



Publiczna Szkoła Podstawowa im. Tadeusza Kościuszki
Mokrzyńska ul. Wiśłana 47, 32-800 Brzesko
tel./fax 14 68 68 444
e-mail: szkola.mokrzyńska@brzesko.pl
www.spmokrzyńska.pl

Załącznik nr 2 do Zarządzenia nr 42/2018/2019
Dyrektora Publicznej Szkoły Podstawowej w Mokrzychach z 23 maja 2019 r.

PROCEDURY REAGOWANIA W PRZYPADKU WYSTĄPIENIA W SZKOLE ZAGROŻEŃ BEZPIECZEŃSTWA CYFROWEGO

	strona
Podstawowe działania na rzecz bezpieczeństwa cyfrowego w szkole	1
Procedury na wypadek wystąpienia zagrożeń bezpieczeństwa cyfrowego	3
1. Dostęp do treści szkodliwych, niepożądanych, nielegalnych – procedura reagowania	3
2. Cyberprzemoc	4
3. Naruszenia prywatności dotyczące nieodpowiedniego lub niezgodnego z prawem wykorzystania danych osobowych lub wizerunku dziecka i pracownika szkoły	5
4. Zagrożenia dla zdrowia dzieci w związku z nadmiernym korzystaniem z Internetu	7
5. Nawiązywanie niebezpiecznych kontaktów w Internecie - uwodzenie, zagrożenie pedofilią	9
6. Seksting, prowokacyjne zachowania i aktywność seksualna jako źródło dochodu osób nieletnich	10
7. Bezkrytyczna wiara w treści zamieszczone w Internecie, nieumiejętność odróżnienia treści prawdziwych od nieprawdziwych, szkodliwość reklam	11
8. Łamanie prawa autorskiego	12
9. Zagrożenia bezpieczeństwa technicznego sieci, komputerów i zasobów online	14

Podstawowe działania na rzecz bezpieczeństwa cyfrowego w szkole.

W przypadkach wystąpienia incydentu naruszenia bezpieczeństwa, zwłaszcza wobec naruszenia prawa, działania szkoły cechuje otwartość i szybka identyfikacja problemu - określenie szkodliwych lub niezgodnych z prawem zachowań - i jego rozwiązywanie adekwatnie do poziomu zagrożenia, jakie wywołało w szkole.

Obligatoryjne działania interwencyjne, będące następstwem wystąpienia zagrożenia, zawsze podzielić można na 3 grupy:

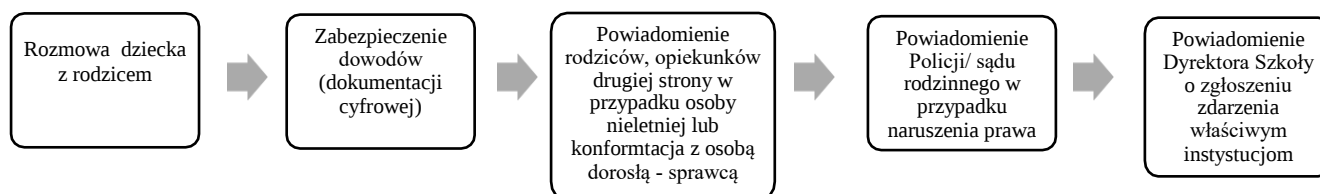
- 1) **działania wobec aktu/zdarzenia** – opis przypadku, ustalenie okoliczności zdarzenia, zabezpieczenie dowodów oraz monitoring point interwencyjny,
- 2) **działania wobec uczestników zdarzenia** (ofiara – sprawca – świadek, rodzice),
- 3) **działania wobec instytucji/organizacji/służb pomocowych i współpracujących** – Policji, wymiaru sprawiedliwości, służb społecznych.

Działania wobec zdarzenia polegają przede wszystkim na zachowaniu (nie usuwaniu) dokumentacji cyfrowej: wiadomości sms, e-maili, nagrań z poczty głosowej telefonu, komentarzy w serwisie społecznościowym, zapisów w blogu i plików filmów wideo. O ile to możliwe, należy także zarchiwizować treść rozmów w komunikatorach oraz linki (konkretne adresy URL) oraz danych o potencjalnym sprawcy. Każde zdarzenie wymaga udokumentowania w stosownym protokole.

