

**Procedury postępowania w przypadku wystąpienia
wewnętrznych i zewnętrznych zagrożeń
w Szkole Podstawowej nr 3
w Sokołowie Podlaskim**

Ustawy regulujące procedury:

1. Ustawa prawo oświatowe z 14.XII.2016r.
2. Ustawa Karta Nauczyciela z 26.I.1982r.
3. Ustawa o postępowaniu w sprawach nieletnich z 26.X.1982r.
4. Ustawa o wychowaniu w trzeźwości i przeciwdziałaniu alkoholizmowi z 2.X. 1982r.
5. Ustawa o przeciwdziałaniu narkomanii z 29.VII.2005r.
6. Kodeks karny z 6.VI.1997r.
7. Ustawa o działaniach antyterrorystycznych z 10.VI.2016r

I. Procedury reagowania po wtargnięciu napastnika do szkoły z niebezpiecznym narzędziem lub bronią.

Napastnik wtargnął z bronią do szkoły, strzela do ludzi na korytarzu lub w salach.

- Jeżeli nie miałeś szansy na ucieczkę, zamknij drzwi na klucz.
- Wycisz i uspokój uczniów.
- Zaopiekuj się szczególnie ze SPE i tymi, którzy potrzebują pomocy.
- Każ bezwzględnie wyciszyć, wyłączyć telefony
- Poinformuj policję wysyłając sms o zaistniałej sytuacji
- Zasłoń okno, zgaś światło
- Nie przemieszczaj się
- Stań poniżej linii okien, zejźdź ze światła drzwi
- Zejźdź z linii strzału, połóż się na podłodze

- Jeżeli padną strzały, nie krzycz
- Nie otwieraj drzwi nikomu

W przypadku bezpośredniego kontaktu z napastnikami, którzy dążą do przejęcia kontroli nad szkołą:

- Wykonuj bezwzględnie polecenia napastnika
- Na żądanie terrorystów oddaj im przedmioty osobiste, np. telefon
- Unikaj kontaktu wzrokowego
- Nigdy nie odwracaj się plecami do napastnika
- Nie zwracaj na siebie uwagi
- Nie lekceważ napastnika i nie bądź agresywny
- Nie oszukuj terrorysty.
- Uspokój uczniów, zwracaj się do nich po imieniu.
- Poinformuj napastników o uczniach ze schorzeniami, niepełnosprawnych
- Pytaj o pozwolenie, jeśli chcesz zwrócić się do uczniów
- Zawsze korzystaj z dobrej woli terrorystów (możliwość zjedzenia posiłku)

W przypadku działań antyterrorystycznych podjętych przez policję:

- Nie uciekaj z miejsca zdarzenia, nie wykonuj gwałtownych ruchów
- Nie próbuj pomagać służbom ratowniczym, dyskutować z nimi
- Połóż się na podłodze , trzymaj ręce z otwartymi dłońmi najlepiej na wysokości głowy- taka pozycja pozwala widzieć ewentualne niebezpieczne narzędzia będące w posiadaniu zamachowców, którzy wtopili się w szeregi zakładników.
- Słuchaj poleceń i instrukcji grupy antyterrorystycznej, poddawaj się jej działaniom
- Pytaj o pozwolenie zaopiekowania się uczniami- samowolne działania utrudniają akcje ratunkową
- Bądź przygotowany na potraktowanie ciebie jako potencjalnego terrorysty ,dopóki twoja tożsamość nie zostanie potwierdzona
- Po wydaniu polecenia wyjścia- opuść pomieszczenie jak najszybciej , oddal się we wskazanym kierunku
- Nie zatrzymuj się dla zabrania rzeczy osobistych, zawsze istnieje ryzyko wybuchu lub pożaru- najważniejsze jest życie i zdrowie

II. Procedury reagowania po otrzymaniu informacji o podłożeniu ładunku wybuchowego:

1. Prowadząc rozmowę z osobą informującą o podłożeniu ładunku wybuchowego zapamiętaj jak najwięcej szczegółów.
2. Zapisz natychmiast wszystkie uzyskane informacje.
3. Poinformuj osobę odpowiedzialną w szkole za uruchomienie procedury ewakuacji- dyrektora
4. Po usłyszeniu sygnału o podłożeniu ładunku wybuchowego rozpocznij ewakuację zgodnie z planem ewakuacji
5. Nie używaj telefonu komórkowego
6. Sprawdź, czy w klasie nie ma przedmiotów, które nie należą do jej wyposażenia.
7. Bezwzględnie wykonuj polecenia osoby kierującej sytuacją kryzysową lub funkcjonariuszy policji.
8. W miejscu ewakuacji policz wszystkie dzieci i poinformuj osobę odpowiedzialną za kierowanie działaniami kryzysowymi .
9. Poinformuj rodziców o miejscu odbioru dzieci i drodze dojazdu w celu sprawnego odbioru dzieci.

