OPRACOWANIE
Zespół ds. Bezpieczeństwa Cyfrowego w szkole
(Bożena Pawlik, Urszula Wajda, Barbara Szkurłat, Dominika Baumgart-Klisz, Anna Noga)

PROCEDURY REAGOWANIA
W PRZYPADKU WYSTĄPIENIA
ZAGROŻEŃ BEZPIECZEŃSTWA CYFROWEGO
W SZKOLE PODSTAWOWEJ NR 1 W BIELSKU-BIAŁEJ

SPIS TREŚCI

1. CEL PROCEDUR

Bezpieczeństwo w środowisku cyfrowym to zarówno zapewnienie bezpiecznej aktywności uczniów w środowisku cyfrowym, jak i przeciwdziałanie zagrożeniom związanym z bezpieczeństwem sieci, serwerów oraz danych przetwarzanych na urządzeniach.

Celem procedur jest wprowadzenie działań profilaktycznych i stworzenie zasad postępowania na wypadek pojawienia się w szkole cyberzagrożeń.

2. RODZAJE CYBERZAGROŻEŃ

1. **Kontakty z nieodpowiednimi treściami:**
- cyberpornografia;
- cyberprostytucja (w tym także sexting prowadzący do osiągania korzyści materialnych);
- treści propagujące niezdrowy tryb życia.
2. **Niebezpieczne działania:** cyberprzemoc, sexting, samobójstwa z inspiracji i pod wpły-wem sieci (w tym samobójstwa transmitowane na żywo w internecie, samobójstwa pod wpływem upokorzenia czy gnębienia doznanego w sieci, instruktaże dla samobójców, a także internetowe pakty samobójcze).
3. **Niebezpieczne kontakty:**
- uwodzenie dzieci online (*child grooming*);
- cyberpedofilia.
4. **Naruszanie prywatności** (*cyberstalking*).
5. **Zagrożenia o charakterze seksualnym** (sexting, cyberseks).
6. **Zespół uzależnienia od internetu** (*internet addiction disorder* – IAD), w tym od informacji, pozostawania online (*fear of missing out* FOMO) oraz od relacji społecznych budowanych i podtrzymywanych w sieci.
7. **Cyberprzestępczość i nieuczciwość w sieci:**
- zagrożenia związane z bezpieczeństwem danych przechowywanych w internecie;
- fałszywe lajki i pliki cookies zawierające szkodliwe oprogramowanie;
- fałszywe witryny i wyłudzenia danych;
- ataki hakerskie na serwisy społecznościowe;
- *tabnabbing* (fałszywe witryny internetowe, podszywające się pod inne serwisy);
- *clickjacking* (maskowanie odnośnika w celu skłonienia użytkownika do kliknięcia w link podsunięty przez przestępcę);
- zagrożenia dla systemów mobilnych[1].

[1] *Klasyfikacja za: Bębas S., (2018), Zagrożenia dla dzieci i młodzieży w świecie wirtualnym, [w:] Ratajek W. (red.), Edukacja i człowiek w czasach nowych technologii. Szanse, nadzieje i zagrożenia, Wrocław: Wydawnictwo Humanistyczne Via Ferrata, s. 36–44.*

3. OBLIGATORYJNE DZIAŁANIA INTERWENCYJNE PODCZAS WYSTĄPIENIA ZAGROŻENIA BEZPIECZEŃSTWA CYFROWEGO

Działania interwencyjne są następstwem wystąpienia zagrożenia. Dzielą się na 3 grupy:

1. **Działania wobec aktu/zdarzenia** – opis przypadku, ustalenie okoliczności zdarzenia, zabezpieczenie dowodów oraz monitoring sytuacji szkolnej;
2. **Działania wobec uczestników zdarzenia** (ofiara – sprawca – świadek, rodzice/ opiekunowie prawni);
3. **Działania wobec instytucji/organizacji/służb pomocowych i współpracujących** – policji, wymiaru sprawiedliwości, służb społecznych.

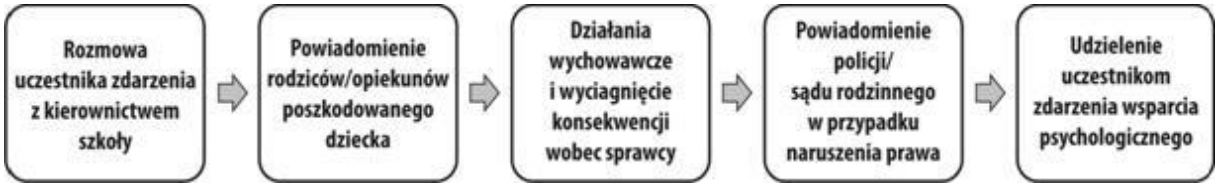
W każdej procedurze związanej z wystąpieniem danego typu zagrożenia cyberbezpieczeństwa w szkole muszą zostać uwzględnione działania, podjęte przez dyrekcję, nauczycieli, pedagogów szkolnych.

Szczegółowy opis znajduje się w publikacji: ***Standard bezpieczeństwa online placówek oświatowych***:
https://akademia.nask.pl/publikacje/ost_Standard_bezpieczenstwa_online_placowek_oswiatowych.pdf

Działania wobec zdarzenia polegają przede wszystkim na zachowaniu (nieusuwaniu) dokumentacji cyfrowej: wiadomości sms, e-maili, nagrań, komentarzy, plików, filmów wideo. O ile to możliwe, należy także zarchiwizować treść rozmów w komunikatorach oraz linki (konkretne adresy URL), a także dane o potencjalnym sprawcy. Każde zdarzenie wymaga udokumentowania w stosownym protokole.

Działania na rzecz uczestników zdarzenia oznaczają te aktywności, które podejmowane są **wobec ofiar** (osób poszkodowanych), **sprawców** i **świadków** zdarzenia.

Rys 1. Standard procedury reakcji na zagrożenie bezpieczeństwa cyfrowego



Źródło:
Wrońska A., Polak Z., (2018), Standard bezpieczeństwa online placówek oświatowych, Warszawa: NASK, s. 27.

Działania wobec instytucji / organizacji / służb pomocowych i współpracujących.
Współpraca z zewnętrznymi instytucjami jest niezbędna w przypadku naruszenia przepisów prawa przez uczniów lub osoby spoza szkoły. Szkoła współpracuje z:

- policją i sądami rodzinnymi,
- służbami społecznymi i placówkami specjalistycznymi,
- dostawcami usług internetowych oraz operatorami telekomunikacyjnymi.

Sprawców wszystkich rodzajów zagrożeń bezpieczeństwa cyfrowego w szkole należy objąć działaniami:

- komunikat o braku akceptacji dla działań jakich dokonał, poznać możliwe skutki i konsekwencje postępowania (np. wynikające ze statutu),
- wezwanie do zaprzestania podobnych działań w przyszłości oraz usunięcia ich skutków,
- objęcie pomocą psychologiczno-pedagogiczną, by podobne zdarzenia nie miały miejsca w przyszłości, gdy sprawców jest więcej, należy z każdym rozmawiać osobno,
- decyzję o karze dla podejmuje rada pedagogiczna, a informację przekazuje dyrektor.

Celem sankcji jest: zatrzymanie działań sprawcy i zapewnienie poczucia bezpieczeństwa ofierze oraz zmiana postawy sprawcy oraz pokazanie społeczności szkolnej, że działania sprawcy nie będą tolerowane i że szkoła skutecznie zareagować w tego rodzaju sytuacjach.

Podejmując decyzję o zastosowaniu sankcji, należy wziąć pod uwagę:

a) **rozmiar i rangę szkody** np. w przypadku cyberprzemocy materiał został upubliczniony w sposób pozwalający na dotarcie do niego wielu osobom (określa 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, czy wie, że wyrządził komuś krzywdę i jak wiele wysiłku włożył w ukrycie swojej tożsamości itp.;
d) **motywacje sprawcy** – należy sprawdzić, czy działanie sprawcy nie jest działaniem odwetowym w odpowiedzi na uprzednie doświadczenia sprawcy.