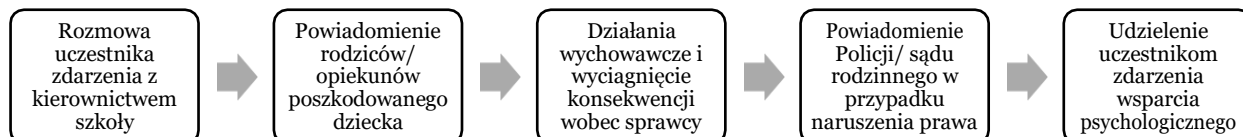
Przez **działania na rzecz uczestników zdarzenia** rozumie się aktywności podejmowane wobec **ofiar** (osób poszkodowanych), **sprawców** i **świadków zdarzenia**. W szkole osobami poszkodowanymi będą w większości przypadków dzieci (nieletni). Dlatego jako kolejną grupę pośrednich uczestników zdarzenia wyróżniamy ich rodziców.

Standardową procedurę reakcji w przypadku wystąpienia zagrożenia bezpieczeństwa cyfrowego prezentuje rysunek:

Sytuacja zaistniała w domu:



Sytuacja zaistniała w szkole:



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

- 1) Sprawca/-y otrzymuje/-ą od przedstawicieli szkoły komunikat o braku akceptacji dla działań, jakich dokonał/-li. W trakcie takiej rozmowy uczniowi przypomina się możliwe skutki jego postępowania, a także konsekwencje, wynikające ze statutu i regulaminu szkoły. Obowiązkiem sprawcy jest natychmiastowe usunięcie zamieszczonych treści również u osób, do których zostały rozpowszechnione.
- 2) Pedagog, wychawca ogranicza się do podjęcia interwencji. O karze decyduje Rada Pedagogiczna, a informacje o niej uczniowi oraz rodzicom/prawnym opiekunom przekazuje Dyrektor Szkoły.
- 3) Jeśli sprawca jest z innej szkoły, należy rozważyć nawiązanie współpracy między placówkami i wspólne rozwiązywanie kryzysowej sytuacji.

W każdym przypadku należy ze spokojem wysłuchać osoby zgłaszającej, ofiary i sprawcy i okazać im wsparcie z zachowaniem ich podmiotowości i poszanowaniem ich uczuć. Taką rozmowę należy przeprowadzić w miejscu bezpiecznym, zapewniającym intymność. Nie należy podejmować kroków, które mogłyby prowadzić do piętnowania, czy wzbudzić podejrzenia w środowisku.

Procedury na wypadek wystąpienia zagrożeń bezpieczeństwa cyfrowego.

1. Dostęp do treści szkodliwych, niepożądanych, nielegalnych – procedura reagowania

DOSTĘP DO TREŚCI SZKODLIWYCH, NIEPOŻĄDANYCH I NIELEGALNYCH	
Podstawy prawne uruchomienia procedury	Kodeks Karny, Statut szkoły, Regulamin 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: dyzurnet@dyzurnet.pl , tel. 801 615 005, Policja 997
SPOSÓB POSTĘPOWANIA W PRZYPADKU WYSTĄPIENIA ZAGROŻENIA	
Opis okoliczności, analiza, zabezpieczenie dowodów	Reakcja szkoły w przypadku pozyskania wiedzy o wystąpieniu zagrożenia będzie zależna od tego, czy: (1) treści te można bezpośrednio powiązać z uczniami danej szkoły, czy też (2) treści nielegalne lub szkodliwe nie mają związku z uczniami danej szkoły, lecz wymagają kontaktu szkoły z odpowiednimi służbami. Sposób postępowania: 1. Zabezpieczenie dowodów w formie elektronicznej lub wydruku. 2. W przypadku sytuacji (1) rozwiązanie leży po stronie szkoły, zaś (2) należy rozważyć zgłoszenie incydentu na Policję oraz zgłosić go do serwisu Dyżurnet (dyzurnet.pl).
Identyfikacja sprawcy(-ów)	Po zidentyfikowaniu sprawców poinformowanie wszystkich rodziców lub opiekunów dzieci uczestniczących w zdarzeniu o sytuacji i ich roli.
Działania wobec sprawców zdarzenia ze szkoły/ spoza szkoły	Przeprowadzenie rozmowy wychowawczo – profilaktycznej (wychowawca-pedagog-dyrektor). W przypadku upowszechniania przez sprawców treści nielegalnych (np. pornografii dziecięcej) złożenie zawiadomienia o zdarzeniu na Policję.
Aktywności wobec ofiar zdarzenia	Podczas rozmowy ustalenie okoliczności uzyskania przez ofiarę dostępu do w/w treści. Powiadomienie rodziców lub opiekunów prawnych o zdarzeniu i uzgodnienie z nimi podejmowanych działań i form wsparcia dziecka.
Aktywności wobec świadków	W przypadku, gdy informacja na temat zdarzenia dotrze do środowiska rówieśniczego ofiary – w klasie, czy szkole, wskazane jest podjęcie działań edukacyjnych i wychowawczych.

