Procedury reagowania w przypadku zagrożenia bezpieczeństwa cyfrowego w Zespole Szkół w Żółkiewce

Spis treści

I. CEL PROCEDURY

Celem procedur jest zapewnienie bezpieczeństwa uczniom w środowisku cyfrowym - wprowadzenie działań profilaktycznych, stworzenie procedur postępowania na wypadek pojawienia się cyberzagrożeń w Zespole Szkół w Żółkiewce.

Cele szczegółowe:
- Zapewnienie młodzieży aktualnej wiedzy na temat korzystania z zasobów Internetu.
- Kształtowanie postaw odpowiedzialnej aktywności w środowisku cyfrowym.
- Zapewnienie spójności prawidłowych zachowań w szkole, w przestrzeni publicznej i w domu rodzinnym.

II. ZAKRES STOSOWANIA

Procedura obowiązuje na terenie Zespołu Szkół w Żółkiewce oraz w trakcie trwania zajęć organizowanych w trybie stacjonarnym, zdalnym i hybrydowym.

III. POLITYKA BEZPIECZEŃSTWA CYFROWEGO

Profilaktyka:
Podstawą zapewnienia bezpieczeństwa cyfrowego w szkole są działania profilaktyczne, prowadzone wobec i z udziałem całej społeczności szkolnej. Jest to praca systemowa, ciągła, skoordynowana i wieloletnia.
W trakcie roku szkolnego, szkoła powinna:
1. Pedagog szkolny powinien zaplanować spotkania dla uczniów z edukatorem / policjantem / informatykiem w zakresie tematyki korzystania z Internetu – 1 raz w roku.

2. Wychowawcy klas powinni przeprowadzić co najmniej jedną lekcję wychowawczą na temat danego aspektu cyberbezpieczństwa – raz w roku.
3. Samorząd Uczniowski powinien utworzyć szkolną tablicę informacyjną, dotyczącą aktualności i różnych zagadnień na temat bezpieczeństwa cyfrowego. Na tablicy powinny znajdować się numery telefonów pod którymi można zgłaszać przypadki naruszenia bezpieczeństwa cyfrowego w sposób anonimowy, kontakty do osób, odpowiedzialnych za bezpieczeństwo cyfrowe w szkole.
4. Dyrektor szkoły powinien zorganizować co najmniej jedno zebranie rady pedagogicznej w danym roku szkolnym o tematyce bezpieczeństwa cyfrowego.
5. Bibliotekarz powinien zachęcać do lektury bezpłatnych publikacji na temat cyberbezpieczeństwa, zamieszczonych na stronie Naukowej i Akademickiej Sieci Komputerowej, będącej operatorem Ogólnopolskiej Sieci Edukacyjnej (https://. saferinternet.pl; https://akademia.nask.pl/baza-wiedzy. html; https://ose.gov.pl/materialy-do-pobra-nia; https://www.gov.pl/web/niezagubdzieckawsieci).
6. Wychowawcy klas powinni uświadamiać rodziców i uczniów w znaczeniu działań wychowawczych z zakresu bezpieczeństwa cyfrowego poprzez:
   6.1. krótkie szkolenia dla rodziców i uczniów z wykorzystaniem ulotek i prezentacji multimedialnych,
   6.2. poruszenie tematu bezpieczeństwa cyfrowego w trakcie zebrania z rodzicami,
   6.3. poinformowanie rodziców (w przypadku wystąpienia zagrożenia cyberbezpieczeństwa w klasie) o tym fakcie i przeprowadzenie spotkania poświęconego temu incydentowi,
   6.4. przesyłanie informacji poprzez dziennik elektroniczny na temat potencjalnych zagrożeń wraz z linkami do materiałów edukacyjnych i multimedialnych.
7. Administrator szkolnej sieci powinien opracować i wdrożyć "politykę bezpieczeństwa cyfrowego", nastawioną na eliminowanie zagrożeń sieci komputerowych, systemów operacyjnych i innego oprogramowania wykorzystywanego w szkole.

IV. Rodzaje cyberzagrożeń

Cyberzagrożenia dzieli się na 7 kategorii:

1. Kontakty z nieodpowiednimi treściami (cyberpornografia, cyberprostytucja, sexting, sponsoring, treści propagujące niezdrowy tryb życia).
2. Niebezpieczne działania (cyberprzemoc, samobójstwa, które są inspirowane wpływem sieci np. transmitowane na żywo w Internecie lub popełnianie wskutek gnębienia — w sieci można również znaleźć instruktaże dla samobójców oraz pakty samobójcze).
3. Niebezpieczne kontakty (child grooming = uwodzenie dzieci online, cyberpedofilia).
4. Naruszenie prywatności (cyberstalking).
5. Zagrożenia seksualne (cyberseks, sexting).
6. Zespół uzależnienia od Internetu.
7. Cyberprzestępczość (kradzież danych osobowych, fałszywe pliki cookies zawierające szkodli-we oprogramowanie, ataki hakerskie na sieci społecznościowe, tabnabbing = fałszywe witryny internetowe, clickjacking = maskowanie odnośnika w celu kliknięcia w link podsunięty przez przestępcę, zagrożenia systemów mobilnych).