ZAGROŻENIA WEWNĘTRZNE

Do najbardziej istotnych zagrożeń wewnętrznych w szkole należą: agresywne zachowania ucznia oraz zjawisko tzw. fali, używanie przez uczniów substancji psychoaktywnych, kradzież lub wymuszenia pieniędzy czy przedmiotów wartościowych, pedofilia, pornografia, prostytutcja, wypadek lub czyn karalny dokonany przez ucznia.

III. Procedury postępowania na wypadek agresywnego zachowania w szkole lub tzw. fali.

Procedura jest uruchamiana przez osobę, która zauważyła agresywne zachowanie lub które jej zgłoszono. Czynnościami interwencyjnymi kieruje dyrektor lub osoba przez niego wyznaczona.

Obowiązkiem każdego pracownika szkoły jest zdecydowana i stanowcza reakcja wobec uczestników agresji, zmierzająca do przerwania agresywnego zachowania.

1. W przypadku zagrożenia życia, zdrowia, należy bezzwłocznie zawiadomić pogotowie ratunkowe, nawet bez zgody rodzica.
2. Decyzję o dalszym leczeniu ucznia podejmują rodzice.
3. Pedagog/psycholog przeprowadzają rozmowy z rodzicami obydwu stron oraz ze sprawcą i ofiarą , ustalając okoliczności zdarzenia. Sporządzają dokumentację zdarzenia.

4. Pedagog/psycholog powinien udzielić pomocy psychologicznej ofierze przemocy.
5. Wobec agresora stosuje się konsekwencje określone w statucie szkoły.
6. W przypadku powtarzania się kolejnych ataków przez agresora-szkoła kieruje sprawę na policję.

IV. Procedury postępowania w przypadku wystąpienia kradzieży lub wymuszenia pieniędzy czy przedmiotów wartościowych

1. Procedury postępowania prowadzi dyrektor, w przypadku nieobecności pedagoga.
2. Osoba , która wykryła kradzież , winna bezwzględnie powiadomić dyrektora szkoły.
3. Należy przekazać sprawcę czynu, o ile jest znany pod opiekę pedagoga lub dyrektora.
4. Należy zabezpieczyć dowody przestępstwa, tj. przedmiotów pochodzących z kradzieży lub wymuszenia i przekazać policji.
5. Należy zażądać , aby uczeń przekazał skradzioną rzecz, pokazał zawartość plecaka oraz kieszenie w obecności wychowawcy, pedagoga, dyrektora. Pracownik szkoły nie może samodzielnie wykonać czynności przeszukiwania rzeczy osobistych ucznia, wyłącznie może to zrobić policja.
6. We współpracy z pedagogiem należy ustalić okoliczności czynu.
7. Dyrektor szkoły wzywa rodziców sprawcy i rozmawia z uczniem w ich obecności.
8. Zawiadamia policję.
9. Sprawca winien dokonać zadośćuczynienia poszkodowanemu.

V. Procedura wystąpienia przypadku pedofilii w szkole.

1. Procedury reagowania uruchamia dyrektor(wicedyrektor lub osoba upoważniona) w przypadku pojawienia się osób, co do których zachodzi podejrzenie psychicznego bądź fizycznego molestowania dzieci lub nakłaniania do czynności seksualnych.
2. Po stwierdzeniu zagrożenia należy zawiadomić dyrektora szkoły.
3. W sytuacji potwierdzenia informacji o pojawieniu się osób obcych, zaczepiających uczniów, należy bezzwzględnie zawiadomić policję.
4. Wychowawcy klas powinni podjąć działania informacyjne wśród uczniów w celu wskazania potencjalnego zagrożenia.

5. W przypadku stwierdzenia, że uczeń był molestowany, bezzwłocznie należy zawiadomić rodziców ucznia oraz policję w celu przeprowadzenia czynności sprawdzających, ustalenie sprawcy.
6. Pedagog/psycholog przeprowadza rozmowę z uczniem w obecności rodzica-ustalając okoliczności zdarzenia.
7. Dyrektor w porozumieniu z rodzicami i psychologiem ustala dalsze działania w celu zapewnienia opieki nad uczniem i pomocy terapeutycznej.
Wychowawcy klas w ramach działań profilaktycznych poinformują uczniów, aby zgłaszali do rodziców i nauczycieli wszelkie przypadki zaczepiania ich przez osoby obce pod szkołą. Uczniowie powinni stanowczo odmawiać na jakiegokolwiek propozycje, np. podwiezienia do domu, przyjmowania cukierków, napojów, innych prezentów, wchodzenia w rozmowy.