Współpraca z Policją i sądami rodzinnymi	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.
Współpraca ze służbami i placówkami specjalistycznymi	Szkoła może udzielić informacji na temat placówek świadczących pomoc, a decyzję o objęciu specjalistyczną opieką podejmują rodzice lub prawni opiekunowie.

1. Cyberprzemoc – procedura reagowania

CYBERPRZEMOC	
Podstawy prawne uruchomienia procedury	Kodeks Karny, Statut szkoły, Regulamin szkoły
Rodzaj zagrożenia objętego procedurą	Cyberprzemoc – przemoc z użyciem technologii informacyjnych i komunikacyjnych, głównie Internetu oraz telefonów komórkowych. Podstawowe formy zjawiska to nękanie, straszenie, szantazowanie z użyciem sieci, publikowanie lub rozsyłanie ośmieszających, kompromiujących informacji, zdjęć, filmów z użyciem sieci oraz podszywanie się w sieci pod kogoś wbrew jego woli. Do działań określanych mianem cyberprzemocy wykorzystywane są głównie: poczta elektroniczna, czaty, komunikatory, strony internetowe, blogi, serwisy społecznościowe, grupy dyskusyjne, serwisy SMS i MMS
Telefony alarmowe krajowe i lokalne	Telefon Zaufania dla Dzieci i Młodzieży - 116 111 Telefon dla Rodziców i Nauczycieli w sprawie Bezpieczeństwa Dzieci – 800 100 100 , dyzurnet@dyzurnet.pl
SPOSÓB POSTĘPOWANIA W PRZYPADKU WYSTĄPIENIA ZAGROŻENIA	
Przyjęcie zgłoszenia i ustalenie okoliczności zdarzenia	Przypadek cyberprzemocy może zostać ujawniony przez ofiarę, świadka (np. innego ucznia, nauczyciela, rodzica). W każdym przypadku należy wysłuchać osoby zgłaszającej i okazać jej wsparcie.
Opis okoliczności, analiza, zabezpieczenie dowodów	Należy zabezpieczyć dowody związane z aktem cyberprzemocy (np. zrobić kopię materiałów, zanotować datę i czas otrzymania materiałów, dane nadawcy, adresy stron www, historię połączeń, itp.). W trakcie zbierania materiałów należy zadbać o bezpieczeństwo osób zaangażowanych w problem.
Identyfikacja sprawcy(-ów)	Jeśli ustalenie sprawcy nie jest możliwe, a w ocenie kadry pedagogicznej jest to konieczne, należy skontaktować się z Policją. Bezwzględnie należy zgłosić rozpowszechnianie nagich zdjęć osób poniżej 18 roku życia (art. 202 par. 3 KK).
Aktywności wobec sprawców zdarzenia ze szkoły/ spoza szkoły	Gdy sprawca cyberprzemocy jest znany i jest on uczniem szkoły, cyberprzemoc podlega sankcjom określonym w wewnętrznych przepisach szkoły. Szkoła może tu stosować konsekwencje przewidziane dla sytuacji „tradycyjnej” przemocy.

Aktywności wobec ofiar zdarzenia	1. Udzielenie wsparcia ofierze. 2. Rozmowa z ofiarą cyberprzemocy wychowawcy, pedagoga, rodzica, dyrektora. 3. Zabezpieczenie dowodów. 4. Monitorowanie sytuacji ofiary. 5. Wskazanie rodzicom lub prawnym opiekunom źródeł specjalistycznej pomocy i przekazanie informacji o możliwości zgłoszenia sprawy Policji.
Aktywność wobec świadków	Należy zadbać o bezpieczeństwo świadków zdarzenia, jeśli byli oni osobami ujawniającymi cyberprzemoc.
Współpraca z Policją i sądami rodzinnymi	Samo wystąpienie zjawiska cyberprzemocy nie jest jednoznaczne z koniecznością zaangażowania Policji i sądu rodzinnego – procedura umożliwia rozwiązanie sytuacji problemowej na poziomie pracy wychowawczej szkoły. Szkoła powinna powiadomić odpowiednie służby (np. sąd rodzinny), gdy wykorzysta wszystkie dostępne jej środki wychowawcze (rozmowa z rodzicami, konsekwencje ze statutu i/lub regulaminu szkoły wobec ucznia) i interwencje pedagogiczne, a ich zastosowanie nie przynosi pożądanych rezultatów (np. nie ma zmian postawy ucznia). Kontakt z Policją wymagają wszelkie sytuacje, w których zostało naruszone prawo (np. groźby karalne, świadome publikowanie nielegalnych treści, rozpowszechnianie nagich zdjęć z udziałem małoletnich). Za zgłoszenie odpowiada dyrektor szkoły.
Współpraca z dostawcami Internetu i operatorami telekomunikacyjnymi	Kontakt z dostawcą usługi może być wskazany w celu usunięcia z sieci kompromitujących lub krzywdzących materiałów. Do podjęcia takiego działania deleguje administratora serwisu art. 14 Ustawy z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną.