V. DZIAŁANIA NA RZECZ BEZPIECZEŃSTWA CYFROWEGO W SZKOLE

Działania profilaktyczne ograniczają zakres zagrożeń, ale ich nie eliminują. W przypadku wystąpienia zagrożenia bezpieczeństwa cyfrowego dyrekcja szkoły powinna: szybko

zidentyfikować problem, określić szkodliwość zachowania lub niezgodność z prawem, poszukiwać rozwiązań adekwatnych do poziomu zagrożenia.

VI. Działania interwencyjne w przypadku wystąpienia zagrożenia bezpieczeństwa cyfrowego.

1. Działania wobec aktu / zdarzenia – opis przypadku, ustalenie okoliczności zdarzenia, zabezpieczenie dowodów oraz monitoring sytuacji szkolnej. Należy pamiętać o zachowaniu (nieusuwaniu) dokumentacji cyfrowej: wiadomości sms, e-maili, nagrań z poczty głosowej telefonu, komentarzy w serwisie społecznościowym, zapisów na blogu czy plików filmów wideo. Każde zdarzenie wymaga udokumentowania w stosownym protokole.
2. Działania wobec uczestników zdarzenia - oznaczają te aktywności, które podejmowane są wobec ofiar (osób poszkodowanych), sprawców i świadków zdarzenia. W przypadku gdy osobami poszkodowanymi są osoby nieletnie kolejną grupą pośrednich uczestników zdarzenia są rodzice.
3. Standardowa procedura reakcji na zagrożenie bezpieczeństwa cyfrowego powinna przebiegać wg schematu:
   3.1. Rozmowa uczestnika zdarzenia z dyrekcją szkoły.
   3.2. Powiadomienie rodziców poszkodowanego.
   3.3. Działania wychowawcze i wyciągnięcie konsekwencji wobec sprawcy.
   3.4. Powiadomienie policji / sądu rodzinnego w przypadku naruszenia prawa.
   3.5. Udzielenie uczestnikom wsparcia psychologicznego.
4. 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:
   4.1. policją i sądami rodzinnymi,
   4.2. służbami społecznymi i placówkami specjalistycznymi,
   4.3. dostawcami usług internetowych oraz operatorami telekomunikacyjnymi.
5. Sprawców wszystkich rodzajów zagrożeń bezpieczeństwa cyfrowego w szkole należy objąć poniższymi działaniami:
   5.1. Sprawca musi otrzymać komunikat o braku akceptacji dla działań jakich dokonał, poznać możliwe skutki i konsekwencje swojego postępowania (np. wynikające ze statutu). Powinien zostać wezwany do zaprzestania podejmowania podobnych działań w przyszłości oraz usunięcia skutków swoich dotychczasowych działań (np. publikacji na portalu społecznościowym). Sprawcę należy objąć pomocą psychologiczno-pedagogiczną, by podobne zdarzenia nie miały miejsca w przyszłości. W przypadku, kiedy sprawców jest więcej, należy z każdym z nich rozmawiać osobno.
   5.2. Decyzję o karze dla sprawcy, powinna podejmować rada pedagogiczna (po poznaniu wszystkich okoliczności zdarzenia), a przekazywać dyrektor szkoły.
6. Celem sankcji wobec sprawcy jest: zatrzymanie jego działań i zapewnienie poczucia bezpieczeństwa ofierze oraz zmiana postawy sprawcy. Sankcje mają na celu także

pokazanie społeczności szkolnej, że działania sprawcy nie będą tolerowane i że szkoła jest w stanie skutecznie zareagować w tego rodzaju sytuacjach.

7. Podejmując decyzję o zastosowaniu sankcji, należy wziąć pod uwagę:
   7.1. rozmiar i rangę szkody np. czy w przypadku cyberprzemocy 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.;
   7.2. czas trwania prześladowania – czy było to długotrwałe działanie, czy pojedynczy incydent;
   7.3. świadomość popełnianego czynu – czy działanie było zaplanowane, a sprawca był świadomy, że postąpił nagannie, czy wie, że wyrządził krzywdę koledze. Należy również zwrócić uwagę na to jak wiele wysiłku włożył w ukrycie swojej tożsamości itp.;
   7.4. motywacje sprawcy – należy sprawdzić, czy działanie sprawcy nie jest działaniem odwetowym w odpowiedzi na uprzednie doświadczenia sprawcy.
8. Rodzice muszą zostać powiadomieni o zdarzeniu oraz zapoznani z materiałami i decyzją co do dalszego postępowania ze sprawcą (np. z zastosowanymi sankcjami). Powinni oni również zostać poinformowani, iż rodzice ofiary mają prawo zgłosić sprawę policji.
9. Jeśli sprawcą czynu jest osoba spoza szkoły, należy zapewnić bezpieczeństwo ofierze i poinformować ją i jej rodziców o przysługujących jej prawach.