VI. Procedura postępowania na wypadek rozpowszechniania pornografii przez ucznia w szkole.

1. W przypadku uzyskania informacji przez nauczyciela/rodzica o rozpowszechnianiu przez ucznia w Internecie, w szkole należy bezzwłocznie powiadomić dyrektora szkoły oraz administratora sieci o zaistniałym zdarzeniu.
2. W przypadku , kiedy uczeń przekazuje informację o osobach, które pokazywały materiały pornograficzne, konieczne jest zapewnienie anonimowości temu uczniowi.
3. Dyrektor wzywa rodziców ucznia, który popełnił wykroczenie, przeprowadza rozmowę w obecności pedagoga/psychologa.
4. Wychowawcy klas winni w ramach działań profilaktycznych wskazać uczniom na zagrożenia , jakie niesie ze sobą upublicznianie materiałów pornograficznych, konsekwencje tego typu działań.

VII. Procedura postępowania w sytuacji wystąpienia przypadków prostytucji w szkole wśród uczniów.

1. W przypadku otrzymania informacji, w której uczeń był świadkiem czynności mogących mieć znamiona prostytucji, nauczyciel/pracownik zawiadamia dyrektora.
2. W przypadku uzyskania informacji, że uczeń , który nie ukończył 18 lat, uprawia nierząd, bądź przejawia inne

zachowania świadczące o demoralizacji, nauczyciel powiadamia wychowawcę klasy, który wzywa rodziców.

3. Wychowawca w obecności psychologa przeprowadza rozmowę z rodzicami oraz z uczniem zobowiązując do zaniechania ujawnionego zachowania. Można ponadto zaproponować rodzicom kontakt ze specjalistą i podjęcie działań terapeutycznych.
4. Jeśli rodzice odmawiają współpracy, dyrektor powinien pisemnie powiadomić o zaistniałej sytuacji sąd rodzinny lub policję.

VIII. Procedury reagowania w przypadku niepokojących zachowań seksualnych uczniów.

1. Nauczyciel lub inny pracownik szkoły powinien powiadomić wychowawcę, pedagoga o zauważeniu niepokojących zachowań seksualnych ucznia/uczniów.
2. Wychowawca/pedagog przeprowadza rozmowę z uczniem, co do którego zachodzi podejrzenie o zachowania powyższe, następnie zawiadamia rodziców ucznia. Wzywa rodziców do szkoły, ustalając okoliczności, przyczyny sytuacji oraz dalsze postępowanie z dzieckiem.
3. Jeśli rodzice odmawiają współpracy, a zachowanie dziecka wskazuje w dalszym ciągu na znaczny stopień demoralizacji, np. uprawianie nierzędu, dyrektor zawiadamia sąd rodzinny lub policję.
4. Gdy zachowanie ucznia może świadczyć o popełnieniu przez niego przestępstwa, np. gwałtu, dyrektor po uprzednim powiadomieniu rodziców o zajściu, powiadamia policję.
5. W przypadku, kiedy uczeń zgłasza, że był świadkiem niepokojących zachowań seksualnych, konieczne jest zapewnienie mu anonimowości w celu ochrony przed konsekwencjami ze strony tych, którzy brali udział w tego typu zachowaniach.

IX. Procedury postępowania na wypadek popełnienia przez ucznia czynu karalnego.

Czyny karalne dotyczą czynów zabronionych przez ustawę o postępowaniu w sprawach nieletnich rozumianych jako przestępstwo, przestępstwo skarbowe albo wykroczenie określone w artykułach:

- art.50a - posiadanie noża, maczety lub innego niebezpiecznego przedmiotów miejscu publicznym
- art.51- zakłócenie spokoju lub porządku publicznego
- art. 69 - umyślne niszczenie, uszkodzanie, usuwanie znaków.
- art.74- niszczenie, uszkodzanie, usuwanie znaków ostrzegawczych
- art.76- rzucanie przedmiotami w pojazd mechaniczny
- art.85- samowolne ustawianie, niszczenie znaków
- art.. 87- prowadzenie pojazdu w stanie po użyciu alkoholu
- art.119- kradzież lub przywłaszczenie
- art.122- paserstwo czyli nabycie mienia, wiedząc , że pochodzi ono z kradzieży
- art. 124- niszczenie lub uszkodzenie cudzej rzeczy
- art.133- spekulacja biletami
- 143- utrudnianie lub uniemożliwianie korzystania z urządzeń użytku publicznego.

