeśli świadkami problemu są rówieśnicy ucznia, należy im w rozmowie zwrócić uwagę na negatywne aspekty nadmiernego korzystania z zasobów Internetu oraz zaapelować o wsparcie dla ucznia dotkniętego problemem.
- Prowadzić na terenie szkoły działania profilaktyczno – wychowawcze

Współpraca ze służbami i placówkami specjalistycznymi

- W przypadku zdiagnozowania przez nauczyciela, wychowawcę, pedagoga, psychologa uzależnienia od korzystania z zasobów Internetu, uczeń powinien zostać skierowany we współpracy z rodzicami/opiekunami prawnymi, do placówki specjalistycznej oferującej program terapeutyczny.

Pkt 5

Nawiązywanie niebezpiecznych kontaktów w Internecie - uwodzenie, zagrożenie pedofilią.

Zagrożenie obejmuje kontakty osób dorosłych z małoletnimi w celu zainicjowania znajomości prowadzących do wyłudzenia poufnych informacji, nawiązania kontaktów seksualnych, skłonienia dziecka do zachowań niebezpiecznych dla jego zdrowia i życia lub wyłudzenia własności (np. danych, pieniędzy, cennych przedmiotów rodzinnych). Kluczowe znaczenie w działaniach szkoły ma czas reakcji - szybkość przeciwdziałania zagrożeniu ze względu na niezwykle szkodliwe konsekwencje realizacji kontaktu online, przeradzającego się w zachowania w świecie rzeczywistym: uwiedzenie i wykorzystanie seksualne, kidnaping, a także wyłudzenie pieniędzy czy przedmiotów dużej wartości. W przypadkach niebezpiecznych kontaktów inicjowanych w Internecie może dochodzić do zagrożenia życia i zdrowia ucznia/ dziecka, szantażu i przymusu realizacji czynności seksualnych.

W przypadku gdy:

- Pozyskamy informacje o zaistniałej sytuacji, należy zidentyfikować i zabezpieczyć w szkole, w formie elektronicznej dowody działania dorosłego sprawcy uwiedzenia

(zapisy rozmów w komunikatorach, na portalach społecznościowych; zrzuty ekranowe, zdjęcia, wiadomości e-mail).

- Dyrektor szkoły bezzwłocznie powiadamia Policję o wystąpieniu zdarzenia.
- Szkoła nie podejmuje samodzielnych działań w celu dotarcia do sprawcy, jednocześnie udziela wszelkiej pomocy organom ścigania min. zabezpieczyć i przekazać zebrane dowody. Identyfikacja sprawcy wykracza poza kompetencje szkoły!

Działania szkoły wobec ofiary zdarzenia (reakcja szkoły na zdarzenie)

- Ofiara zdarzenia powinna zostać otoczona opieką pedagoga i psychologa. Uczeń powinien mieć wsparcie, zapewnione poczucia bezpieczeństwa.
- Szkoła ma obowiązek o zaistniałej sytuacji powiadomić rodziców/ prawnych opiekunów ucznia
- Rozmowa z uczniem powinna przebiegać w warunkach komfortu psychicznego.
- Rozmowa powinna przebiegać w życzliwej, spokojnej atmosferze, w czasie której próbujemy uzyskać jak najwięcej informacji o sprawcy
- Pedagog/ psycholog informuje o zaistniałej sytuacji dyrektora szkoły, który powiadamia o zdarzeniu Policję.
- Należy upewnić się, że kontakt ofiary ze sprawcą został przerwany, a uczeń odzyskał poczucie bezpieczeństwa.
- Wszelkie działania wobec ucznia powinny być uzgadniane z rodzicami / prawnymi opiekunami ucznia i inicjowane za ich zgodą.
- Szkoła powinna również udzielić ofierze wsparcia pedagogicznego i psychologicznego w przypadku zaobserwowania antyzdrowotnych i zagrażających życiu zachowań uczniów (samookaleczenia, zażywanie substancji psychoaktywnych).

Działania szkoły wobec sprawcy zdarzenia (reakcja szkoły na zdarzenie)

- Nie należy podejmować aktywności zmierzających bezpośrednio do kontaktu ze sprawcą. Zadaniem szkoły jest zebranie dowodów i opieka nad ofiarą oraz świadkami.

Współpraca z Policją i Sądami Rodzinnymi.