VII. PODSTAWOWE DZIAŁANIA W PRZYPADKU WYSTĄPIENIA INCYDENTU

A. DOSTĘP DO TREŚCI SZKODLIWYCH, NIEPOŻĄDANYCH I NIELEGALNYCH.

Podstawy prawne: Kodeks karny, art. 200 § 1–5 kk, art. 200a kk, art. 200b kk, art. 202 § 1-4b, art. 256 kk, art. 257.I.

Procedury postępowania w przypadku dostępu do treści szkodliwych, niepożądanych, nielegalnych (pornografia, treści obrazujące przemoc, propagowane działania szkodliwe dla zdrowia i życia, popularyzujące faszyzm, łamanie prawa, samobójstwa, samookaleczenia, narkotyki, werbowanie do organizacji nielegalnych i terrorystycznych):

1. Należy zabezpieczyć szkodliwe treści w formie dowodów elektronicznych z pomocą rodziców oraz w razie konieczności przedstawiciela szkoły, który posiada odpowiednie kompetencje techniczne.
2. Jeżeli dane treści można powiązać bezpośrednio z uczniami - rozwiązanie leży po stronie szkoły, a o danym zdarzeniu i roli uczniów powinni zostać poinformowani wszyscy rodzice. Jeżeli natomiast treści nielegalne lub szkodliwe nie mają związku z uczniami danej szkoły - należy rozważyć poinformowanie policji (numer alarmowy: 112, 997) oraz serwisu www.dyzurnet.pl
3. Jeżeli w udostępnianiu szkodliwych lub nielegalnych treści biorą udział inni rówieśnicy, konieczne jest poinformowanie wszystkich rodziców o danym zajściu. W przypadku upowszechnienia przez sprawcę treści nielegalnych (np. dziecięcej pornografii) trzeba zawiadomić policję.

4. Uczniów (ofiary i świadków) należy otoczyć opieką psychologiczno-pedagogiczną. Należy ustalić okoliczności uzyskania szkodliwych treści oraz zadbać o komfort psychiczny uczniów oraz poszanowanie ich poufności oraz podmiotowości (takie zdarzenie może mieć bardzo silny wpływ na ich psychikę). Należy uzgodnić z rodzicami formy działania oraz wsparcia uczniów oraz sposób w jaki doszło do incydentu (m.in. czy nie było to spowodowane udziałem w rekrutacji do danej sekty lub innej niebezpiecznej grupy, kontaktem z handlarzami narkotykami).
5. Jeżeli informacje o incydencie dotrą do środowiska ucznia (klasa, szkoła), należy podjąć działania edukacyjne i wychowawcze.
6. 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 niezwłocznie powiadomić policję.
7. Jeżeli zaistnieje potrzeba skorzystania przez ofiarę za specjalistycznej opieki psychologicznej, decyzja o jej udzieleniu powinna zostać podjęta w porozumieniu z jego rodzicami.

B. PRYWATNOŚCI DOTYCZĄCE NIEODPOWIEDNIEGO BĄDŹ NIEZGODNEGO Z PRAWEM WYKORZYSTYWANIA DANYCH OSOBOWYCH LUB WIZERUNKU UCZNIA I PRACOWNIKA SZKOŁY.

Podstawy prawne: Kodeks karny, art.190a, RODO

Zagrożenie prywatności to często przejęcie profilu na portalu społecznościowym w celu dyskredytacji lub naruszenia wizerunku ofiary, szantażowania, dokonania zakupów i innych transakcji finansowych. Podszywanie się pod inną osobę lub wykorzystywanie jej wizerunku czy danych jest PRZESTĘPSTWEM.