3. Naruszenia prywatności dotyczące nieodpowiedniego lub niezgodnego z prawem wykorzystania danych osobowych lub wizerunku dziecka i pracownika szkoły - procedura reagowania

NARUSZENIA PRYWATNOŚCI DOTYCZĄCE NIEODPOWIEDNIEGO BĄDŹ NIEZGODNEGO Z PRAWEM WYKORZYSTANIA DANYCH OSOBOWYCH LUB WIZERUNKU DZIECKA I PRACOWNIKA SZKOŁY	
Podstawy prawne uruchomienia procedury	Kodeks Karny (art. 190a par. 2)

Rodzaj zagrożenia objętego procedurą	1. Naruszenie prywatności dziecka lub pracownika szkoły poprzez nieodpowiednie lub niezgodne z prawem wykorzystanie danych osobowych lub wizerunku dziecka i pracownika szkoły. 2. Podszywanie się pod inną osobę, wykorzystywanie jej wizerunku lub danych osobowych w celu wyrządzenia jej szkody osobistej lub majątkowej (wyłudzenia, kradzieże). 3. Przejęcie profilu na portalu społecznościowym w celu dyskredytacji lub naruszenia dobrego wizerunku ofiary (np. publikacja zdjęć intymnych bądź montowanych). 4. Szantaż (w celu uzyskania korzyści finansowych w zamian za niepublikowanie zdjęć bądź treści naruszających dobry wizerunek ofiary). 5. Dokonanie zakupów i innych transakcji finansowych (np. w sklepach internetowych na koszt ofiary) lub uzyskania korzyści (np. usługi premium SMS).
SPOSÓB POSTĘPOWANIA W PRZYPADKU WYSTĄPIENIA ZAGROŻENIA	
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 lub 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 i powiadomić o tym szkołę (zgodnie z Kodeksem Karnym ściganie następuje tu na wniosek pokrzywdzonego). Istotne dla ścigania sprawcy będzie uzyskanie dowodów, że sprawca zmierzał do wyrządzenia ofierze szkody majątkowej lub osobistej. Samo podszywanie się pod ofiarę nie jest karalne.
Opis okoliczności, analiza, zabezpieczenie dowodów	1. Zabezpieczenie dowodów nieodpowiedniego lub niezgodnego z prawem działania – w formie elektronicznej (e-mail, zrzut ekranu, konwersacja w komunikatorze lub sms) oraz dokonanie zmian tych danych identyfikujących, które zależą od ofiary, tj. haseł i loginów lub kodów dostępu do platform i portali internetowych, tak aby uniemożliwić kontynuację procederu naruszania prywatności. 2. Usunięcie skutków działań - likwidacja stron internetowych czy profili w portalach społecznościowych, które wymagać będą interwencji w zebrane dowody, musi odbywać się za zgodą Policji (o ile została powiadomiona).
Identyfikacja sprawcy (-ów)	W przypadku, gdy dowody jasno wskazują na konkretnego sprawcę, również gdy trudno go ustalić, sytuację należy przekazać Policji.

Aktywności wobec sprawców zdarzenia ze szkoły/ spoza szkoły	1. Uświadomienie sprawcy nieodpowiedniego i nielegalnego charakteru czynu, jakiego dokonał. 2. Podjęcie decyzji przez Dyrektora Szkoły o powiadomieniu o incydencie Policji, biorąc pod uwagę wiek sprawcy, jego dotychczasowe zachowanie, postawę po odkryciu incydentu oraz opinie wychowawcy i pedagoga. Przed podjęciem decyzji o zgłoszeniu incydentu na Policję należy rozważyć, czy istnieją dowody, iż uczeń – sprawca zmierzał do wyrządzenia ofierze szkody majątkowej lub osobistej. W takim przypadku dobrym rozwiązaniem jest uzyskanie interpretacji prawnej adwokata lub radcyprawnego.
Aktywności wobec ofiar zdarzenia	1. Otoczenie opieką ofiary incydentu w porozumieniu z rodzicami/prawnymi opiekunami. 2. Powiadomienie o interwencji w celu usunięcia skutków działania sprawcy (np. usunięcie z Internetu intymnych zdjęć ofiary, zablokowanie dostępu do konta w portalu społecznościowym). Jeśli kradzież tożsamości, bądź naruszenie dobrego wizerunku ofiary jest znane tylko jej i rodzicom, szkoła winna zapewnić poufność działań, tak aby informacje narażające ofiarę na naruszenie wizerunku nie były rozpowszechniane.
Aktywności wobec świadków	Gdy kradzież tożsamości, bądź naruszenie dobrego wizerunku ofiary jest znane szerszemu gronu uczniów szkoły, należy podjąć wobec nich działania wychowawcze, zwracające uwagę na negatywną ocenę naruszania wizerunku ucznia – koleżanki lub kolegi oraz ryzyko czynu zabronionego (przestępstwo, wykroczenie).
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.
Współpraca ze służbami placówkami specjalistycznymi	Szkoła może udzielić informacji na temat placówek świadczących pomoc, a decyzję o objęciu specjalistyczną opieką podejmują rodzice lub prawni opiekunowie.