1. Osoba będąca świadkiem zdarzenia zobowiązana jest do powiadomienia dyrektora
2. Dyrektor odpowiada za ustalenie okoliczności czynu i ewentualnych świadków zdarzenia
3. W przypadku , gdy sprawca jest znany i przebywa na terenie szkoły, winien być zatrzymany i przekazany pod opiekę pedagoga lub dyrektora.
4. Dyrektor zawiadamia rodziców ucznia o zaistniały przypadku.
5. Dyrektor jest zobowiązany do niezwłocznego powiadomienia policji w przypadku, gdy sprawa jest poważna, np. rozbój, uszkodzenie ciała lub w sytuacji, gdy nieletni sprawca nie jest uczniem szkoły i jego tożsamość jest nieznana. Do obowiązków dyrektora należy również zabezpieczenie ewentualnych przedmiotów pochodzących z przestępstwa i przekazanie policji.
6. W sytuacji ucznia będącego ofiarą czynu karalnego należy udzielić mu odpowiedniej pomocy.
7. Osoba będąca świadkiem zagrożenia, winna udzielić poszkodowanemu pierwszej pomocy, wezwać lekarza, jeśli ofiara doznała obrażeń.
8. Obowiązkiem dyrektora jest powiadomić rodziców ucznia – ofiary czynu karalnego o zdarzeniu.
9. Uczeń powinien otrzymać profesjonalną pomoc psychologiczną- w porozumieniu z jego rodzicami.

X. Procedury postępowania w sytuacji wypadku ucznia.

Wypadek ucznia jest to nagle zdarzenie wywołane przyczyną zewnętrzną, powodujące uraz lub śmierć. Które nastąpiło w czasie pozostawania ucznia pod opieką szkoły lub poza jej terenem (wycieczki, wyjazdu pod opieką nauczyciela)

1. Pracownik szkoły, który uzyskał informację o wypadku ucznia niezwłocznie zapewnia poszkodowanemu opiekę, zawiadamiając pogotowie ratunkowe, udzielając pierwszej pomocy. Jest to prawny obowiązek każdego pracownika szkoły. Nieudzielenie pomocy skutkuje sankcją karną.
2. Jeśli wypadek ma miejsce na lekcji, nauczyciel przerywa lekcję, zawiadamia dyrektora szkoły. Jeżeli istnieje zagrożenie dla bezpieczeństwa uczniów w Sali, wyprowadza ich na zewnątrz.
3. O każdym wypadku zawiadamia się niezwłocznie rodziców ucznia, pracownika szkoły odpowiedzialnego za bezpieczeństwo i higienę pracy, społecznego inspektora pracy, organ prowadzący szkołę oraz radę rodziców.

O wypadku śmiertelnym zawiadamia się prokuratora i kuratora oświaty. Zawiadomień dokonuje dyrektor, dokumentując zgłoszenie w dzienniku zajęć lekcyjnych.

Jeżeli wypadek zdarzył się na wycieczce, imprezie szkolnej, wszystkie stosowne decyzje podejmuje opiekun grupy/kierownik wycieczki i odpowiada za nie. Do czasu rozpoczęcia pracy przez zespół powypadkowy dyrektor zabezpiecza miejsce wypadku w sposób wykluczający osoby niepowołane.

4. Dyrektor szkoły powołuje zespół powypadkowy, który przeprowadza postępowanie powypadkowe i sporządza odpowiednią dokumentację-protokół powypadkowy.

XI. Procedury postępowania wobec ucznia, który jest pod wpływem środków uzależniających (lub istnieje takie podejrzenie).

1. Nauczyciel lub inny pracownik szkoły powiadamia o swoich podejrzeniach wychowawcę klasy i dyrektora.
2. Odizolowuje ucznia od reszty klasy , zapewniając mu bezpieczeństwo.
3. Dyrektor informuje o zaistniałym zdarzeniu rodziców ucznia i wzywa ich do natychmiastowego stawiennictwa w szkole.
4. W przypadku ucznia , który zagraża bezpieczeństwu innych, a rodzice odmawiają przyjazdu do szkoły, dyrektor powiadamia Policję.

5. Psycholog szkolny dokonuje wstępnej diagnozy problemu ucznia i w porozumieniu z rodzicami określa rodzaj udzielanej pomocy psychologicznej/terapeutycznej.
6. Uczeń podpisuje tzw. kontrakt, w którym zobowiązuje się do zaniechania używania substancji psychoaktywnych. Poności konsekwencje ustalone w statucie szkoły.