Sposób postępowania w przypadku wystąpienia zagrożenia:

1. W pierwszej kolejności należy zabezpieczyć dowody nieodpowiedniego działania (e-mail, zrzut ekranu, adres strony internetowej, SMS, konwersacja w komunikatorze) oraz dokonać zmian danych identyfikujących, które należą do ofiary (hasła, loginy, kody).
2. Jeżeli sprawcą naruszenia prywatności jest uczeń (kolega ofiary ze szkoły) - osoba pokrzywdzona / rodzice powinni zgłosić się do dyrektora szkoły, wychowawcy lub pedagoga. Jeżeli zebrane dowody jednoznacznie wskazują na to, iż sprawca dążył do wyrządzenia ofierze szkody majątkowej lub osobistej, należy je zabezpieczyć i przekazać policji (jeżeli trudno to ustalić, identyfikacji powinna dokonać policja).
3. W przypadku gdy sprawcą naruszenia prywatności jest osoba dorosła lub osoba trzecia, rodzice powinni skontaktować się bezpośrednio z policją i powiadomić szkołę.
4. Jeżeli sprawcą incydentu jest uczeń szkoły, należy skonsultować się z rodzicami i podjąć wobec niego działania wychowawcze, które uświadomią mu charakter jego nieodpowiedzialnych i nielegalnych czynów - powinno dojść do zadośćuczynienia osobie poszkodowanej. Działania te szkoła powinna podjąć niezależnie od powiadomienia policji lub sądu, gdyż celem nadrzędnym jest trwała zmiana postawy ucznia na prezentującą szacunek wobec cudzego wizerunku i prywatności.
5. Dyrekcja powinna podjąć decyzję w sprawie powiadomienia policji w oparciu o rodzaj czynu, wiek sprawcy, jego dotychczasowe zachowanie, postawę po odkryciu incydentu, opinie wychowawcy i pedagoga – dobrze byłoby uzyskać interpretację prawną radcy prawnego.
6. Nieletnia ofiara incydentu powinna być otoczona w porozumieniu z rodzicami opieką psychologiczno-pedagogiczną (jeśli jest taka potrzeba). Należy ją również powiadomić

o działaniach podjętych w celu usunięcia skutków działania sprawcy (usunięcie z Internetu nieodpowiednich treści, zablokowanie konta w serwisie społecznościowym...).
7. W sytuacji gdy o danym zajściu (kradzież tożsamości, naruszenie dobrego imienia) wiedzą tylko ofiara, jej rodzice i szkoła, dyrekcja szkoły powinna zapewnić poufność działań.
8. Jeżeli kradzież tożsamości bądź naruszenie dobrego imienia ofiary jest znane szerszemu gronu uczniów, należy podjąć wobec nich działania wychowawcze - zwracając uwagę na negatywną ocenę narażania na uszczerbek wizerunku ucznia oraz odpowiedzialność prawną.
9. W przypadku gdy naruszenie prywatności lub wyłudzenie czy kradzież tożsamości skutkują wyrządzeniem ofierze szkody majątkowej lub osobistej, rodzice ucznia powinni o tym fakcie powiadomić policję.
10. W razie konieczności ofiarę można skierować, za zgodą i we współpracy z rodzicami, do placówki specjalistycznej.

C. NADMIERNE KORZYSTANIE Z INTERNETU

Podstawy prawne:
Ustawa z dnia 14 grudnia 2016 r. Prawo oświatowe Dz.U.2020, poz.910, z późn. zm.
Infoholizm (siecioholizm) to nadmierne, obejmujące niekiedy niemal całą dobę, korzystanie z zasobów Internetu i gier komputerowych oraz portali społecznościowych przez dzieci. Jego negatywne efekty to: pogarszanie się stanu zdrowia fizycznego, psychicznego, zaniedbywanie codziennych czynności oraz osłabianie relacji rodzinnych i społecznych.

Sposób postępowania w przypadku wystąpienia zagrożenia:
1. W przypadku wystąpienia nadmiernego korzystania z komputera lub podejrzeń infoholizmu konieczne jest podjęcie działa pomocowych – skierowanie ucznia do placówki specjalistycznej za zgodą rodziców.
2. Szkoła wraz z rodzicami powinna ustalić skutki zdrowotne i psychiczne wywołane przez nadmierne korzystanie z zasobów Internetu (np. gorsze wyniki w nauce, niedosypianie, niedojada-nie...) ma to na celu wybór odpowiedniej ścieżki rozwiązania problemu.
3. Nauczyciele powinni zwrócić uwagę na uczniów nieangażujących się w życie klasy i poświęcające wolny czas na kontakt online lub przychodzącymi do szkoły po nieprzespanej nocy.
4. Osoba, która ma problem z infoholizmem powinna zostać otoczona zindywidualizowaną opieką pedagoga / psychologa szkolnego, który powinien przeprowadzić z nią (i rodzicami) wywiad w celu określenia sytuacji i wstępnego ustalenia poziomu zagrożenia, a następnie proponuje się kontakt ze specjalistą. Dziecku należy zapewnić komfort psychiczny a o jego sytuacji i specyfice uwarunkowań osobistych powinni wiedzieć wszyscy uczący i oceniający go nauczyciele. Należy również omówić wspólne rozwiązanie danej sytuacji z rodzicami ucznia.
5. W przypadku zdiagnozowania przez psychologa uzależnienia od Internetu, uczeń powinien zostać skierowany, w porozumieniu z rodzicami, na program terapeutyczny do placówki specjalistycznej.
6. Jeśli inni uczniowie są świadkami problemu, należy zwrócić ich uwagę na negatywne skutki nadmiernego korzystania z zasobów Internetu oraz zaapelować o wsparcie ucznia dotkniętego problemem.