4. Zagrożenia dla zdrowia dzieci w związku z nadmiernym korzystaniem z Internetu – procedura reagowania

ZAGROŻENIA DLA ZDROWIA DZIECI W ZWIĄZKU Z NADMIERNYM KORZYSTANIEM Z INTERNETU	
Podstawy prawne uruchomienia procedury	Ustawa z dnia 14 grudnia 2016 r. – Prawo oświatowe

Rodzaj zagrożenia objętego procedurą (opis)	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.
SPOSÓB POSTĘPOWANIA W PRZYPADKU WYSTĄPIENIA ZAGROŻENIA	
Przyjęcie zgłoszenia i ustalenie okoliczności zdarzenia	Szkoła po zaobserwowaniu niepokojących symptomów u ucznia – podejrzenie o infoholizm - przeprowadza rozmowę z rodzicami lub prawnymi opiekunami.
Opis okoliczności, analiza, zabezpieczenie dowodów	1. Przeprowadzenie rozmowy z rodzicami lub prawnymi opiekunami w celu ustalenia skutków zdrowotnych i psychicznych, jakie niesie nadmierne korzystanie z zasobów Internetu. 2. Szkoła może udzielić informacji na temat placówek świadczących pomoc, a decyzję o objęciu specjalistyczną opieką podejmują rodzice lub prawni opiekunowie.
Aktywności wobec ofiar zdarzenia	1. Rozmowa ucznia i rodziców lub prawnych opiekunów z pedagogiem szkolnym. 2. Omówienie możliwych rozwiązań ze wskazaniem konieczności specjalistycznej diagnozy dziecka w odpowiednich placówkach. 3. Poinformowanie Rady Pedagogicznej o istniejącym problemie w celu podjęcia wspólnych, spójnych działań. 4. W przypadku niepodjęcia przez rodziców lub prawnych opiekunów działań zmierzających do poprawy sytuacji dziecka szkoła przekazuje informacje do sądu rodzinnego.
Aktywności wobec świadków	Jeśli świadkami problemu są rówieśnicy dziecka, należy im w rozmowie zwrócić uwagę na negatywne aspekty nadmiernego korzystania z zasobów Internetu oraz zaapelować o codzienne wsparcie dla dziecka dotkniętego problemem, a także o informowanie wychowawcy w przypadku wystąpienia kolejnych przypadków u innych dzieci.
Współpraca ze służbami i placówkami specjalistycznymi	W przypadku zdiagnozowania przez psychologa zaawansowanego uzależnienia od korzystania z zasobów Internetu dziecko zostanie pod opieką tego specjalisty. Rodzic jest zobowiązany poinformować szkołę o podjętych krokach.

5. Nawiązywanie niebezpiecznych kontaktów w Internecie - uwodzenie, zagrożenie pedofilią – procedura reagowania

NAWIĄZYWANIE NIEBEZPIECZNYCH KONTAKTÓW W INTERNECIE - UWODZENIE, ZAGROŻENIE PEDOFILIĄ	
Podstawy prawne uruchomienia procedury	Kodeks Karny, art. 200, 200a par 1 i 2, art. 286 par.1
Rodzaj zagrożenia objętego procedurą (opis)	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 Telefon dla Rodziców i Nauczycieli w sprawie Bezpieczeństwa Dzieci – 800 100 100 Zgłaszanie nielegalnych treści: Dyżurnet, dyzurnet.pl
SPOSÓB POSTĘPOWANIA W PRZYPADKU WYSTĄPIENIA ZAGROŻENIA	
Przyjęcie zgłoszenia i ustalenie okoliczności zdarzenia	1. Osobami zgłaszającymi incydent mogą być: rodzice lub opiekunowie prawni dziecka, ofiara, środowisko rówieśnicze ofiary. 2. Określenie rodzaju incydentu: uwiedzenie i wykorzystanie seksualne, kidnaping, wyłudzenie pieniędzy czy przedmiotów dużej wartości. 3. Przeprowadzenie rozmowy z ofiarą w obecności rodziców lub prawnych opiekunów, pedagoga, wychowawcy i dyrektora.
Opis okoliczności, analiza, zabezpieczenie dowodów	Zidentyfikowanie i zabezpieczenie w formie elektronicznej lub wydruków dowodów działania dorosłego sprawcy uwiedzenia (zapisy rozmów w komunikatorach, na portalach społecznościowych; zrzuty ekranowe, zdjęcia, wiadomości e-mail). Jednocześnie bezzwłoczne zawiadomienie Policji o wystąpieniu zdarzenia.
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.
Aktywności 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.
Aktywności wobec ofiar zdarzenia	1. Zapewnienie wsparcia ofierze w przypadku zaobserwowania antyzdrowotnych i zagrażających życiu zachowań uczniów (samookaleczenia, zażywanie substancji psychoaktywnych), które mogą być skutkiem kontaktów w Internecie. 2. Powiadomienie rodziców lub prawnych opiekunów. 3. Uzyskanie informacji o sprawcy i przekazanie ich Policji.