Rodzice/opiekunowie prawni muszą zostać powiadomieni o zdarzeniu, zapoznani z materiałami i decyzją co do dalszego postępowania ze sprawcą (oraz sankcjach). Powinni zostać też poinformowani, że rodzice ofiary mają prawo zgłosić sprawę policji.
Jeśli sprawcą czynu jest osoba spoza szkoły, należy zapewnić bezpieczeństwo ofierze i poinformować ją i jej rodziców o przysługujących jej prawach.

4. ZABEZPIECZENIE DOWODÓW CYBERPRZEMOCY

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. Takie 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.
3. Jak możesz zarejestrować dowody cyberprzemocy?
a) telefon komórkowy (nie kasuj wiadomości, zapisuj wszystkie wiadomości, zarówno tekstowe, jak i nagrane na pocztę głosową w pamięci telefonu).
b) komunikatory (jeśli to możliwe zapisz lub skopiuj rozmowę, wklej do edytora tekstu, zapisz i wydrukuj).
c) strony serwisów społecznościowych, www (zachowaj kopię materiału – „zrzut ekranu", klawiszami Alt+ Print Screen, „Wklej" do edytora tekstu, zapisz lub wydrukuj)
d) czat (zachowaj kopię materiału – zrób „zrzut ekranu", „wklej" do edytora tekstu, zapisz.
e) e-mail (wydrukuj wiadomość, prześlij ją do nauczyciela lub pedagoga, który zajmuje się ustaleniem okoliczności zajścia (zachowanie całości wiadomości, a nie tylko samego tekstu jest bardziej pomocne, bo zawiera informacje o jej pochodzeniu).
4. Identyfikacja sprawcy
a) Gdy ustalenie sprawcy nie jest możliwe, należy się skontaktować 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.
b) W przypadku gdy zostało złamane prawo, a tożsamości sprawcy nie udało się ustalić, należy bezwzględnie skontaktować się z policją.

Źródło: https://edukacja.fdds.pl/pluginfile.php/85881/course/section/904/szkolne-standardy-bezpieczenstwa-online-FDDS-12042017_broszura.pdf>

5. DOSTĘP DO TREŚCI SZKODLIWYCH, NIEPOŻĄDANYCH, NIELEGALNYCH – PROCEDURA REAGOWANIA /INFOGRAFIKA/

Podstawy prawne uruchomienia procedury

Kodeks karny, art. 200 § 1–5 kk, art. 200a kk, art. 200b kk, art. 202 § 1-4b, art. 256 kk, art. 257. Statut szkoły, Regulamin Wewnętrzny Szkoły

Rodzaj zagrożenia objętego procedurą

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)

Telefony/kontakty alarmowe krajowe

Zgłaszanie nielegalnych treści: www.dyzurnet.pl, numer alarmowy 112 , policja 997

SPOSÓB POSTĘPOWANIA W PRZYPADKU WYSTĄPIENIA ZAGROŻENIA

1. **Opis okoliczności, analiza, zabezpieczenie dowodów**
   Reakcja szkoły w przypadku pozyskania wiedzy o wystąpieniu zagrożenia, zależy, czy:
   (1) treści można bezpośrednio powiązać z uczniami danej szkoły,
   (2) treści nielegalne lub szkodliwe nie mają związku z uczniami danej szkoły, lecz wymagają kontaktu szkoły z odpowiednimi służbami.
   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 pomagać przedstawiciel szkoły).
   W (1) przypadku rozwiązanie leży po stronie szkoły,
   W (2) przypadku należy rozważyć zgłoszenie incydentu na Policję oraz zgłosić go do serwisu Dyżurnet (dyzurnet.pl).
2. **Identyfikacja sprawcy(-ów)**
   W identyfikacji sprawców kluczowe znaczenie odgrywają zgromadzone dowody.
3. **Działania wobec sprawców zdarzenia ze szkoły**
   W przypadku udostępniania 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.
4. **Działania wobec sprawców zdarzenia z poza szkoły**
   W przypadku upowszechniania przez sprawców treści nielegalnych (np. pornografii dziecięcej) należy złożyć zawiadomienie o zdarzeniu na Policję.
5. **Działania wobec ofiar zdarzenia**
   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. W jej trakcie należy ustalić okoliczności uzyskania przez ofiarę dostępu do ww. treści. 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 z wszystkimi uczestnikami zdarzenia oraz udzielającymi wsparcia.

6. **Działania wobec świadków**
   Gdy informacja na temat zdarzenia dotrze do środowiska rówieśniczego ofiary – w klasie, czy szkole, wskazane jest podjęcie działań edukacyjnych i wychowawczych.
7. **Współpraca z Policją i sądem rodzinnym**
   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
8. **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 dziecka.

6. NARUSZENIA PRYWATNOŚCI DOTYCZĄCE NIEODPOWIEDNIEGO LUB NIEZGODNEGO Z PRAWEM WYKORZYSTANIA DANYCH OSOBOWYCH LUB WIZERUNKU DZIECKA I PRACOWNIKA SZKOŁY – PROCEDURA REAGOWANIA /INFOGRAFIKA/

Podstawy prawne uruchomienia procedury
Kodeks Karny (art. 190a par. 2) , RODO

Rodzaj zagrożenia objętego procedurą

To nieodpowiednie lub niezgodne z prawem wykorzystanie danych osobowych lub wizerunku dziecka i pracownika szkoły. Podszywanie się pod inną osobę, wykorzystywanie jej wizerunku lub danych osobowych w celu wyrządzenia jej szkody osobistej lub majątkowej jest w świetle prawa przestępstwem. Najczęstsze formy wyłudzenia lub kradzieży danych to przejęcie profilu na portalu społecznościowym w celu dyskredytacji lub naruszenia dobrego wizerunku ofiary (np. publikacja zdjęć intymnych bądź montowanych), szantażu (w celu uzyskania korzyści finansowych w zamian za niepublikowanie zdjęć bądź treści naruszających dobry wizerunek ofiary), dokonania zakupów i innych transakcji finansowych.

SPOSÓB POSTĘPOWANIA W PRZYPADKU WYSTĄPIENIA ZAGROŻENIA

1. **Przyjęcie zgłoszenia i ustalenie okoliczności zdarzenia**
   Gdy sprawcą jest uczeń - kolega ofiary ze szkoły czy klasy, uczniowie lub rodzice winni skontaktować się z dyrektorem szkoły, wychowawcą. W przypadku, gdy do naruszenia prywatności poprzez kradzież, wyłudzenie danych osobowych wykorzystanie wizerunku dziecka dochodzi ze strony dorosłych osób trzecich, rodzice winni skontaktować się bezpośrednio z Policją.
2. **Opis okoliczności, analiza, zabezpieczenie dowodów**
   W pierwszej kolejności należy zabezpieczyć dowody nieodpowiedniego lub niezgodnego z prawem działania - w formie elektronicznej (e-mail, zrzut ekranu, konwersacja w komunikatorze lub sms). Równolegle należy dokonać zmian tych danych identyfikujących. Jeśli wykradzione dane zostały wykorzystane w celu naruszenia dobrego wizerunku ofiary, bądź w innych celach niezgodnych z prawem należy 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).