DEZINFORMACJA, BEZKRYTYCZNA WIARA W TREŚCI ZAMIESZCZONE W INTENECIE, NIEUMIEJĘTNOŚĆ ODRÓŻNIENIA TREŚCI PRAWDZIWYCH OD NIEPRAWDZIWYCH,W TYM SZKODLIWOŚĆ REKLAM

Podstawy prawne:

USTAWA Z 14 GRUDNIA 2016 R. Prawo oświatowe DZ.U.2020, poz. 910, z późn. zm.

Cała społeczność szkolna powinna zostać wyposażona w wiedzę, która pozwoli na krytyczne podejście do informacji oraz radzenie sobie z dezinformacją. Brak umiejętności odróżniania prawdziwych informacji od nieprawdziwych publikowanych w Internecie, bezkrytyczne wierzenie we wpisy publikowane na forach internetowych, kierowanie się informacjami zawartymi w reklamach prowadzi do zagrożeń życia i zdrowia, skutkuje rozczarowaniami i porażkami życiowymi, utrudnia lub uniemożliwia osiągnięcie dobrych wyników w edukacji, a także utrwala u ucznia ambiwalentne postawy moralne.

Sposób postępowania w przypadku wystąpienia zagrożenia:

1. Nauczyciele wszystkich przedmiotów powinni identyfikować uczniów nieumiejących odróżniać prawdy od fałszu informacji publikowanych w Internecie. Często jest to możliwe w trakcie sprawdzania prac domowych, gdyż uczniowie tacy charakteryzują się używaniem nieprawdziwych informacji zaczerpniętych z sieci - takie sytuacje powinny być każdorazowo zauważone przez nauczyciela, przeanalizowane i skomentowane.
2. Jak działać wobec sprawców zdarzenia? Należy opublikować sprostowanie nieprawdziwych informacji i w miarę możliwości rozpowszechnić je Internecie.
3. Zadaniem szkoły jest prowadzenie działań profilaktycznych - edukacji multimedialnej (informacyjnej) także w trakcie zajęć nieinformatycznych przez wszystkie lata nauki ucznia w szkole lub na zajęciach pozalekcyjnych.
4. Program profilaktyczny szkoły powinien zaplanować działania mające na celu zapobieganie angażowania się ogółu młodzieży w zachowania autodestrukcyjne.

E. CYBERPRZEMOC

Podstawy prawne:
Kodeks karny: art.190 § 1–2, art. 190a § 1–3, art. 212 § 1–2, art. 256, art. 267 § 1–4, art. 268a.
Cyberprzemoc to seria agresywnych zachowań, celowo i regularnie skierowanych przeciwko bezbronnej osobie. Ma ona najczęściej formę słowną - pojawia się np. w komentarzach, na memach czy nagraniach wideo i przyjmuje takie formy jak: 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. Może też być bardziej zawoalowana: polegać na wykluczeniu z grupy, manipulowaniu czy nienawiązywaniu relacji. Potencjalni agresorzy są przekonani o anonimowości, ponieważ działają z ukrycia, mogą spreparować nienawistną treść „na spokojnie” oraz o dowolnej porze.

Telefony alarmowe:

1. Dziecięcy Telefon Zaufania, telefon rzecznika praw dziecka: 800 12 12 12
2. Telefon zaufania dla dzieci i młodzieży: 116 111, https://11611.pl/
3. Telefon dla rodziców i nauczycieli w sprawie bezpieczeństwa dzieci: 800 100 100, https://800100100.pl/
4. Zgłaszanie nielegalnych treści: dyzurnet.pl dyzurnet@dyzurnet.pl

Sposób postępowania w przypadku wystąpienia zagrożenia:

1. Z należytym spokojem należy wysłuchać osobę, która zgłasza akt cyberprzemocy i okazać jej wsparcie. Rozmowę powinno się przeprowadzić w miejscu bezpiecznym, zapewniającym intymność. Należy zebrać informację dotyczącą zdarzenia, czy faktycznie posiada ono znamiona cyberprzemocy czy może jest niezbyt udanym żartem.
2. Należy zabezpieczyć wszystkie dowody związane z aktem cyberprzemocy (np. zrobić kopię materiałów, zanotować datę i czas otrzymania materiałów, zapisać dane nadawcy, adresy stron www, historię połączeń itd.).
3. Na podstawie zebranych informacji i materiałów dowodowych należy w miarę możliwości zidentyfikować sprawcę. Ofiara często domyśla się kto stosuje wobec niej cyberprzemoc. Jeżeli ustalenie sprawcy nie jest możliwe, a w ocenie nauczycieli jest to konieczne, należy skontaktować się z policją. Należy pamiętać, że czyny karalne ścigane z urzędu powinny być niezwłocznie zgłoszone na policję lub do prokuratury. Dotyczy to sytuacji takich jak rozpowszechnianie zdjęć lub filmów z udziałem osoby nieletniej, mających cechy pornograficzne, czy publikowanie materiałów prezentujących seksualne wykorzystywanie nieletnich(art.202kk)
4. Działania wobec sprawców cyberprzemocy ze szkoły:
   4.1. pedagog przeprowadza rozmowę dyscyplinującą dotyczącą nagannego zachowania ucznia. Ma ona na celu ustalenie okoliczności zdarzenia, analizę zaistniałej sytuacji (powodów i motywów działania) oraz próbę naprawienia sytuacji konfliktowej,
   4.2. sprawcy cyberprzemocy powinna być wymierzona kara, którą przewidują wewnętrzne przepisy szkoły (statut, regulaminy).
5. Działania wobec sprawcy cyberprzemocy spoza szkoły — w sytuacji, gdy sprawca jest nieznany, podstawowe działanie polega na: przerwaniu aktu cyberprzemocy (zawiadomieniu administratora serwisu w celu usunięcia materiału po wcześniejszym zabezpieczeniu dowodów) oraz ewentualnym zgłoszeniu sprawy policji.
6. Działania wobec ofiar zdarzenia:
   6.1. udzielenie wsparcia ofierze — musi się ona czuć bezpieczna i otoczona opieką dorosłych,
   6.2. poinformowanie ucznia o krokach, jakie może podjąć szkoła i sposobach, w jaki może zapewnić mu bezpieczeństwo,
   6.3. omówienie strategii postępowania wobec sprawcy (np. zerwanie kontaktu ze sprawcą, niepodejmowanie agresywnej konfrontacji itp.),
   6.4. monitorowanie sytuacji, np. zwrócenie uwagi, czy nie są podejmowane wobec niej dalsze działania przemocowe, obserwowanie, jak sobie radzi w grupie po ujawnieniu incydentu cyberprzemocy,
   6.5. włączenie rodziców w działania wobec ofiary – trzeba na bieżąco ich informować o sytuacji, zaproponować pomoc specjalisty (np. psycholog szkolny, poradnia psychologiczno-pedagogiczna) oraz przekazać informację o możliwości zgłoszenia sprawy policji.

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

Podstawy prawne: Kodeks karny – art. 191a, art. 202 § 1–4c.
Seksting to przesyłanie wiadomości drogą elektroniczną w formie wiadomości MMS lub z wykorzystaniem różnych aplikacji i komunikatorów albo publikowanie np. na portalach społecznościowych prywatnych treści, głównie zdjęć lub filmów, o kontekście seksualnym, erotycznym.
Występują 3 rodzaje sekstingu:

1. Wymiana materiałów o charakterze seksualnym następuje tylko w ramach związku między dwojgiem rówieśników. Materiały nie uległy rozprzestrzenieniu dalej. Należy wezwać uczniów do dyrekcji szkoły, gdzie przedstawione im zostaną dowody ich aktywności. Konieczne jest również przeprowadzenie rozmów w obecności rodziców uczniów.
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. Należy powiadomić policję lub sąd rodzinny ze względu na pornograficzny charakter materiałów. Wszelkie działania wobec sprawców incydentu powinny być podejmowane w porozumieniu z ich rodzicami.
3. Materiały zostały rozesłane większej liczbie osób (bez względu na intencje) i na tym tle dochodzi do cyberprzemocy. Należy zastosować procedury dotyczące cyberprzemocy. Każdy z tych rodzajów sekstingu uruchamia zmodyfikowane procedury reagowania. Za każdym razem, niezależnie od zakresu negatywnych zachowań, należy udzielić uczniom wsparcia pedagogicznego i psychologicznego oraz współpracować z rodzicami uczniów.