	4. W razie konieczności, w porozumieniu z rodzicami lub prawnymi opiekunami należy podjąć decyzję o udzieleniu profesjonalnej opieki terapeutycznej i/lub lekarskiej.
Aktywności wobec świadków	Jeżeli zgłaszającym zagrożenie był rówieśnik ofiary, należy również objąć go opieką psychologiczną, pozytywnie wzmacniając jego reakcję na zdarzenie.
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.
Współpraca ze służbami społecznymi i placówkami specjalistycznymi	W przypadkach uwiedzenia nieletnich przez osoby dorosłe zaleca się – w porozumieniu z rodzicami lub opiekunami prawnymi – skierowanie ofiary na terapię do placówki specjalistycznej opieki psychologicznej.

6. Seksting, prowokacyjne zachowania i aktywność seksualna jako źródło dochodu osób nieletnich – procedura reagowania

SEKSTING, PROWOKACYJNE ZACHOWANIA I AKTYWNOŚĆ SEKSUALNA JAKO ŹRÓDŁO DOCHODU OSÓB NIELETNICH	
Podstawy prawne uruchomienia procedury	Kodeks Karny (art. 191a i 202)
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	
Przyjęcie zgłoszenia i ustalenie okoliczności zdarzenia	Zgłoszeń przypadków sekstingu dokonują: rodzice lub opiekunowie prawni dziecka – ofiary, sama ofiara, jak również rówieśnicy lub pracownicy szkoły.
Opis okoliczności, analiza, zabezpieczenie dowodów	Wyróżniamy 3 podstawowe rodzaje sekstingu, które skutkują koniecznością realizacji zmodyfikowanych procedur reagowania: 1. Wymiana materiałów o charakterze seksualnym następuje tylko w ramach związku między dwojgiem rówieśników. Materiały nie uległy rozprzestrzenieniu dalej. 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. 3. Materiały zostały rozesłane większej liczbie osób w celu upokorzenia osoby na nich zaprezentowanej – lub zostają rozpowszechnione omyłkowo, jednak są zastosowane jako narzędzie cyberprzemocy.

Identyfikacja sprawcy (-ów)	Identyfikacja sprawcy będzie możliwa przede wszystkim dzięki zabezpieczeniu dowodów – przesyłanych zdjęć, czy zrzutów ekranów portali, w których opublikowano zdjęcie(-a).
Aktywności wobec sprawców zdarzenia ze szkoły/spoza szkoły	Rozmowa Dyrektora Szkoły ze sprawcami sekstingu w obecności rodziców i pedagoga szkolnego. Rodzaj 1. Pouczenie sprawców zdarzenia, że dalsze rozpowszechnianie materiałów może być nielegalne i będzie miało ostrzejsze konsekwencje, w tym prawne. Rodzaj 2. Materiały uznane za pornograficzne, będą zgłaszane przez Dyrektora Szkoły na Policję (zgodnie z par. 2020 Kodeksu Karnego). Wszelkie działania wobec sprawców incydentu będą 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”.
Aktywności wobec ofiar zdarzenia	1. Rozmowa na temat identyfikacji potencjalnego sprawcy. 2. Otoczenie wszechstronną, dyskretną opieką psychologiczną – pedagogiczną ofiary oraz zaproponowanie odpowiednich działań wychowawczych.
Aktywności wobec świadków	Jeśli przypadek sekstingu zostanie upowszechniony w środowisku rówieśniczym należy podjąć działania wychowawcze, uświadamiające negatywne aspekty moralne sekstingu oraz narażanie się na dotkliwe kary.
Współpraca z Policją i sądami rodzinnymi	W przypadku publikacji lub upowszechniania zdjęć o charakterze pornografii dziecięcej (co jest wykroczeniem ściganym z urzędu) Dyrektor Szkoły jest zobowiązany do powiadomienia o tym zdarzeniu Policji lub sądu rodzinnego.
Współpraca ze służbami społecznymi i placówkami specjalistycznymi	Kontakt ofiar z placówkami specjalistycznymi może okazać się konieczny w indywidualnych przypadkach. Szkoła może udzielić informacji na temat placówek świadczących pomoc, a decyzję o objęciu specjalistyczną opieką podejmują rodzice lub prawni opiekunowie.