3. **Identyfikacja sprawcy(-ów)**
   W przypadku, gdy dowody jasno wskazują na konkretnego sprawcę oraz na spełnianie przesłanki, iż sprawca zmierzał do wyrządzenia ofierze szkody majątkowej lub osobistej należy je zabezpieczyć i przekazać Policji. W przypadku, gdy trudno to ustalić, identyfikacji dokonać winna Policja. W przypadku znanego sprawcy, który jednak nie działał z powyższych pobudek, szkoła powinna dążyć do rozwiązania problemu w ramach działań wychowawczo – edukacyjnych uzgodnionych rodzicami.
4. **Aktywności wobec sprawców zdarzenia ze szkoły/ spoza szkoły**
   Gdy sprawcą incydentu jest uczeń szkoły, należy wobec niego – w porozumieniu z rodzicami – podjąć działania wychowawcze, zmierzające do uświadomienia nieodpowiedniego i nielegalnego charakteru czynów, jakich dokonał. Jednym z elementów takich działań powinno być zadośćuczynienie osobie poszkodowanej (działania niezależnie od powiadomie-nia policji/ sądu rodzinnego). Dyrekcja szkoły podejmuje decyzję 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. Dobrym rozwiązaniem jest uzyskanie interpretacji prawnej radcy prawnego.
5. **Aktywności wobec ofiar zdarzenia**
   Ofiary 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
6. **Działania wobec świadków**
   Gdy kradzież tożsamości bądź naruszenie dobrego imienia ofiary jest znane szerszemu gronu uczniów szkoły, należy podjąć wobec nich działania wychowawcze, zwracające uwagę na negatywną ocenę narażania na uszczerbek wizerunku koleżanki/kolegi – oraz odpowiedzialność prawną.
7. **Współpraca z Policją i sądami rodzinnymi**
   Gdy naruszenie prywatności, czy wyłudzenie lub kradzież tożsamości skutkują wyrządzeniem ofierze szkody majątkowej lub osobistej, rodzice dzieci winni o nim powiadomić Policję.
8. **Współpraca z dostawcami Internetu i operatorami telekomunikacyjnymi**
   W przypadku konieczności podejmowania dalszych działań pomocowych wobec ofiary, można skierować ucznia, za zgodą i we współpracy z rodzicami, do placówki specjalistycznej, np. terapeutycznej.

7. ZAGROŻENIA DLA ZDROWIA DZIECI W ZWIĄZKU Z NADMIERNYM KORZYSTANIEM Z INTERNETU - PROCEDURA REAGOWANIA /INFOGRAFIKA/

Podstawy prawne
Ustawa z dnia 14 grudnia 2016 r. Prawo oświatowe (Dz.U. 2020, poz.910, z późn. zm.)
Rodzaj zagrożenia objętego procedurą:
Infoholizm (siecioholizm) – nadmierne, obejmujące niekiedy niemal całą dobę, korzystanie z zasobów Internetu i gier komputerowych (najczęściej sieciowych) oraz portali społecznościowych przez dzieci. 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.

SPOSÓB POSTĘPOWANIA W PRZYPADKU WYSTĄPIENIA ZAGROŻENIA

1. **Przyjęcie zgłoszenia i ustalenie okoliczności zdarzenia**
   W przypadku nadmiernego korzystania z komputera lub podejrzenia infoholizmu, konieczne jest podejmowanie działań pomocowych - głównie skierowanie ucznia, za zgodą i we współpracy z rodzicami/opiekunami prawnymi, do placówki specjalistycznej, np. terapeutycznej. Kluczowe są tutaj pozostałe objawy wskazane wyżej, zaobserwowane przez nauczycieli, rodziców lub zgłoszone przez rówieśników.
2. **Opis okoliczności, analiza, zabezpieczenie dowodów**
   Reakcja szkoły powinna polegać w pierwszej kolejności na ustaleniu we współpracy z rodzicami skutków zdrowotnych i psychicznych, jakie nadmierne korzystanie z zasobów Internetu wywołało u dziecka (np. gorsze wyniki w nauce, niedosypianie, niedojadanie, rezygnacja z dawnych zainteresowań, załamanie się relacji z rodziną czy rówieśnikami).
   Celem tych ustaleń jest wybór odpowiedniej ścieżki rozwiązywania problemu:
   z udziałem specjalistów (lekarzy, terapeutów) lub bez – wyłącznie w szkole.
3. **Działania wobec ofiar zdarzenia**
   Osoba, której problem dotyczy, powinna zostać otoczona zindywidualizowaną opieką pedagoga szkolnego.
   Pierwszy krok to zebranie wywiadu od ucznia i jego rodziców w celu określenia sytuacji i wstępnego ustalenia poziomu zagrożenia.
   Następnie, w zależności od stwierdzonego zagrożenia, proponuje się konsultacje ze specjalistą, który pozwoli zdiagnozować poziom zagrożenia, określić przyczyny popadnięcia ucznia w nałóg (np. takie jak trudna sytuacja domowa, brak sukcesów edukacyjnych w szkole, izolacja w środowisku rówieśniczym) i ukazać specyfikę przypadku. Każde dziecko, u którego podejrzewa się nałóg korzystania z Internetu, powinno zostać profesjonalnie zdiagnozowane za zgodą rodziców/opiekunów prawnych przez psychologa zatrudnionego np. w poradni psychologiczno-pedagogicznej. Dziecku w trakcie wsparcia należy zapewnić komfort psychiczny - o jego sytuacji i specyfice uwarunkowań osobistych powinni zostać powiadomieni uczący je nauczyciele.
   Z rodzicami/opiekunami prawnymi dziecka należy omówić wspólne rozwiązania trudnej sytuacji. Tylko synergiczne współdziałanie rodziców i szkoły może zagwarantować powodzenie podejmowanych działań wspierających dziecko.
4. **Działania wobec świadków zdarzenia**
   Jeśli świadkami problemu są rówieśnicy dziecka, należy im w rozmowie zwrócić uwagę na negatywne aspekty nadmiernego korzystania z zasobów Internetu oraz zaapelować o wsparcie dziecka dotkniętego problemem.

5. **Współpraca ze służbami i placówkami specjalistycznymi**
   W przypadku podejrzenia uzależnienia od internetu, dziecko powinno zostać skierowane we współpracy z rodzicami/opiekunami prawnymi, do placówki specjalistycznej oferującej program terapeutyczny w celu diagnozy oraz ewentualnej terapii.

8. DEZINFORMACJA, BEZKRYTYCZNA WIARA W TREŚCI ZAMIESZCZONE W INTERNECIE, NIEUMIEJĘTNOŚĆ ODRÓŻNIENIA TREŚCI PRAWDZIWYCH OD NIEPRAWDZIWYCH, W TYM SZKODLIWOŚĆ REKLAM – PROCEDURY REAGOWANIA

/INFOGRAFIKA/

Podstawy prawne uruchomienia procedury
Ustawa z 14 grudnia 2016 r. Prawo oświatowe (Dz. U. 2020, poz. 910, z późn. zm.).
Rodzaj zagrożenia objętego procedurą (opis)
Brak umiejętności odróżniania informacji prawdziwych od nieprawdziwych publikowanych w internecie, bezkrytyczne uznawanie za prawdę tez publikowanych na forach internetowych, kierowanie się informacjami zawartymi w reklamach. 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 (korzystanie z upraszczających i zawężających wiedzę nieprofesjonalnych opracowań), a także do utrwalania się u ucznia ambiwalentnych postaw moralnych.

SPOSÓB POSTĘPOWANIA W PRZYPADKU WYSTĄPIENIA ZAGROŻENIA

1. **Przyjęcie zgłoszenia i ustalenie okoliczności zdarzenia**
   Identyfikowanie przez nauczycieli i wychowawców uczniów nieumiejących odróżniać prawdy od fałszu informacji publikowanych w Internecie (np. niepożądana postawa ujawnia się podczas przygotowania prac domowych).
   Procedury interwencyjne mają uzasadnienie w przypadku uczniów podejmujących zachowania ryzykowne (np. samookaleczających się lub stosujących ryzykowne diety).
2. **Opis okoliczności, analiza, zabezpieczenie dowodów**
   Nauczyciel po zauważeniu, analizuje i komentuje posługiwanie się nieprawdziwymi informacjami zaczerpniętymi z internetu w procesie dydaktycznym (podczas lekcji lub w zadaniach domowych).
3. **Działania wobec sprawców zdarzenia ze szkoły/spoza szkoły**
   Wystarczającą reakcją jest opublikowanie sprostowania nieprawdziwych informacji i – w miarę możliwości – rozpowszechnienie go w internecie, na portalach o zbliżonej tematyce.
4. **Działania wobec ofiar zdarzenia i świadków**
   Szkoła prowadzi działania profilaktyczne – edukację medialną (informacyjną), np. w trakcie zajęć nieinformatycznych (np. historii, języka polskiego) przez wszystkie lata nauki w szkole lub podczas lekcji ukierunkowanych na zdobywanie przez dzieci i młodzież kompetencji cyfrowych. Działania mające na celu zapobieganie angażowaniu się w zachowania autodestrukcyjne realizowane są w ramach programu profilaktycznego szkoły.