XII. Procedury w przypadku podejrzenia ucznia o posiadanie środków uzależniających:

1. Nauczyciel powiadamia dyrektora szkoły, który powiadamia Policję.
2. Dyrektor żąda od ucznia pokazania zawartości plecaka, kieszeni.
3. Zawiadamia rodziców ucznia i informuje o obowiązujących procedurach w szkole.
4. Dyrektor w obecności pedagoga/psychologa przeprowadza rozmowę z uczniem.
5. Uczeń zostaje objęty działaniami profilaktycznymi, psychologicznymi – w porozumieniu z rodzicami.

XIII. Procedury w przypadku znalezienia środków uzależniających.

1. Nauczyciel zabezpiecza znalezioną substancję przed dostępem innych uczniów.
2. Powiadamia o tym dyrektora, który informuje o tym fakcie Policję.

XIV. Procedury postępowania wobec osoby obcej na terenie szkoły bądź przyszkolnym.

Przez osobę obcą na terenie szkoły rozumie się osobę, która:

- nie jest rodzicem ucznia szkoły
- nie jest pracownikiem szkoły
- nie jest osobą wypełniającą aktualnie zadania zleczone przez dyrektora szkoły.
- swoim zachowaniem w wyraźny sposób narusza zasady i normy współżycia społecznego bądź stanowi zagrożenie dla bezpieczeństwa uczniów i pracowników szkoły.

1. Nauczyciel lub pracownik szkoły ustala powody obecności osoby postronnej w szkole.
2. W sytuacji niepokojących zachowań powiadamia dyrektora, który nakazuje tej osobie opuścić teren placówki.
3. W przypadkach drastycznych dyrektor powiadamia niezwłocznie policję, podejmując działania, mające na celu ochronę dzieci i pracowników.

ZASADY REAGOWANIA W SYTUACJI NARUSZENIA BEZPIECZEŃSTWA CYFROWEGO

Wyróżniono 9 podstawowych zagrożeń bezpieczeństwa cyfrowego w środowisku szkolnym, którym przypisano opracowane według jednego standardu opisu procedury reagowania.

RODZAJE ZAGROŻEŃ:

1. DOSTĘP DO TREŚCI SZKODLIWYCH, NIEPOŻĄDANYCH I NIELEGALNYCH

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

2. CYBERPRZEMOC

Zjawisko cyberprzemocy najkrócej definiuje się jako przemoc z użyciem technologii informacyjnych i komunikacyjnych. Technologie te to głównie Internet oraz telefony komórkowe. Część definicji ogranicza stosowanie terminu *cyberbullying* czy *cyberprzemoc* wyłącznie do przemocy rówieśniczej, inne nie stawiają ograniczeń wiekowych, niewątpliwie jednak najczęściej terminów tych używa się właśnie w kontekście przemocy wśród najmłodszych. ***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. W odróżnieniu od „tradycyjnej” przemocy (ang. *bullying*) zjawisko cyberprzemocy charakteryzuje wysoki poziom anonimowości sprawcy. Ponadto na znaczeniu traci klasycznie rozumiana „siła”, mierzona cechami fizycznymi czy społecznymi, a atutem sprawcy staje się umiejętność wykorzystywania możliwości, jakie dają media elektroniczne.

3. NARUSZENIA PRYWATNOŚCI DOTYCZĄCE NIEODPOWIEDNIEGO BĄDŹ NIEZGODNEGO Z PRAWEM WYKORZYSTANIA DANYCH OSOBOWYCH LUB WIZERUNKU DZIECKA I PRACOWNIKA SZKOŁY

Zagrożenie to polega na naruszeniu prywatności dziecka lub pracownika szkoły poprzez nieodpowiednie lub niezgodne z prawem wykorzystanie danych osobowych lub wizerunku dziecka i pracownika szkoły. Należy zwrócić uwagę, iż podszywanie się pod inną osobę, wykorzystywanie jej wizerunku lub danych osobowych w celu wyrządzenia jej szkody osobistej lub majątkowej jest w świetle polskiego prawa przestępstwem. Najczęstszymi formami wyłudzenia lub kradzieży danych jest 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 (np. w sklepach internetowych na koszt ofiary) lub uzyskania korzyści (np. usługi premium SMS). Często naruszenia prywatności łączy się z cyberprzemocą

4. ZAGROŻENIA DLA ZDROWIA DZIECI W ZWIĄZKU Z NADMIERNYM KORZYSTANIEM Z INTERNETU

Infoholizm (siecioholizm) – nadmierne, obejmujące niekiedy niemal całą dobę korzystanie z zasobów Internetu i gier komputerowych (najczęściej sieciowych) i 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.