- obowiązkiem szkoły jest powiadomienie Policji lub Sądu Rodzinnego
- Telefon Zaufania dla Dzieci i Młodzieży - **116 111,** https://116111.pl/

- Telefon dla Rodziców i Nauczycieli w sprawie Bezpieczeństwa Dzieci – **800 100 100,** https://800100100.pl/
- **Zgłaszanie nielegalnych treści:** dyzurnet@dyzurnet.pl , dyzurnet.pl **801 615 005**

Pkt 6

Seksting.

Prowokacyjne zachowania i aktywność seksualna jako źródło dochodu osób nieletnich.

Seksting to przesyłanie drogą elektroniczną w formie wiadomości MMS lub publikowanie np. na portalach (społecznościowych) prywatnych treści, głównie zdjęć, o kontekście seksualnym, erotycznym. Zgłoszeń przypadków sekstingu dokonują głównie rodzice lub opiekunowie prawni ofiary. Delikatny charakter sprawy, a także odpowiedzialność karna sprawcy, wymagają zachowania daleko posuniętej dyskrecji i profesjonalnej reakcji. Niekiedy zgłoszenia dokonują ofiary lub osoby je znające.

Wyróżniamy 3 podstawowe rodzaje sekstingu, które skutkują koniecznością realizacji zmodyfikowanych procedur reagowania:

- Rodzaj 1. Wymiana materiałów o charakterze seksualnym następuje tylko w ramach związku między dwojgiem rówieśników. Materiały nie uległy rozprzestrzenieniu dalej.
- Rodzaj 2. Materiały o charakterze seksualnym zostały rozesłane większej liczbie osób, jednak nie dochodzi do cyberprzemocy na tym tle. Młodzież traktuje materiał jako formę wyrażenia siebie.
- Rodzaj 3. Materiały zostały rozesłane większej liczbie osób w celu upokorzenia osoby na nich zaprezentowanej – lub zostają rozpowszechnione omyłkowo, jednak są zastosowane jako narzędzie cyberprzemocy.

W przypadku gdy: **Opis okoliczności i zabezpieczenie dowodów**

- Przypadek sekstingu zostanie upowszechniony w środowisku rówieśniczym – np. poprzez media społecznościowe czy MMS lub publikację w portalu społecznościowym, szkoła zobowiązana jest podjąć działania wychowawcze, uświadamiające negatywne aspekty moralne sekstingu oraz narażanie się na poniesienie odpowiedzialności prawnej.

Działania szkoły wobec ofiary:

- Szkoła otacza ofiarę pomocą pedagogiczno – psychologiczną oraz zabezpiecza dostępne dowody

- Rozmowa na temat identyfikacji potencjalnego sprawcy powinna być realizowana w warunkach komfortu psychicznego dla ucznia/ dziecka – ofiary sekstingu, z szacunkiem dla Niego.
- Wychowawca klasy, pedagog / psycholog proponują odpowiednie działania wychowawcze w przypadku upublicznienia przypadku sekstingu w środowisku rówieśniczym.
- Szkoła – w marę możliwości – stara się zabezpieczyć dowody tj. przesyłane zdjęcia, zrzuty ekranów portali, w których opublikowano zdjęcie(-a). Jako, że seksting jest karalny, skrupulatność i wiarygodność dokumentacji ma duże znaczenie.
- Szkoła – wychowawca, pedagog/ psycholog zachowuje zasady dyskrecji, szczególnie w środowisku rówieśniczym ofiary.

Działania szkoły wobec sprawcy:

- Zidentyfikowani małoletni sprawcy sekstingu winni zostać wezwani do dyrekcji szkoły, gdzie zostaną im przedstawione dowody ich aktywności.
- Niezależnie od zakresu negatywnych zachowań i działań wszyscy sprawcy powinni otrzymać wsparcie pedagogiczne i psychologiczne.
- Szkoła kontaktuje się z rodzicami uczniów, informuje ich o zaistaniałej sytuacji, zaprasza na spotkanie.
- Konieczne są także rozmowy ze sprawcami w obecności ich rodziców zaproszonych do szkoły.
- Dalsze działania poza zapewnieniem wsparcia i opieki psychologiczno-pedagogicznej nie są konieczne, jednak istotne jest pouczenie sprawców zdarzenia, że dalsze rozpowszechnianie materiałów może być nielegalne i będzie miało ostrzejsze konsekwencje, w tym prawne.
- Niektóre tego typu materiały mogą zostać uznane za pornograficzne. Rozpowszechnianie materiałów pornograficznych z udziałem nieletnich jest przestępstwem ściganym z urzędu (art. 202 Kodeksu Karnego), **dlatego też dyrektor szkoły zgłosza incydentu na Policję i/lub do sądu rodzinnego.**
- Wszelkie działania wobec sprawców incydentu powinny być podejmowane w porozumieniu z ich rodzicami lub opiekunami prawnymi.
- W sytuacji zaistnienia znamion cyberprzemocy, należy dodatkowo zastosować procedurę: Cyberprzemoc.