9. CYBERPRZEMOC – PROCEDURA REAGOWANIA /INFOGRAFIKA/

Podstawy prawne

Kodeks Karny, najczęściej: art. 190 kk2 – groźba karalna, art. 190a kk – uporczywe nękanie (stalking), podszywanie się, art. 191 kk – zmuszenie do określonego działania, art. 191a kk – naruszenie intymności seksualnej, utrwalenie wizerunku nagiej osoby bez jej zgody, art. 212 kk – zniesławienie, art. 216 kk – zniewaga, art. 267 kk – bezprawne uzyskanie informacji, art. 268 kk – utrudnianie zapoznania się z informacją, art. 268a kk – niszczenie danych informatycznych, art. 269 kk – uszkodzenie danych informatycznych, art. 269a kk – zakłócanie systemu komputerowego, art. 287 kk – oszustwo komputerowe, art. 107 kw3 – dokuczenia lub złośliwe wprowadzanie w błąd

Statut Szkoły, Regulamin Wewnętrzny Szkoły

Rodzaj zagrożenia objętego procedurą

Cyberprzemoc – przemoc z użyciem nowych technologii (mediów elektronicznych) w internecie. Może przybierać formy: wyzywanie, straszenie, prześladowanie, oczernianie lub poniżanie, przerabianie i publikowanie ośmieszających materiałów, zdjęć, filmów, upublicznianie sekretów ofiar, wulgarne i złośliwe komentowanie wpisów i zdjęć, podszywanie się pod inną osobę za pomocą przechwyconego profilu lub poczty, celowe ignorowanie aktywności ofiary w sieci.

Cyberprzemoc charakteryzuje się ciągłością trwania (zwykle nie kończy się na jednorazowym zdarzeniu) oraz szybkością rozpowszechniania się informacji/materiałów skierowanych przeciwko jej ofierze, a także ich dostępnością.

Do cyberprzemocy wykorzystywane są głównie: poczta elektroniczna, czaty, komunikatory, strony internetowe, blogi, media społecznościowe, grupy dyskusyjne, SMS i MMS.

Telefony alarmowe krajowe i lokalne

- telefon rzecznika praw dziecka: 800 12 12 12
- telefon zaufania dla dzieci i młodzieży: 116 111, https://11611.pl/
- telefon dla rodziców i nauczycieli w sprawie bezpieczeństwa dzieci: 800 100 100 https://800100100.pl/

Zgłaszanie nielegalnych treści: dyzurnet.pl dyzurnet@dyzurnet.pl

SPOSÓB POSTĘPOWANIA W PRZYPADKU WYSTĄPIENIA ZAGROŻENIA

1. **Przyjęcie zgłoszenia i ustalenie okoliczności zdarzenia**:
   Akt 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 sprawy. W trakcie ustalania okoliczności trzeba określić charakter zdarzenia (rozmiar i rangę szkody, jednorazowość/ powtarzalność). Realizując procedurę, należy unikać działań, które mogłyby wtórnie stygmatyzować ofiarę lub sprawcę. Trzeba dokonać oceny, czy zdarzenie wyczerpuje znamiona cyberprzemocy, czy jest np. niezbyt udanym żartem (wtedy podjąć działania profilaktyczne, mające na celu niedopuszczenie do eskalacji tego typu zachowań).
2. **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, itd.). W trakcie zbierania materiałów trzeba zadbać o bezpieczeństwo osób zaangażowanych w problem.
3. **Identyfikacja sprawcy (-ów)**
   Na podstawie zebranych materiałów w wyniku rozmów z osobą zgłaszającą i z ofiarą oraz analizy tych materiałów. Jeśli ustalenie sprawcy wydaje się niemożliwe, rada pedagogiczna

decyduje, czy jest konieczne skontaktowanie się z policją. Bezwzględnie należy zgłosić rozpowszechnianie nagich zdjęć osób poniżej 18. r. ż. (art. 202 § 3 kk).

4. **Działania wobec sprawców zdarzenia ze szkoły/ spoza szkoły**

   Gdy sprawca cyberprzemocy jest znany i jest uczniem szkoły, pedagog szkolny przeprowadza z nim rozmowę o jego zachowaniu. Rozmowa ma służyć ustaleniu okoliczności zdarzenia, jego wspólnej analizie (w tym przyjrzeniu się przyczynom) oraz próbie rozwiązania sytuacji konfliktowej (w tym sposobów zadośćuczynienia ofiarom).

   W sytuacji, gdy sprawca jest nieznany, podstawowe działanie polega na przerwaniu aktu cyberprzemocy (zawiadomieniu administratora serwisu w celu usunięcia materiału po wcześniejszym zabezpieczeniu dowodów), zapewnieniu pomocy psychologiczno-pedagogicznej poszkodowanemu oraz wsparciu rodziców poszkodowanego ucznia w ewentualnym zgłoszeniu sprawy policji.

5. **Działania wobec ofiar zdarzenia**

   W pierwszej kolejności należy udzielić wsparcia ofierze, aby czuła się bezpieczna i otoczona opieką dorosłych i szkoły, która podejmuje kroki w celu rozwiązania problemu.

   Podczas rozmowy z uczniem – ofiarą cyberprzemocy:

   a) Należy zapewnić go, że nie jest winny zaistniałej sytuacji oraz że nikt nie ma prawa tak zachowywać się wobec niego, a także podkreślić, że dobrze zrobił, ujawniając sytuację.
   b) 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 uruchomione odpowiednie procedury interwencyjne.
   c) Należy poinformować ucznia o krokach, jakie może podjąć szkoła i sposobach, w jaki może zapewnić mu bezpieczeństwo.
   d) Należy pomóc ofierze (rodzicom/opiekunom prawnym) w zabezpieczeniu dowodów, omówić strategię postępowania wobec sprawcy, zadbać o podstawowe zasady bezpieczeństwa online.
   e) W trakcie rozmowy z dzieckiem i/lub jego rodzicami/opiekunami, jeśli jest to wskazane, można zaproponować pomoc specjalisty oraz przekazać informację o możliwości zgłoszenia sprawy policji.

   W działania wobec ofiary należy także włączyć rodziców/opiekunów ofiary – trzeba na bieżąco ich informować o sytuacji. 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. Pomoc ofierze nie może kończyć się w momencie zamknięcia procedury.

6. **Działania wobec świadków zdarzenia**

   Należy zadbać o bezpieczeństwo świadków zdarzenia, zwłaszcza jeśli byli oni osobami ujawniającymi cyberprzemoc. W trakcie rozmowy ze świadkami należy okazać zrozumienie i empatię wobec ich uczuć – obawy przed posądzeniem o donosicielstwo, strachu przed staniem się kolejną ofiarą sprawcy itp.

7. **Współpraca z Policją i Sądem**

   Samo wystąpienie zjawiska cyberprzemocy nie jest jednoznaczne z koniecznością zaangażowania Policji i Sądu Rodzinnego. Szkoła powiadamia odpowiednie służby (np. sąd rodzinny), gdy wykorzysta wszystkie dostępne jej środki wychowawcze (rozmowa z rodzicami, konsekwencje wobec sprawcy wynikające ze statutu i/lub regulaminu) i interwencje pedagogiczne, a ich zastosowanie nie zmieni 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). Zgłoszenia dokonuje dyrektor szkoły.

8. **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 (t.j. Dz.U.2020, poz. 344).