G. BEZPRAWNE UŻYCIE WIZERUNKU

Podstawy prawne: Kodeks cywilny i Ustawa z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych, t.j. Dz.U. 2019, poz. 1231; 2020, poz. 288.
Użycie (upublicznianie zdjęć / filmów) wizerunku osoby fizycznej, czy stworzenie możliwości zapoznania się z wizerunkiem w Internecie bez wymaganej prawem zgody, może skutkować odpowiedzialnością cywilną i karną (szczególnie w sytuacjach, gdy osoba ukazywana jest w sposób prześmiewczy i poniżający).
Zgoda na upublicznienie wizerunku musi zostać wyrażona wprost, a osoba jej udzielająca musi być świadoma formy w jakiej jej wizerunek będzie przedstawiony (miejsce, czas publikacji, towarzyszący jej komentarz, zestawienie z innymi wizerunkami). Z art. 24 § 1 i 2 Kodeksu cywilnego wynika, że osoba, której dobro osobiste zostało zagrożone (np. poprzez bezprawne upublicznienie wizerunku), może żądać zaprzestania tego działania. Domagać się dopełnienia czynności potrzebnych do usunięcia jego skutków, może również żądać zadośćuczynienia pieniężnego lub zapłaty określonej sumy na wskazany cel społeczny.
Jeżeli wskutek naruszenia dóbr osobistych została wyrządzona szkoda majątkowa to zgodnie z zasadami określonymi w Kodeksie cywilnym można domagać się jej naprawienia. Te same uprawnienia przysługują osobie, której prawa zostały zagrożone cudzym działaniem zgodnie z zapisami zawartymi w Ustawie o prawie autorskim i prawach pokrewnych (zgodnie z art. 78 ust.1).

Sposób postępowania w przypadku wystąpienia zagrożenia:

1. W przypadku naruszenia dóbr osobistych, należy zebrać informacje o osobie zgłaszającej (trzeba sprawdzić czy wizerunek został naruszony bezprawnym działaniem),

okolicznościach oraz możliwych dowodach np. zrzut ekranowy dokumentujący użycie wizerunku.
2. Dochodzenie naruszeń dóbr osobistych jest działaniem podejmowanym przez osobę uprawnioną a w przypadku naruszeń będących przestępstwem, możliwe jest zaangażowanie organów ścigania. Szkoła może zaangażować się w spór w charakterze mediatora między stronami w przypadku, kiedy sprawca lub ofiara są jej uczniami.
3. Inne działania jakie dyrekcja szkoły powinna podejmować mają charakter prewencyjny. Poza realizacją zapisów podstawy programowej związanych z prawem autorskim, można w trakcie lekcji wychowawczych wprowadzić uczniów w tematykę świadomego i zgodnego z prawem użycia wizerunku w Internecie.

H. NAWIĄZYWANIE NIEBEZPIECZNYCH KONTAKTÓW W INTERNECIE — UWODZENIE, ZAGROŻENIE PEDOFILIĄ

Podstawy prawne: Kodeks karny, art. 200, art. 200a. § 1 i 2, art. 286 § 1.
Niebezpieczne kontakty w Internecie to m.in. kontakt osoby dorosłej z małoletnią w celu: wyłudzenia poufnych informacji lub własności (pieniądze, wartościowe przedmioty), nawiązania kontaktów seksualnych, szantażu, chęci kidnappingu lub skłonienia do zachowań niebezpiecznych dla zdrowia i życia.

Telefony alarmowe:
1. Dziecięcy Telefon Zaufania, telefon rzecznika praw dziecka: 800 12 12 12
2. Telefon zaufania dla dzieci i młodzieży: 116 111, https://11611.pl/
3. Telefon dla rodziców i nauczycieli w sprawie bezpieczeństwa dzieci: 800 100 100, https://800100100.pl/
4. Zgłaszanie nielegalnych treści: dyzurnet.pl dyzurnet@dyzurnet.pl

Sposób postępowania w przypadku wystąpienia zagrożenia:
1. Osobami najczęściej zgłaszającymi omawiany problem są rodzice, osoby ścigające pedofilów lub informacja uzyskiwana jest od rówieśników. W działaniach szkoły najważniejsze jest szybkie przeciwdziałanie zagrożeniu ze względu na szkodliwe konsekwencje realizacji kontaktu online, przeradzającego się w zachowania w świecie rzeczywistym gdyż istnieje duże prawdopodobieństwo zagrożenia życia lub zdrowia dziecka.
2. Należy zawiadomić policję o wystąpieniu zdarzenia, udzielić wszelkiego możliwego wsparcia organom ścigania, m.in. zabezpieczyć i przekazać zebrane dowody.
3. Nie należy podejmować aktywności zmierzających do kontaktu ze sprawcą. Zadaniem szkoły jest zebranie dowodów i opieka nad ofiarą i ewentualnymi świadkami.
4. Ofiarę należy objąć pomocą psychologiczno-pedagogiczną, zapewnić komfort psychiczny i poczucie bezpieczeństwa (do pomocy powinny być zaangażowane osoby do których ofiara ma zaufanie np. wychowawca, pedagog szkolny). Należy również upewnić się, że kontakt ofiary ze sprawcą został przerwany.
5. Trzeba zbadać sytuację domową ucznia i zastanowić się czy nie tkwi w niej źródło poszukiwania kontaktów w Internecie.
6. Jeżeli wśród uczniów są świadkowie zdarzenia to należy otoczyć ich opieką psychologiczno- pedagogiczną we współpracy z rodzicami.
7. W przypadku, kiedy doszło do naruszenia prawa (uwiedzenie dziecka do lat 15) szkoła ma obowiązek powiadomić policję lub sąd rodzinny. W odniesieniu do osoby ofiary rekomendowane jest skierowanie jej w porozumieniu z rodzicami na terapię do placówki specjalistycznej opieki psychologicznej.