7. Bezkrytyczna wiara w treści zamieszczone w Internecie, nieumiejętność odróżnienia treści prawdziwych od nieprawdziwych, szkodliwość reklam – procedury reagowania

BEZKRYTYCZNA WIARA W TREŚCI ZAMIESZCZONE W INTERNECIE, NIEUMIEJĘTNOŚĆ ODRÓŻNIENIA TREŚCI PRAWDZIWYCH OD NIEPRAWDZIWYCH, SZKODLIWOŚĆ REKLAM	
Podstawy prawne uruchomienia procedury	Ustawa z 11 stycznia 2017 r. – Prawo oświatowe

Rodzaj zagrożenia objętego procedurą (opis)	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 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 temat „ściągi” i „bryków”), a także utrwalenia się u ucznia ambiwalentnych postaw moralnych.
SPOSÓB POSTĘPOWANIA W PRZYPADKU WYSTĄPIENIA ZAGROŻENIA	
Przyjęcie zgłoszenia i ustalenie okoliczności zdarzenia	Identyfikowanie przez nauczycieli i wychowawców uczniów, którzy nie potrafią odróżnić prawdy od fałszu w informacjach publikowanych w Internecie.
Opis okoliczności, analiza, zabezpieczenie dowodów	Posługiwanie się nieprawdziwymi informacjami zaczerpniętymi z Internetu, po zauważeniu przez nauczyciela, musi być przeanalizowane i sprostowane. Przypadki spektakularne powinny być archiwizowane przez nauczycieli i wykorzystywane podczas zajęć z wychowawcą poświęconych edukacji medialnej (informacyjnej).
Aktywności wobec sprawców zdarzenia ze szkoły/ spoza szkoły	Wystarczającą reakcją jest opublikowanie sprostowania nieprawdziwych informacji i – w miarę możliwości – rozpowszechnienie ich w Internecie, w portalach o zbliżonej tematyce.
Aktywności wobec ofiar zdarzenia i świadków	Szkoła prowadzi działania profilaktyczne ukierunkowane na zdobywanie przez dzieci i młodzież kompetencji medialnych.

8. Łamanie prawa autorskiego – procedura reagowania

ŁAMANIE PRAWA AUTORSKIEGO	
Podstawy prawne uruchomienia procedury	Kodeks Karny
Rodzaj zagrożenia objętego procedurą (opis)	Ryzyko poniesienia odpowiedzialności cywilnej lub karnej z tytułu naruszenia prawa autorskiego albo negatywnych skutków pochopnego spełnienia nieuzasadnionych roszczeń (tzw. <i>copyright trolling</i>)
SPOSÓB POSTĘPOWANIA W PRZYPADKU WYSTĄPIENIA ZAGROŻENIA	

Przyjęcie zgłoszenia i ustalenie okoliczności zdarzenia	1. Szkoła w sytuacji naruszenia praw autorskich powinna zasięgnąć fachowej pomocy prawnej. 2. Szkoła skupia się na swojej roli edukacyjno – wychowawczej poprzez organizację lekcji na temat praw autorskich, zwracając przy tym uwagę, że powinny one rzeczowo i konkretnie informować, jakie czyny są dozwolone, a jakie zabronione prawem.
Opis okoliczności, analiza, zabezpieczenie dowodów	1. Sprawdzenie czy okoliczności podane w zgłoszeniu faktycznie miały miejsce i czy powoływane tam dowody nie zostały zmanipulowane. 2. Przekazanie sprawy odpowiednim służbom.
Identyfikacja sprawcy(-ów)	Szkoła nie może wkraczać w kompetencje uprawnionych organów. Skupia się na swojej roli wychowawczej i edukacyjnej, wykorzystując otrzymanie zgłoszenia rzekomego naruszenia do przekazania zaangażowanym osobom (a być może i wszystkim uczniom, nauczycielom i opiekunom) wiedzy na temat tego, jak faktycznie prawo reguluje tę konkretną sytuację.
Aktywności wobec sprawców zdarzenia ze szkoły/ spoza szkoły	Zasadniczo 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.
Aktywności wobec ofiar zdarzenia	1. Jeżeli osobą, której prawa autorskie naruszono, jest uczeń, należy rozważyć pomoc szkoły w kompromisowym zakończeniu powstałego sporu. 2. W przypadku, gdy ofiarą jest osoba spoza szkoły, szkoła może pomóc sprawcy w doprowadzeniu do zaniechania naruszeń i naprawienia ich skutków bez niepotrzebnej eskalacji sporu.
Aktywności wobec świadków	Stosownie do okoliczności, należy samodzielnie zebrać ich zeznania lub skierować sprawę do odpowiednich organów.
Współpraca z Policją i sądami rodzinnymi	Dochodzenie roszczeń z tytułu naruszeń zależy od decyzji uprawnionego, to on ustala, czy zawiadamiać Policję lub składać powództwo. Szkoła może zaangażować się w ułatwianie zakończenia sporu bez takiej eskalacji.
Współpraca ze służbami społecznymi i placówkami specjalistycznymi	Organizowanie szkoleń lub warsztatów z zakresu prawa autorskiego w internecie dla wszystkich zainteresowanych osób w szkole.
Współpraca z dostawcami Internetu i operatorami telekomunikacyjnymi	Zależnie od okoliczności, może być wskazana asysta sprawcy bądź ofiary przy kontakcie z tego typu podmiotami, np. w celu zablokowania dostępu do utworu umieszczonego w Internecie z naruszeniem prawa. Ponadto, stosownie do przepisów prawa, tego typu usługodawcy mogą zostać zobowiązani do przekazania szczegółów dotyczących naruszenia dokonanego z użyciem ich usług (do czego jednak może być potrzebne postanowienie sądowe).