10. SEKSTING, PROWOKACYJNE ZACHOWANIA I AKTYWNOŚĆ SEKSUALNA JAKO ŹRÓDŁO DOCHODU OSÓB NIELETNICH - PROCEDURA REAGOWANIA /INFOGRAFIKA/

Podstawy prawne uruchomienia procedury
Kodeks karny – art. 191a, art. 202 § 1–4c.
Rodzaj zagrożenia objętego procedurą
Seksting to przesyłanie drogą elektroniczną w formie wiadomości MMS lub publikowanie np. w portalach (społecznościowych) prywatnych treści, głównie zdjęć, o kontekście seksualnym, erotycznym i intymnym.

SPOSÓB POSTĘPOWANIA W PRZYPADKU WYSTĄPIENIA ZAGROŻENIA

1. **Przyjęcie zgłoszenia i ustalenie okoliczności zdarzenia**
   Zgłoszenie sekstingu dokonują rodzice lub opiekunowie prawni dziecka – ofiary, sama ofiary, jej znajomi, nauczyciele lub inni pracownicy szkoły. Delikatny charakter sprawy, a także odpowiedzialność karna sprawcy, wymagają zachowania daleko posuniętej dyskrecji i profesjonalnej reakcji.
2. **Opis okoliczności, analiza, zabezpieczenie dowodów**
   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.
3. **Identyfikacja sprawcy (-ów)**
   Identyfikacja sprawcy będzie możliwa przede wszystkim dzięki zabezpieczeniu dowodów - przesyłanych zdjęć, czy zrzutów ekranów portali, w których opublikowano zdjęcie (-a). Seksting jest karalny, dlatego trzeba dbać o skrupulatność i wiarygodność dokumentacji oraz przestrzegać zasad dyskrecji, szczególnie w środowisku rówieśniczym ofiary.
4. **Działania wobec sprawców zdarzenia ze szkoły/spoza szkoły**
   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. Konieczne są także rozmowy ze sprawcami w obecności ich rodziców zaproszonych do szkoły.
   Rodzaj 1. Dalsze działania poza zapewnieniem wsparcia i opieki 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.

Rodzaj 2. Niektóre z tego typu materiałów mogą zostać uznane za pornograficzne, w takim wypadku dyrektor ma obowiązek zgłoszenia incydentu na Policję. Rozpowszechnianie materiałów pornograficznych z udziałem nieletnich jest przestępstwem ściganym z urzędu (par. 2020 Kodeksu Karnego), dlatego też dyrektor placówki zgłasza incydent na Policję i/lub do sądu rodzinnego. Wszelkie działania wobec sprawców incydentu powinny być podejmowane w porozumieniu z ich rodzicami lub opiekunami prawnymi**.**

Rodzaj 3. Niektóre z tego typu materiałów mogą zostać uznane za pornograficzne – konieczne zgłoszenie takiego przypadku na Policję. W sytuacji zaistnienia znamion cyberprzemocy, należy dodatkowo zastosować procedurę: Cyberprzemoc. Decyzję o ewentualnym poinformowaniu opiekunów podejmuje pedagog biorąc pod uwagę dobro małoletnich, w zależności od charakteru sytuacji.

5. **Działania wobec ofiar zdarzenia**
   Pierwszą reakcją szkoły i rodziców, obok dokumentacji dowodów jest otoczenie wszechstronną, dyskretną opieką pedagogiczną ofiary oraz zaproponowanie odpowiednich działań wychowawczych, w przypadku upublicznienia przypadku sekstingu w środowisku rówieśniczym. Rozmowa na temat identyfikacji potencjalnego sprawcy powinna być realizowana w warunkach komfortu psychicznego dla dziecka – ofiary sekstingu, z szacunkiem dla jego indywidualności i przeżytego stresu.
6. **Działania wobec świadków**
   Jeśli przypadek sekstingu zostanie upowszechniony w środowisku rówieśniczym (np. przesłanie MMS do uczniów tej samej szkoły lub klasy lub publikację w portalu społecznościowym), należy podjąć działania wychowawcze, uświadamiające negatywne aspekty moralne sekstingu oraz narażanie się na dotkliwe kary.
7. **Współpraca z Policją i sądami rodzinnymi**
   W przypadku publikacji lub upowszechniania zdjęć o charakterze pornografii dziecięcej (co jest wykroczeniem ściganym z urzędu) dyrektor szkoły powiadamia o tym zdarzeniu Policję lub sąd rodzinny.
8. **Współpraca ze służbami społecznymi i placówkami specjalistycznymi**
   Kontakt ofiar z placówkami specjalistycznymi może okazać się konieczny w indywidualnych przypadkach. O skierowaniu do nich decyzję powinien podjąć pedagog szkolny wspólnie z rodzicami/opiekunami prawnymi ofiary.

11. BEZPRAWNE UŻYCIE CUDZEGO WIZERUNKU W SIECI – PROCEDURA REAGOWANIA

Podstawy prawne uruchomienia procedury
Kodeks cywilny art.23 i Ustawa z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych, t.j. Dz.U. 2019, poz. 1231; 2020, poz. 288.
Rodzaj zagrożenia objętego procedurą
Bezprawne, tj. bez wymaganej prawem zgody, użycie wizerunku osoby fizycznej w internecie.

SPOSÓB POSTĘPOWANIA W PRZYPADKU WYSTĄPIENIA ZAGROŻENIA

1. **Przyjęcie zgłoszenia i ustalenie okoliczności zdarzenia**
   Wizerunek jest jednym z dóbr osobistych wymienionych w art. 23 *Kodeksu cywilnego* obok zdrowia, wolności, czci, swobody sumienia, nazwiska lub pseudonimu, tajemnicy korespondencji, nietykalności mieszkania, twórczości naukowej, artystycznej, wynalazczej i racjonalizatorskiej.
   Ochronę wizerunku gwarantuje także prawo autorskie. Art. 81 ust. 1 zd. 1 *Ustawy o prawie autorskim i prawach pokrewnych* stanowi, że: *Rozpowszechnianie wizerunku wymaga zezwolenia osoby na nim przedstawionej*.
   Naruszeniem tego prawa: jest bezprawne rozpowszechnianie wizerunku rozumiane jako publiczne udostępnianie, czy też stworzenie możliwości zapoznania się z wizerunkiem np. użytkownikom internetu (zwłaszcza upublicznienia zdjęcia/filmu ukazującego kolegę czy koleżankę w sposób prześmiewczy i poniżający).
   Opublikowanie czyjegoś zdjęcia bez zgody tej osoby może skutkować odpowiedzialnością cywilną i karną osoby, która takiej publikacji się dopuściła. Zgoda na publikowanie wizerunku powinna zostać wyrażona wprost, z pełną świadomością formy, w jakiej zostanie przedstawiony jej wizerunek, miejsca i czasu publikacji tego wizerunku, ewentualnego zestawienia jej wizerunku z innymi wizerunkami czy towarzyszącego publikacji komentarza.
   Osoba, której dobro osobiste zostało zagrożone, może żądać zaprzestania tego działania, o ile jest ono bezprawne i żądać, aby osoba, która dopuściła się naruszenia, dopełniła czynności potrzebnych do usunięcia jego skutków, w szczególności złożyła oświadczenie odpowiedniej treści i w odpowiedniej formie. Ofiara może też żądać zadośćuczynienia pieniężnego lub zapłaty odpowiedniej sumy pieniężnej na wskazany cel społeczny (wg orzeczenia sądu).
2. **Opis okoliczności, analiza, zabezpieczenie dowodów**
   Należy zebrać informacje przede wszystkim o:
   a) osobie dokonującej zgłoszenia, czy jest do tego uprawniona, tj. czy to jej wizerunek lub wizerunek osoby, która jest pod jej władzą rodzicielską, został naruszony bezprawnym działaniem,
   b) okolicznościach zdarzenia,
   c) możliwych dowodach, np. zrzut ekranu dokumentujący bezprawne użycie wizerunku.
3. **Identyfikacja sprawcy (-ów)**
   Dochodzenie naruszeń dóbr osobistych, w tym wizerunku, jest podejmowane z inicjatywy samego uprawnionego przed sądami. Natomiast w przypadku naruszeń stanowiących przestępstwo dodatkowo mogą być zaangażowane organy ścigania.
4. **Działania wobec sprawców zdarzenia ze szkoły/spoza szkoły**
   Decyzja o dalszych krokach prawnych w sprawach o naruszenie dóbr osobistych, w tym wizerunku, należy do osoby, której wizerunek został bezprawnie użyty w internecie.