Współpraca z Policją, Sądem i placówkami specjalistycznymi:

- W przypadku publikacji lub upowszechniania zdjęć o charakterze pornografii dziecięcej (co jest wykroczeniem ściganym z urzędu) dyrektor szkoły jest zobowiązany do powiadomienia o tym zdarzeniu Policji i/ lub Sadu Rodzinnego
- Kontakt ofiar z placówkami specjalistycznymi może okazać się konieczny w indywidualnych przypadkach. O skierowaniu do nich decyzję powinien podjąć psycholog/pedagog szkolny wspólnie z rodzicami/opiekunami prawnymi ofiary.

Pkt 7

Bezkrytyczna wiara w treści zamieszczone w Internecie, nieumiejętność odróżnienia treści prawdziwych od nieprawdziwych, szkodliwość reklam

Zagrożenie dotyczy braku umiejętności odróżniania informacji prawdziwych od nieprawdziwych publikowanych w Internecie, Bezkrytyczne uznawanie za prawdę publikowanych w forach internetowych informacji. Taka postawa dzieci prowadzić może do zagrożeń życia i zdrowia (np. stosowania wyniszczającej diety, samookaleczeń), skutkować rozczarowaniami i porażkami życiowymi (w efekcie korzystania z fałszywych informacji), utrudniać lub uniemożliwiać osiąganie dobrych wyników w edukacji, a także utrwalenia się u ucznia ambiwalentnych postaw moralnych.

W przypadku gdy:

- Uczniowie nie umiejący odróżniać prawdy od fałszu informacji publikowanych w Internecie winni być identyfikowani przez nauczycieli i wychowawców w trakcie lekcji wszystkich przedmiotów.
- Szkoła – nauczyciel/ wychowawca zauważy, że taka postawa ujawnia się podczas przygotowania prac domowych – sytuacja jest stosunkowo łatwa do zidentyfikowania przez oceniającego je nauczyciela.

Działania szkoły:

- Posługiwanie się nieprawdziwymi informacjami zaczerpniętymi z Internetu w procesie dydaktycznym – podczas lekcji lub w zadaniach domowych, każdorazowo winno być zauważone przez nauczyciela, przeanalizowane i sprostowane.
- Szkoła powinna prowadzić działania profilaktyczne - edukację medialną (informacyjną), np. w trakcie zajęć nieinformatycznych (np. historii, języka polskiego,) przez wszystkie

lata nauki ucznia w szkole lub lekcji ukierunkowanych na zdobywanie przez dzieci i młodzież kompetencji informatycznych. Edukacja medialna może być prowadzona również na zajęciach pozalekcyjnych.

Pkt 8

Łamanie prawa autorskiego

Zagrożenie dotyczy ryzyka poniesienia odpowiedzialności cywilnej lub karnej z tytułu naruszenia prawa autorskiego albo negatywnych skutków pochopnego spełnienia nieuzasadnionych roszczeń *(Kodeks Karny)*

Najczęstszym przypadkiem, w którym szkoła może zetknąć się z problemem naruszenia praw autorskich jest użycie materiałów prawnie chronionych na stronach internetowych szkoły, poza zakresem dozwolonego użytku, przez jej pracowników bądź uczniów. W przypadku naruszeń dokonanych przez uczniów szkoła nie może występować w roli sędziego - dochodzenie roszczeń należy pozostawić osobom uprawnionym. Szkoła powinna na każdym etapie skupić się na swojej roli edukacyjno-wychowawczej poprzez organizację lekcji na temat praw autorskich, zwracając przy tym uwagę, że powinny one rzeczowo i konkretnie informować, jakie czyny są dozwolone, a jakie zabronione prawem.