9. Zagrożenia bezpieczeństwa technicznego sieci, komputerów i zasobów online
– procedura reagowania

ZAGROŻENIA BEZPIECZEŃSTWA TECHNICZNEGO SIECI, KOMPUTERÓW I ZASOBÓW ONLINE	
Podstawy prawne uruchomienia procedury	Ustawa z dnia 14 grudnia 2016 r. – Prawo oświatowe Statut szkoły, Regulamin szkoły
Rodzaj zagrożenia objętego procedurą (opis)	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 bez opieki, czy brak zabezpieczeń na wypadek braku energii elektrycznej.
SPOSÓB POSTĘPOWANIA W PRZYPADKU WYSTĄPIENIA ZAGROŻENIA	
Przyjęcie zgłoszenia i ustalenie okoliczności zdarzenia	W przypadku wystąpienia incydentów zagrożenia bezpieczeństwa cyfrowego pracownik szkoły zobowiązany jest do zgłoszenia go Dyrektorowi Szkoły.
Opis okoliczności, analiza, zabezpieczenie dowodów	Szczegółowy opis procedur reagowania na wystąpienie w szkole różnorodnych zagrożeń bezpieczeństwa cyfrowego zawiera „Polityka ochrony danych osobowych” obowiązująca w szkole. Jeżeli szkoła nie poradzi sobie we własnym zakresie, konieczne będzie skorzystanie z zewnętrznego wsparcia wyspecjalizowanych firm.
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.
Aktywności wobec sprawców zdarzenia ze szkoły/ spoza szkoły	Jeśli sprawcami incydentu są uczniowie danej szkoły, o zaistniałej sytuacji należy powiadomić ich rodziców lub prawnych opiekunów, zaś wobec nich podjąć działania wychowawcze. Jeżeli skutki ataku mają dotkliwy charakter, doprowadziły do zniszczenia mienia lub utraty istotnych danych (np. gromadzonych w e-dzienniku szkoły), należy taki przypadek zgłosić na Policję.
Aktywności wobec świadków	O incydencie należy powiadomić społeczność szkolną (uczniów, nauczycieli, rodziców) i zaprezentować podjęte sprawnie działania, tak przywracające działanie aplikacji i sieci komputerowej w szkole, jak i wychowawczo – edukacyjne wobec dzieci.
Współpraca z Policją i sądami rodzinnymi	W przypadku wystąpienia strat materialnych oraz utraty danych (szczególnie danych wrażliwych) należy zgłosić incydent na Policję.

Współpraca ze służbami społecznymi i placówkami specjalistycznymi	W przypadkach zaawansowanych awarii (np. wywołanych przez trojany) lub strat (np. utrata danych z e-dziennika) konieczne jest skorzystanie z zewnętrznego wsparcia eksperckiego, kontakt z serwisem twórcy oprogramowania lub zamówienie usługi w wyspecjalizowanej firmie.
--	---

Tam można zwrócić się o pomoc:

- Telefon Zaufania dla Dzieci i Młodzieży - **116 111**
- Telefon dla Rodziców i Nauczycieli w sprawie Bezpieczeństwa Dzieci – **800 100 100**,

Zgłosić nielegalne treści:

- dyzurnet@dyzurnet.pl,
- tel. 801 615 005
- Policja 997