I. ŁAMANIE PRAWA AUTORSKIEGO

Podstawy prawne: Ustawa o prawie autorskim i prawach pokrewnych, Kodeks karny, Kodeks cywilny
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. Informacja o incydencie może zostać zgłoszona w sposób formalny (pozew, pismo urzędowe) i nieformalny (ustnie, telefonicznie, pocztą elektroniczną). W przypadku nieformalne zgłoszenia należy sporządzić notatkę służbową.
2. Zanim zostaną podjęte działania wobec ofiary (przyznanie roszczeń, spełnienie żądań) i sprawcy należy ustalić wszystkie okoliczności sprawy a w razie potrzeby skonsultować ją z prawnikiem.
3. Najczęstszym przypadkiem, w którym szkoła może zetknąć się z problemem naruszenia praw autorskich jest użycie materiałów prawnie chronionych przez jej pracowników bądź uczniów na stronach internetowych szkoły poza zakresem dozwolonego użytku.
4. Jeżeli naruszenia praw autorskich dotyczą uczniów, szkoła nie może występować w roli sędziego - dochodzenie roszczeń jest rolą osób uprawnionych.
5. Zadaniem szkoły jest edukowanie i wychowywanie poprzez realizację podstawy programowej, organizowanie pogadanek na temat praw autorskich. Działania szkoły powinny polegać na wyjaśnianiu na czym polega naruszenie i jak do niego nie dopuścić.
6. Konieczna jest weryfikacja informacji na temat: osoby dokonującej zgłoszenia (czy przysługują jej prawa autorskie do danego utworu), wykorzystanego utworu (czy jest chroniony przez prawo autorskie i jaki jest zakres tej ochrony). Jeżeli osoba uprawniona powołuje się na toczące się postępowanie w sprawie, to informację tę należy zweryfikować np. poprzez kontakt z odpowiednimi służbami, najlepiej przez adwokata lub radcę prawnego.
7. Wobec sprawcy złamania prawa autorskiego szkoła powinna podjąć działania o charakterze edukacyjno - wychowawczym oraz wyjaśnić na czym polegało naruszenie i przekazać wiedzę jak do danych naruszeń nie dopuścić w przyszłości.
8. Dochodzenie naruszeń praw autorskich realizowane jest, co do zasady, z inicjatywy samego uprawnionego przed sądami. W przypadku naruszeń stanowiących przestępstwo, dodatkowo zaangażowane mogą być Policja i prokuratura. W przypadku, kiedy osobą, której prawa autorskie zostały naruszone jest uczeń, szkoła może występować w roli mediatora, aby ułatwić stronom zaangażowanym ugodowe zakończenie sporu.
9. Jeżeli istnieje taka możliwość należy podjąć współpracę z dostawcami Internetu bądź operatorami telekomunikacyjnymi w celu zablokowania dostępu do utworu zamieszczonego w Internecie z naruszeniem prawa.

III. POSTANOWIENIA KOŃCOWE

1. W przypadku nauczania zdalnego, sposoby postępowania w sytuacjach wystąpienia cyberzagrożeń nie ulegają zmianie z wyjątkiem metod porozumiewania się z uczestnikami konfliktu. Nauczyciele i specjaliści szkolni porozumiewają się z uczniami, rodzicami uczniów przy pomocy dziennika elektronicznego VULCAN lub platformy internetowej Microsoft 365.
2. Niniejsza procedura uchwalona jest przez Radę Pedagogiczną jako procedura wewnątrzszkolna, a jej modyfikacje mogą odbywać się na wniosek dyrektora, członków

lub komisji rady pedagogicznej, w wyniku obserwacji praktycznej realizacji jej postanowień albo zmian w statucie szkioły.

3. Niniejsza procedura może być w całości uchylona w drodze uchwały Rady Pedagogicznej, o ile wprowadzone zostaną w statucie szkoły, albo w dokumentach wyższej rangi zmiany skutkujące brakiem zasadności jej stosowania.
4. W przypadkach nierozstrzygniętych niniejszą procedurą, decyzję podejmuje dyrektor szkoły w oparciu o przepisy wyższego rzędu.