Szkoła, oprócz realizacji zapisów podstawy programowej związanych z prawem autorskim, realizuje na lekcjach wychowawczych tematykę związaną z bezpiecznym i przemyślanym udostępnianiem wizerunku w internecie, w tym przede wszystkim w mediach społecznościowych, aby zapobiec podobnym zdarzeniom w przyszłości.

5. **Działania wobec ofiar zdarzenia**
   Ofiarę zdarzenia, w szczególności jeśli wizerunek został bezprawnie użyty w sposób prześmiewczy i poniżający, należy objąć opieką pedagoga szkolnego.
6. **Działania wobec świadków**
   W przypadku gdy więcej osób wiedziało o bezprawnym użyciu wizerunku w sposób prześmiewczy lub poniżający, należy przeprowadzić z nimi rozmowy wychowawcze mające na celu uzmysłowienie im problemu i ukształtowanie w nich postawy sprzeciwu wobec podobnych działań.
7. **Współpraca z policją i sądami rodzinnymi**
   Decyzja o dalszych krokach prawnych w sprawach o naruszenie dóbr osobistych, w tym wizerunku, należy do ofiary. Szkoła może zaangażować się w spór, jeśli dotyczy to sytuacji, w której bezprawnego użycia wizerunku dopuścił się uczeń wobec drugiego ucznia, np. w charakterze mediatora pomiędzy stronami w celu uniknięcia procesu sądowego.
8. **Współpraca ze służbami społecznymi i placówkami specjalistycznymi**
   Informacje, szkolenia dla pracowników szkoły oraz pogadanki dla uczniów z zakresu świadomego i zgodnego z prawem użycia wizerunku innej osoby w internecie.

12. NAWIĄZYWANIE NIEBEZPIECZNYCH KONTAKTÓW W INTERNECIE – UWODZENIE, ZAGROŻENIE PEDOFILIĄ - PROCEDURA REAGOWANIA /INFOGRAFIKA/

Podstawy prawne: *Kodeks karny*: art. 200, art. 200a § 1 i 2, art. 286 § 1.
Rodzaj zagrożenia objętego procedurą: 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).
Telefony alarmowe krajowe
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.pl dyzurnet@dyzurnet.pl, 801 615 005

SPOSÓB POSTĘPOWANIA W PRZYPADKU WYSTĄPIENIA ZAGROŻENIA

1. **Przyjęcie zgłoszenia i ustalenie okoliczności zdarzenia**
   Osobami najczęściej zgłaszającymi problem są rodzice/opiekunowie prawni dziecka lub informacja uzyskana jest ze środowiska rówieśników ofiary. 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, a także wyłudzenie pieniędzy czy przedmiotów dużej wartości.
2. **Opis okoliczności, analiza, zabezpieczenie dowodów**
   Należy bezzwłocznie powiadomić Policję o wystąpieniu zdarzenia. Należy zidentyfikować i zabezpieczyć w szkole, w formie elektronicznej dowody działania dorosłego sprawcy

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

3. **Identyfikacja sprawcy(-ów)**
   Ze względu na bezpieczeństwo nie należy podejmować samodzielnych działań w celu dotarcia do sprawcy, lecz udzielać wszelkiego możliwego wsparcia organom ścigania, m.in. zabezpieczyć i przekazać zebrane dowody. Identyfikacja sprawcy wykracza poza kompetencje i możliwości szkoły.
4. **Działania wobec sprawców ze szkoły/ spoza szkoły**
   Nie należy podejmować aktywności zmierzających bezpośrednio do kontaktu ze sprawcą. Zadaniem szkoły jest zebranie dowodów i opieka nad ofiarą i ewentualnymi świadkami.
5. **Działania wobec ofiar zdarzenia**
   W każdym przypadku próby nawiązania niebezpiecznego kontaktu należy przed wszystkim zapewnić ofierze poczucie bezpieczeństwa. O możliwym nawiązaniu takich kontaktów dzieci w Internecie należy powiadomić rodziców. Pierwszą czynnością w ramach reakcji na zagrożenie jest otoczenie ofiary pomocą pedagogiczną we współpracy szkoły z rodzicami/ opiekunami prawnymi. Należy upewnić się, że kontakt ofiary ze sprawcą został przerwany. Wszelkie działania szkoły wobec dziecka winny być uzgadniane z rodzicami/opiekunami prawnymi i inicjowane za ich zgodą.
6. **Działania wobec świadków**
   Jeżeli zgłaszającym zagrożenie był rówieśnik ofiary, należy również objąć go opieką pedagogiczną, pozytywnie wzmacniając jego reakcję na zdarzenie, docenić jego prospołeczną postawę.
7. **Współpraca z Policją i sądami rodzinnymi**
   W przypadkach naruszenia prawa – szczególnie w przypadku uwiedzenia dziecka do lat 15 – obowiązkiem szkoły jest powiadomienie Policji lub sądu rodzinnego.
8. **Współpraca ze służbami społecznymi i placówkami specjalistycznymi**
   W przypadkach uwiedzenia nieletnich przez osoby dorosłe rekomenduje się – w porozumieniu z rodzicami/opiekunami prawnymi – skierowanie ofiary na terapię do placówki specjalistycznej opieki psychologicznej.

13. ŁAMANIE PRAWA AUTORSKIEGO - PROCEDURA REAGOWANIA /INFOGRAFIKA/

Podstawy prawne uruchomienia procedury

Ustawa o prawie autorskim i prawach pokrewnych, Kodeks karny, Kodeks cywilny.

Rodzaj zagrożenia objętego procedurą

Ryzyko poniesienia odpowiedzialności cywilnej lub karnej z tytułu naruszenia prawa autorskiego albo negatywnych skutków pochopnego spełnienia nieuzasadnionych roszczeń (tzw. *copyright trolling*).

SPOSÓB POSTĘPOWANIA W PRZYPADKU WYSTĄPIENIA ZAGROŻENIA

1. **Przyjęcie zgłoszenia i ustalenie okoliczności zdarzenia**
   Nieformalne (ustnie, telefonicznie, pocztą elektroniczną, na forum internetowym, na piśmie w postaci wezwania) lub formalne (w postaci doręczenia odpisu pozwu lub innego pisma urzędowego, np. wezwania z policji lub prokuratury). Przyjęcie zgłoszenia dokonanego w sposób nieformalny powinno zostawić "ślad" w postaci notatki służbowej lub zakomunikowania przełożonemu, w zależności od wagi sprawy.
   Najczęstszym przypadkiem naruszenia praw autorskich, jest użycie materiałów prawnie chronionych na stronach internetowych szkoły, poza zakresem dozwolonego użytku.

W przypadku naruszeń dokonanych przez uczniów, dochodzenie roszczeń przeprowadzą osoby uprawnione. Szkoła skupia się na roli edukacyjno-wychowawczej poprzez realizację podstawy programowej w tym zakresie oraz organizację pogadanek na temat praw autorskich z informacją jakie czyny są dozwolone, a jakie zabronione prawem.

2. **Opis okoliczności, analiza, zabezpieczenie dowodów**
   Należy zebrać informacje przede wszystkim o:
   a) osobie dokonującej zgłoszenia, czy jest do tego uprawniona (czy przysługują jej prawa autorskie do danego utworu, czy posiada ważne pełnomocnictwo itd.);
   b) wykorzystanym utworze (czy jest chroniony przez prawo autorskie, w jakim zakresie został wykorzystany i czy zakres ten mieści się w zakresie posiadanych licencji lub dozwolonego użytku).