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).

6. SEKSTING, PROWOKACYJNE ZACHOWANIA I AKTYWNOŚĆ SEKSUALNA JAKO ŹRÓDŁO DOCHODU OSÓB NIELETNICH

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.

7. BEZKRYTYCZNA WIARA W TREŚCI ZAMIESZCZONE W INTERNECIE, NIEUMIEJĘTNOŚĆ ODRÓŻNIENIA TREŚCI PRAWDZIWYCH OD NIEPRAWDZIWYCH, SZKODLIWOŚĆ REKLAM

Brak umiejętności odróżniania informacji prawdziwych od nieprawdziwych publikowanych w Internecie, bezkrytyczne uznawanie za prawdę też publikowanych w forach internetowych, kierowanie się informacjami zawartymi w reklamach. Taka postawa dzieci prowadzi 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 osiągnięcie dobrych wyników w edukacji (korzystanie z upraszczających i zawężających temat „ściągi” i „bryków”), a także utrwalenia się u ucznia ambiwalentnych postaw moralnych

8. ŁAMANIE PRAWA AUTORSKIEGO

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

9. ZAGROŻENIA BEZPIECZEŃSTWA TECHNICZNEGO SIECI, KOMPUTERÓW I ZASOBÓW ONLINE

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, exploit, ataki słownikowe i back door, skanowanie portów, phishing, pharming, sniffing, spoofing, ataki Denial of service (DoS), 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.

Procedura reagowania w szkole w sytuacji naruszenia bezpieczeństwa cyfrowego.

I. Ujawnienie przypadku naruszenia bezpieczeństwa cyfrowego

Informacja o tym, że w szkole miała miejsce naruszenia bezpieczeństwa cyfrowego, może pochodzić z różnych źródeł. Osobą zgłaszającą fakt prześladowania może być poszkodowany uczeń, jego rodzice lub inni uczniowie – świadkowie zdarzenia, nauczyciele. Niezależnie od tego, kto zgłasza przypadek, procedura interwencyjna powinna obejmować:

- udzielenie wsparcia ofierze przemocy;
- zabezpieczenie dowodów i ustalenie okoliczności zdarzenia;
- wyciągnięcie konsekwencji wobec sprawcy przemocy oraz praca nad zmianą postawy ucznia.

II. Ustalenie okoliczności zdarzenia

Wszystkie przypadki przemocy, a więc także przemocy z wykorzystaniem mediów elektronicznych, powinny zostać właściwie zbadane, zarejestrowane i udokumentowane.

1. Jeśli wiedzę o zajściu posiada nauczyciel niebędący wychowawcą, powinien przekazać informację wychowawcy klasy, który informuje o fakcie pedagoga szkolnego/psychologa i dyrektora.

2. Pedagog szkolny/psycholog i dyrektor wspólnie z wychowawcą powinni dokonać analizy zdarzenia i zaplanować dalsze postępowanie.

3. Do zadań szkoły należy także ustalenie okoliczności zdarzenia i ewentualnych świadków.

4. Warto zadbać o udział nauczyciela informatyki w procedurze interwencyjnej, szczególnie na etapie zabezpieczania dowodów i ustalania tożsamości sprawcy naruszenia bezpieczeństwa cyfrowego.

III. Zabezpieczenie dowodów

1. Wszelkie dowody naruszenia bezpieczeństwa cyfrowego 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/psycholog, rodzice, a wreszcie policja, jeśli doszło do złamania prawa.

3. Na etapie zabezpieczania dowodów naruszenia bezpieczeństwa cyfrowego i identyfikacji sprawcy warto korzystać z pomocy nauczyciela informatyki.

IV. Identyfikacja sprawcy

Co może pomóc w identyfikacji sprawcy?

1. **Świadkowie** – inni uczniowie odwiedzający „obraźliwe” strony mogą posiadać informacje na temat ich autora, mogą też zidentyfikować numer telefonu komórkowego sprawcy, jeśli nie jest on zastrzeżony.

2. Kontakt z dostawcą usługi internetowej – może on nie tylko zablokować konto agresora lub usunąć szkodliwe treści, ale także podać dane sprawcy naruszenia bezpieczeństwa cyfrowego. Dane takie nie mogą być jednak udostępniane osobom prywatnym. Aby je pozyskać, konieczny jest kontakt z policją.