W przypadku gdy:

- szkoła pozyska informacje w w/w temacie powinna zweryfikować wszystkie informacje podawane przez zgłaszającego
- sprawdzić, czy okoliczności podane w zgłoszeniu faktycznie miały miejsce
- Zgłosić sprawę odpowiednim służbom (Policja, Prokuratura). **Należy pamiętać, iż Szkoła nie powinna i nie może wyręczać tych organów w ich rolach, zatem nie może też wkraczać w ich kompetencje!**

Działania szkoły:

- Szkoła powinna skupić się na swojej roli wychowawczej i edukacyjnej.
- Szkoła powinna rozważyć zorganizowanie szkoleń lub warsztatów z zakresu „prawa autorskiego w intrenecie” dla wszystkich zainteresowanych osób w szkole – zajęcia wychowawcze dla uczniów, konferencje szkoleniowe dla nauczycieli.
- O dochodzeniu roszczeń wobec sprawcy decyduje sam uprawniony (tzn. autor lub inna osoba, której przysługują prawa autorskie). Szkoła powinna natomiast podjąć

działania o charakterze edukacyjno-wychowawczym, polegające na obszernym wyjaśnieniu, na czym polegało naruszenie oraz przekazaniu wiedzy, jak do naruszeń nie dopuścić w przyszłości.

- Jeżeli osobą, której prawa autorskie naruszono jest uczeń, szkoła może rozważyć możliwość wystąpienia w roli mediatora, aby stosownie do okoliczności ułatwić stronom ugodowe lub inne kompromisowe zakończenie powstałego sporu.

Należy pamiętać iż: „Prawo autorskie" jest regulacją skomplikowaną, dlatego to Sądy decydują w sprawach o naruszenie praw autorskich, szkoła przekazuje sprawę odpowiednim organom.

Pkt 9

Zagrożenia bezpieczeństwa technicznego sieci, komputerów i zasobów.

Kategoria technicznych zagrożeń bezpieczeństwa cyfrowego obejmuje obecnie szerokie spectrum problemów: (1) ataki przez wirusy, robaki i trojany, (2) ataki na zasoby sieciowe (hakerstwo, spyware, crimeware, eksploit, ataki słownikowe i back door, skanowanie portów, phishing, pharming, sniffing, spoofing, ataki Denial of service (DoS,DDoS rootkit) i ataki socjotechniczne. Na styku z zagadnieniami technicznymi lokalizują się zagrożenia wynikające z nieprawidłowych i szkodliwych zachowań użytkowników np. używanie łatwych do odgadnięcia haseł, pozostawianie komputerów włączonych bez opieki, czy brak zabezpieczeń na wypadek braku energii elektrycznej.

W przypadku gdy:

- Nastąpi w szkole zgłoszenie wystąpienia incydentów zagrożenia bezpieczeństwa cyfrowego, pracownik szkoły zobowiązany jest do zgłoszenia go osobie odpowiedzialnej za infrastrukturę cyfrową szkoły oraz dyrekcji szkoły.
- Dyrektor szkoły zleca osobie odpowiedzialnej za infrastrukturę cyfrową szkoły, w możliwie szybkim czasie zebranie i zabezpieczenie dowodów w formie elektronicznej (zrzuty z ekranu, itp. j.w)

Działania szkoły:

- Jeśli sprawcami incydentu są uczniowie szkoły, dyrektor placówki o zaistniałej sytuacji powiadamia ich rodziców,
- Dyrektor wobec w/w uczniów wyciąga odpowiednie konsekwencje wychowawcze.
- Jeżeli skutki ataku mają dotkliwy charakter, doprowadziły do zniszczenia mienia lub utraty istotnych danych (np. gromadzonych w e-dzienniku szkoły), dyrektor szkoły zgłasza przypadek na Policję.
- O zaistniałym incydencie dyrektor powiadamia społeczność szkolną (uczniów, nauczycieli, rodziców) i przedstawia podjęte działania – zarówno te związane z przywróceniem bezpiecznej sieci komputerowej, jak i działań wychowawczyczo – edukacyjnych.

Współpraca ze służbami, Policją i placówkami specjalistycznymi.

- W przypadku wystąpienia strat materialnych oraz utraty danych (szczególnie danych wrażliwych) należy zgłosić incydent na Policji.
- W przypadkach zaawansowanych awarii (np. wywołanych przez np. trojany) lub strat (np. utrata danych z e-dziennika) szkoła może skorzystać z zewnętrznego wsparcia eksperckiego – z kontaktu z serwisem twórcy oprogramowania lub zamówieniem usługi w wyspecjalizowanej firmie.

LM