   Należy zweryfikować wszystkie informacje podane przez zgłaszającego (np. powoływanie się on na toczące się w sprawie postępowanie karne), podjąć kontakt z odpowiednimi służbami za pośrednictwem adwokata lub radcy prawnego, aby sprawdzić, czy okoliczności w zgłoszeniu są faktyczne i czy przedstawiane dowody nie zostały zmanipulowane.
3. **Identyfikacja sprawcy(-ów)**
   Dochodzenie naruszeń praw autorskich realizowane jest z inicjatywy samego uprawnionego przed sądami, a w przypadku naruszeń stanowiących przestępstwo dodatkowo zaangażowane mogą być policja i prokuratura. Szkoła skupia się na swojej roli wychowawczej i edukacyjnej, przekazując zaangażowanym osobom (lub wszystkim uczniom, nauczycielom i opiekunom) wiedzy na temat przepisów prawa regulujących konkretne kwestie.
4. **Działania wobec sprawców zdarzenia ze szkoły/ spoza szkoły**
   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.
5. **Działania wobec ofiar zdarzenia**
   Jeżeli osobą, której prawa autorskie naruszono, jest uczeń, należy rozważyć możliwość wystąpienia w roli mediatora, aby ułatwić stronom ugodowe lub kompromisowe zakończenie powstałego sporu. Gdy ofiarą jest osoba spoza szkoły, autorytet szkoły może pomóc sprawcy w doprowadzeniu do zaniechania naruszeń i naprawienia ich skutków bez eskalacji sporu.
6. **Działania wobec świadków**
   Stosownie do okoliczności, należy samodzielnie zebrać zeznania lub zadbać, aby zostały one zebrane przez uprawnione organy.
7. **Współpraca z policją i sądami rodzinnymi**
   Dochodzenie roszczeń z tytułu naruszeń zależy od decyzji ofiary, to uprawniony musi zdecydować, czy zawiadamiać policję lub składać powództwo. Szkoła jako mediator, może zaangażować się w ułatwienie zakończenia sporu bez nadmiernej jego eskalacji.
8. **Współpraca ze służbami społecznymi i placówkami specjalistycznym**
   Szkoła może zorganizować szkolenia z zakresu prawa autorskiego, w tym w internecie.
9. **Współpraca z dostawcami internetu i operatorami telekomunikacyjnymi**
   Zależnie od okoliczności może być wskazana asysta sprawcy bądź ofiary podczas kontaktu z tego typu podmiotami, np. w celu zablokowania dostępu do utworu umieszczonego w internecie z naruszeniem prawa. Ponadto, stosownie do przepisów prawa, usługodawcy mogą zostać zobowiązani do przekazania szczegółów dotyczących naruszenia dokonanego z użyciem ich usług (do tego może być potrzebne postanowienie sądowe).

14. PROCEDURY REAGOWANIA W PRZYPADKU WYSTĄPIENIA INCYDENTU ZAGROŻENIA CYBERBEZPIECZEŃSTWA W SZKOLE

/INFOGRAFIKA/

Podstawy prawne uruchomienia procedury

Ustawa z dnia 14 grudnia 2016 r. Prawo oświatowe, Dz.U. 2020, poz. 910, z późn. zm.
Statut szkoły, Regulamin Wewnętrzny Szkoły
Kodeks karny, Rozdział XXXIII *Przestępstwa przeciwko ochronie informacji*: art. 267 § 1–4, art. 268 § 1–3, art. 268a § 1–2, art. 269 § 1–2, art. 269a, art. 269b § 1–2
Kodeks cywilny: art. 415.

Rodzaj zagrożenia objętego procedurą

Zagrożenia bezpieczeństwa technicznego sieci, komputerów i zasobów onlin

Kategoria technicznych zagrożeń bezpieczeństwa cyfrowego obejmuje obecnie szerokie spektrum problemów:

a) ataki przeprowadzane za pomocą szkodliwego oprogramowania,
b) ataki skierowane na zasoby teleinformatyczne szkoły przy wykorzystaniu wielu skomplikowanych technik i narzędzi informatycznych (m.in.: skanowanie sieci w celu wykrycia podatnych na zagrożenia systemów, próby logowania się do serwerów www i poczty e-mail, za pomocą podsłuchanych lub odgadniętych haseł, wykorzystywanie podatności (luk) w oprogramowaniu systemów komputerowych) i socjotechnicznych (*phishing*).

Na styku z zagadnieniami technicznymi lokalizują się zagrożenia wynikające z nieprawidłowych i szkodliwych zachowań użytkowników, np. uleganie atakom socjotechnicznym, używanie w różnych serwisach tych samych, łatwych do odgadnięcia haseł, zaniechanie wykonywania aktualizacji systemu operacyjnego urządzeń, przeglądarek internetowych i innego używanego przez użytkowników oprogramowania.

SPOSÓB POSTĘPOWANIA W PRZYPADKU WYSTĄPIENIA ZAGROŻENIA

1. **Przyjęcie zgłoszenia i ustalenie okoliczności zdarzenia**
   W przypadku wystąpienia incydentów zagrożenia bezpieczeństwa cyfrowego pracownik szkoły zobowiązany jest do zgłoszenia go osobie odpowiedzialnej za infrastrukturę teleinformatyczną szkoły oraz dyrekcji. Kluczowe znaczenie ma zebranie i zabezpieczenie przez specjalistę dowodów w formie elektronicznej.
2. **Opis okoliczności, analiza, zabezpieczenie dowodów**
   Szczegółowy opis procedur reagowania na wystąpienie w szkole różnorodnych zagrożeń bezpieczeństwa cyfrowego zawarty jest w dokumencie **„polityka bezpieczeństwa cyfrowego”** szkoły. W części przypadków szkoła jest w stanie poradzić sobie we własnym zakresie, w niektórych konieczne jest skorzystanie z zewnętrznego wsparcia wyspecjalizowanych firm.
3. **Identyfikacja sprawcy(-ów)**
   Identyfikację sprawców ataku należy pozostawić specjalistom – informatykom. W sytuacji gdy incydent spowodował w szkole straty materialne lub wiązał się z utratą danych, należy powiadomić policję, aby podjęła działania na rzecz zidentyfikowania sprawcy.
4. **Działania wobec sprawców zdarzenia ze szkoły/ spoza szkoły**
   Jeśli sprawcami incydentu są uczniowie danej szkoły, należy wobec nich podjąć działania wychowawcze i o zaistniałej sytuacji powiadomić ich rodziców. Jeżeli skutki ataku mają dotkliwy charakter, doprowadziły do zniszczenia mienia lub utraty istotnych danych (np. w dzienniku elektronicznym szkoły), należy taki przypadek zgłosić policji.

5. **Działania wobec świadków**
   O incydencie należy powiadomić społeczność szkolną (uczniów, nauczycieli, rodziców) i zaprezentować podjęte działania, zarówno przywracające działanie aplikacji i sieci komputerowej w szkole, jak i wychowawczo-edukacyjne wobec dzieci.
6. **Współpraca z policją i sądami rodzinnymi**
   W przypadku wystąpienia strat materialnych oraz utraty danych (szczególnie danych wrażliwych) należy zgłosić incydent policji.
7. **Współpraca ze służbami społecznymi i placówkami specjalistycznymi**
   W przypadku zaawansowanych awarii (np. wywołanych przez „konie trojańskie") lub strat (np. utrata danych z dziennika elektronicznego) konieczne jest skorzystanie z zewnę-trznego wsparcia eksperckiego, kontakt z serwisem twórcy oprogramowania lub zamówienie usługi w wyspecjalizowanej firmie.

15. DZIAŁANIA SZKOŁY NA RZECZ BEZPIECZEŃSTWA CYFROWEGO

Istotą bezpieczeństwa cyfrowego jest bieżąca identyfikacja potencjalnych zagrożeń w środowisku cyfrowym oraz świadome działanie ukierunkowane na zapobieganie ich wystąpieniu oraz minimalizowanie negatywnych ich skutków.