3. Kontakt z operatorem sieci komórkowej w przypadku, gdy numer telefonu sprawcy jest zastrzeżony – może on podjąć kroki w kierunku ustalenia sprawcy, jeśli otrzyma dane o dacie i godzinie rozmowy. Również w tym przypadku operator może udostępnić te dane tylko policji.

4. Gdy ustalenie sprawcy nie jest możliwe, należy skontaktować się z dostawcą usługi w celu usunięcia z sieci kompromitujących lub krzywdzących materiałów. Do podjęcia takiego działania zobowiązuje administratora serwisu art. 14 Ustawy z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną.

5. W przypadku, gdy zostało złamane prawo, a tożsamości sprawcy nie udało się ustalić należy bezwzględnie skontaktować się z policją.

V. Działania wobec sprawcy naruszenia bezpieczeństwa cyfrowego.

Gdy sprawca naruszenia bezpieczeństwa cyfrowego jest znany i jest on uczniem szkoły, pedagog szkolny/psycholog powinien podjąć dalsze działania.

1. Rozmowa z uczniem-sprawcą przemocy o jego zachowaniu

- celem rozmowy powinno być ustalenie okoliczności zajścia, wspólne zastanowienie się nad jego przyczynami i poszukanie rozwiązania sytuacji konfliktowej;
- sprawca powinien otrzymać jasny i zdecydowany komunikat o tym, że szkoła nie akceptuje żadnych form przemocy;

- należy omówić z uczniem skutki jego postępowania i poinformować o konsekwencjach regulaminowych, które zostaną wobec niego zastosowane;
- sprawca powinien zostać zobowiązany do zaprzestania swojego działania i usunięcia z sieci szkodliwych materiałów;
- ważnym elementem rozmowy jest też określenie sposobów zadośćuczynienia wobec ofiary cyberprzemocy;
- jeśli w zdarzeniu brała udział większa grupa uczniów, należy rozmawiać z każdym z nich z osobna, zaczynając od lidera grupy;
- nie należy konfrontować sprawcy i ofiary naruszenia bezpieczeństwa cyfrowego.

2. Powiadomienie rodziców sprawcy i omówienie z nimi zachowania dziecka:

- rodzice sprawcy powinni zostać poinformowani o przebiegu zdarzenia i zapoznani z materiałem dowodowym, a także z decyzją w sprawie dalszego postępowania i podjętych przez szkołę środków dyscyplinarnych wobec ich dziecka;
- w miarę możliwości należy starać się pozyskać rodziców do współpracy i ustalić jej zasady;

3. Objęcie sprawcy opieką psychologiczno-pedagogiczną:

- praca ze sprawcą powinna zmierzać w kierunku pomocy uczniowi w zrozumieniu konsekwencji swojego zachowania, w zmianie postawy i postępowania ucznia, w tym sposobu korzystania z nowych technologii;

- jeśli szkoła posiada odpowiednie warunki, pomoc psychologiczna może być udzielona sprawcy na terenie szkoły;

VI .Zastosowanie środków dyscyplinarnych wobec sprawcy naruszenia bezpieczeństwa cyfrowego.

1. Należy pamiętać, iż celem sankcji wobec sprawcy jest:

- zatrzymanie przemocy i zapewnienie poczucia bezpieczeństwa poszkodowanemu uczniowi;
- wzbudzenie refleksji na temat swojego zachowania, zrozumienie krzywdy, jaką spowodował, i powstrzymanie przed podobnym zachowaniem w przyszłości;
- pokazanie społeczności szkolnej, że naruszenia bezpieczeństwa cyfrowego nie będzie tolerowana i że szkoła jest w stanie efektywnie zareagować w tego rodzaju sytuacji.

2. Podejmując decyzję o rodzaju kary, należy wziąć pod uwagę:

- rozmiar i rangę szkody – czy materiał został upubliczniony w sposób pozwalający na dotarcie do niego wielu osobom (określa to rozmiar upokorzenia, jakiego doznaje ofiara), czy trudno jest wycofać materiał z sieci itp.;
- czas trwania prześladowania – czy było to długotrwałe działanie, czy pojedynczy incydent;
- świadomość popełnianego czynu – czy działanie było zaplanowane, a sprawca był świadomy, że wyrządza krzywdę koledze (niektóre akty naruszenia bezpieczeństwa cyfrowego popełniane są nieświadomie lub z niewielką

świadomością konsekwencji), jak wiele wysiłku włożył w ukrycie swojej tożsamości itp.;

- motywację sprawcy – należy sprawdzić, czy działanie sprawcy nie jest działaniem odwetowym w odpowiedzi na uprzednio doświadczone prześladowanie;
- rodzaj rozpowszechnianego materiału.

VII .Działania wobec ofiary naruszenia bezpieczeństwa cyfrowego.

1. *Wsparcie psychiczne*

Podobnie jak w przypadku innych form przemocy, ofiara naruszenia bezpieczeństwa cyfrowego potrzebuje pomocy i emocjonalnego wsparcia ze strony dorosłych. Musi także wiedzieć, że szkoła podejmie odpowiednie kroki w celu rozwiązania problemu.

2. *Porada*

Uczeń będący ofiarą naruszenia bezpieczeństwa cyfrowego powinien otrzymać poradę, jak ma się zachować, aby zapewnić sobie poczucie bezpieczeństwa i nie doprowadzić do eskalacji prześladowania.

3. *Monitoring*

- Po zakończeniu interwencji warto monitorować sytuację ucznia sprawdzając, czy nie są wobec niego podejmowane dalsze działania przemocowe bądź odwetowe ze strony sprawcy.

- Rodzice dziecka będącego ofiarą naruszenia bezpieczeństwa cyfrowego powinni być poinformowani o problemie i otrzymać wsparcie i pomoc ze strony szkoły. W rozmowie z nimi pedagog/psycholog lub wychowawca przedstawiają kroki, jakie zostały podjęte w celu wyjaśnienia zajścia oraz zapewnienia bezpieczeństwa poszkodowanemu uczniowi, a także, jeśli to wskazane, zaproponować rodzicom i dziecku pomoc specjalisty.

VIII. Ochrona świadków zgłaszających zdarzenie

Jak zachować się wobec świadka zgłaszającego naruszenia bezpieczeństwa cyfrowego?

1. Powiedz, że dobrze zrobił, zgłaszając fakt przemocy.
2. Powiedz, że wymagało to od niego wiele odwagi.
3. Zapewnij o swojej dyskrecji.
4. Nie ujawniaj jego danych, jeśli nie jest to konieczne (np. gdy sprawa została zgłoszona na policję).
5. Pod żadnym pozorem nie konfrontuj go ze sprawcą.
6. Zadbaj o jego bezpieczeństwo, nie upubliczniając jego udziału w sprawie

IX. Sporządzenie dokumentacji z zajścia

1. Pedagog szkolny/psycholog zobowiązany jest do sporządzenia notatki służbowej.
2. Jeśli rozmowa przebiegała w obecności świadka (np. wychowawcy), powinien on podpisać notatkę po jej sporządzeniu.

3. Jeśli zostały zabezpieczone dowody cyberprzemocy, należy je również włączyć do dokumentacji pedagogicznej (wydruki, opis itp.).

X. Współpraca szkoły z policją i sądem rodzinnym

Większość przypadków cyberprzemocy nie wymaga powiadamiania sądu rodzinnego czy policji i powinna być rozwiązywana przy użyciu dostępnych szkole środków wychowawczych. Istnieją jednak sytuacje, gdy konieczne staje się zgłoszenie sprawy do sądu rodzinnego, a mianowicie:

1) jeśli rodzice sprawcy naruszenia bezpieczeństwa cyfrowego odmawiają współpracy lub nie stawiają się do szkoły, a uczeń nie zaniechał dotychczasowego postępowania, dyrektor szkoły powinien pisemnie powiadomić o zaistniałej sytuacji sąd rodzinny, szczególnie jeśli do szkoły napływają informacje o innych przejawach demoralizacji dziecka;

2) gdy szkoła wykorzysta wszystkie dostępne jej środki wychowawcze (rozmowa z rodzicami, konsekwencje regulaminowe wobec ucznia, spotkania z pedagogiem/psychologiem itp.), a ich zastosowanie nie przynosi pożądanych rezultatów, dyrektor powinien zwrócić się do sądu rodzinnego z wnioskiem o podjęcie odpowiednich środków wynikających z Ustawy o postępowaniu z nieletnimi.

W ramach ogólnej współpracy szkoły z policją mogą być organizowane:

- spotkania pedagogów szkolnych, nauczycieli, dyrektora szkoły z zaproszonymi specjalistami ds. nieletnich dotyczące zagrożeń naruszenia bezpieczeństwa cyfrowego w środowisku lokalnym;

- spotkania młodzieży szkolnej z udziałem policjantów m.in. na temat odpowiedzialności nieletnich za popełniane czyny karalne, na temat zasad bezpieczeństwa oraz sposobów unikania zagrożeń związanych z naruszenia bezpieczeństwa cyfrowego ;