Działania profilaktyczne (prewencyjne) w szkole prowadzone są z udziałem wszystkich członków społeczności szkolnej: uczniów, rodziców i nauczycieli. Aktywizowanie uczniów ma sprawić, by czuli się współodpowiedzialni za swoje funkcjonowanie w sieci oraz za bezpieczeństwo własne i swoich rówieśników online.

Szkoła podejmuje w tym zakresie działania:

1. Publikowanie informacji na szkolnej stronie internetowej dotyczących promocji pozytywnych aspektów internetu, bezpiecznych zachowań w sieci, profilaktyki zagrożeń oraz wskazówek, gdzie szukać pomocy w razie poczucia zagrożenia:
   a) UCZEŃ/BEZPIECZEŃSWO W SIECI https://sp1bielsko.pl/bezpieczenstwo-w-sieci-3
   b) RODZIC/BEZPIECZEŃSTWO W SIECI https://sp1bielsko.pl/bezpieczenstwo-w-sieci-2
   c) NAUKA ZDALNA/BEZPIECZEŃSWO W SIECI https://sp1bielsko.pl/bezpieczenstwo-w-sieci
2. Udział w projekcie „Dzień Bezpiecznego Internetu" (od 2009 r.), organizowanie lokalnych obchodów DBI, mający na celu promocję pozytywnego wykorzystania internetu oraz propagowanie bezpieczeństwa cyfrowego
   (Organizator: https://www.saferinternet.pl/dbi/o-dbi.html)
3. Działania profilaktyczne aktywizujące uczniów w akcje promujące rozwój umiejętności cyfrowych oraz świadomego funkcjonowania w mediach społecznościowych:
   a) nauka kodowania i programowania („Europejski Tydzień kodowania", globalna akcja "Godzina kodowania")
   b) praca na platforamch e-learningowych https://code.org/, https://pixblocks.com/
   c) udział w konkursach informatycznych szkolnych, międzyszkolnych i międzynarodowych.

16. AKTY PRAWNE, TELEFONY/KONTAKTY ALARMOWE

Akty prawne

Ustawa z dnia 7 września 1991 r. o systemie oświaty (Dz. U. z 2019 r. poz. 1481)

Ustawa z dnia 14 grudnia 2016 r. – Prawo oświatowe (Dz. U. z 2019 r., poz. 1148, z późn. zm.)

Ustawa z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną. (Dz.U. 2002 nr 144 poz. 1204)

Ustawa z dnia 23 kwietnia 1964 r. – Kodeks cywilny. (Dz.U. 1964 nr 16 poz. 93)

Konwencja o prawach dziecka, przyjęta przez Zgromadzenie Ogólne Narodów Zjednoczonych dnia 20 listopada 1989 r. (Dz.U. 1991 nr 120 poz. 526)

Telefony alarmowe krajowe

- 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.pl dyzurnet@dyzurnet.pl, 801 615 005

Procedura wezwania odpowiednich służb drogą telefoniczną:

1. Wybranie numeru odpowiedniej służby:
   - policja 997
   - pogotowie ratunkowe 999
   - europejski telefon alarmowy (obowiązujący na terenie całej Unii Europejskiej) 112
   - infolinia policji (połączenie bezpłatne) 800 120 226
2. Po zgłoszeniu się dyżurnego operatora danej służby podanie następujących informacji:
   - rodzaj stwierdzonego zagrożenia
   - nazwa i adres szkoły
   - imię i nazwisko oraz pełniona funkcję
   - telefon kontaktowy
   - zrealizowane dotąd działania w reakcji na zagrożenie

17. ŹRÓDŁA INFORMACJI I ZAŁĄCZNIKI

- **Bezpieczna szkoła. Zagrożenia i zalecane działania profilaktyczne w zakresie bezpieczeństwa fizycznego i cyfrowego uczniów – poradnik MEN**
  PORADNIK – Bezpieczna Szkoła. Zagrożenia i zalecane działania profilaktyczne w zakresie bezpieczeństwa fizycznego i cyfrowego uczniów
  Ministerstwo Edukacji Narodowej, we współpracy z organizacjami pozarządowymi, innymi resortami i instytucjami odpowiedzialnymi za bezpieczeństwo, przygotowało Poradnik „Bezpieczna szkoła. Zagrożenia i zalecane działania profilaktyczne w zakresie bezpieczeństwa fizycznego i cyfrowego uczniów", opublikowano 01.09.2020 r.
- **Standard bezpieczeństwa online placówek oświatowych**
  Publikacja opracowana przez zespół ekspertów Naukowej i Akademickiej Sieci Komputerowej (NASK) oraz Wyższej Szkoły Pedagogicznej im. Janusza Korczaka w Warszawie, w ramach projektu „Działania na rzecz bezpiecznego korzystania z Internetu", Wydanie II uzupełnione, Warszawa 2018
  https:// ose.gov.pl/materialy-do-pobrania/standardy-bezpieczenstwa
  rekomendacje: https://akademia.nask.pl/publikacje/ost_Standard_bezpieczenstwa_online_placowek_oswiatowych.pdf
- **Szkolne standardy bezpieczeństwa cyfrowego dzieci i młodzieży,** wydane przez Fundację Dajemy Dzieciom Siłę w 2014 r., kompendium wiedzy na temat rozwiązywania problemów z zagrożeniami internetowymi dotyczącymi dzieci i młodzieży wraz z propozycjami edukacyjnymi nt. bezpieczeństwa w sieci.
  http://dziec- kowsieci.fdn.pl/sites/default/files/file/dziecko-w-sieci/szkolne-standardy-bezpieczenstwa-online.pdf

- **Cyfrowobezpieczni.pl – Bezpieczna Szkoła Cyfrowa**
  Projekt odpowiadający na wyzwania związane z bezpiecznym korzystaniem z zasobów cyberprzestrzeni w polskich szkołach. https://www.cyfrowobezpieczni.pl/

- **ZAŁĄCZNIKI - infografiki obrazujące schemat działań poszczególnych procedur**
  https://www.cyfrowobezpieczni.pl/procedury-bezpieczenstwa-cyfrowego-w-szkolach

1. Dostęp do treści szkodliwych, niepożądanych, nielegalnych publikowanych w Internecie
   https://www.cyfrowobezpieczni.pl/uploads/filemanager/procedury-bezpieczenstwa-cyfrowego/PR_1bl.pdf
2. Cyberprzemoc
   https://www.cyfrowobezpieczni.pl/uploads/filemanager/procedury-bezpieczenstwa-cyfrowego/PR_2bl.pdf
3. Naruszenia prywatności
   https://www.cyfrowobezpieczni.pl/uploads/filemanager/procedury-bezpieczenstwa-cyfrowego/PR_3bl.pdf
4. Zagrożenia dla zdrowia dzieci w związku z nadmiernym korzystaniem z Internetu
   https://www.cyfrowobezpieczni.pl/uploads/filemanager/procedury-bezpieczenstwa-cyfrowego/PR_4bl.pdf
5. Nawiązywanie niebezpiecznych kontaktów w Internecie
   https://www.cyfrowobezpieczni.pl/uploads/filemanager/procedury-bezpieczenstwa-cyfrowego/PR_5bl.pdf
6. Seksting
   https://www.cyfrowobezpieczni.pl/uploads/filemanager/procedury-bezpieczenstwa-cyfrowego/PR_6bl.pdf
7. Bezkrytyczna wiara w treści zamieszczone w Internecie
   https://www.cyfrowobezpieczni.pl/uploads/filemanager/procedury-bezpieczenstwa-cyfrowego/PR_7bl.pdf
8. Łamanie prawa autorskiego
   https://www.cyfrowobezpieczni.pl/uploads/filemanager/procedury-bezpieczenstwa-cyfrowego/PR_8bl.pdf
9. Zagrożenia bezpieczeństwa technicznego sieci, komputerów i zasobów online
   https://www.cyfrowobezpieczni.pl/uploads/filemanager/procedury-bezpieczenstwa-cyfrowego/PR_9bl.pdf