

**PROCEDURY REAGOWANIA
W PRZYPADKU WYSTĄPIENIA ZAGROŻEŃ
BEZPIECZEŃSTWA CYFROWEGO
W SZKOLE PODSTAWOWEJ
IM. Ks. MARIANA WIEWIÓROWSKIEGO
W GOMULINIE**

Podstawa prawna:

Ustawa z dnia 14 grudnia 2016r. Prawo oświatowe (Dz. U. z 2020 r. poz. 910 i 1378 oraz z 2021 r. poz.4)

Ustawa z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (Dz. U. 2020 r. poz. 344)

Ustawa z dnia 4 lutego 1994 r. o prawach autorskich i prawach pokrewnych (Dz. U. z 2019 r. poz. 1231, z 2020 r. poz. 288)

Ustawa z dnia 6 czerwca 1997 r. Kodeks karny (Dz. U. z 2020 r. poz. 1444, 1517)

PODSTAWOWE DZIAŁANIA NA RZECZ BEZPIECZEŃSTWA CYFROWEGO W SZKOLE

Rozwojowi sieci towarzyszy pojawienie się w Internecie niebezpiecznych zjawisk i przestępczości. Możemy mówić zarówno o przenoszeniu się negatywnych zjawisk ze świata realnego do sieci jak i o tworzeniu się całkiem nowych kategorii zjawisk niekorzystnych i przestępstw. Lista zagrożeń rozszerza się, co związane jest zarówno z coraz większym zasięgiem i jakością sieci, ale także z postrzeganiem Internetu jako miejsca w którym można pozostać anonimowym, a co za tym idzie bezkarnym, nawet działając w złej wierze lub niezgodnie z prawem. Nie istnieje „złota recepta”, którą zastosować można we wszystkich przypadkach wystąpienia zagrożeń spowodowanych przez uczniów. Szkoła uwzględnia kontekst indywidualnych przypadków, a także ich szkolne i środowiskowe tło oraz reaguje adekwatnie do poziomu odpowiedzialności i winy ucznia.

W związku z szerzeniem się negatywnych zjawisk online, dokonano ich podziału na dwie podstawowe grupy:

- zagrożenia o charakterze społeczno-wychowawczym
- zagrożenia technologiczne.

ZAGROŻENIA O CHARAKTERZE SPOŁECZNO – WYCHOWAWCZYM:

- **szkodliwe i nielegalne treści** – prezentujące przemoc, obrażenia fizyczne, śmierć (ofiary wypadków, okrucieństwo wobec ludzi i zwierząt), nawołujące do autodestrukcji (samookaleczeń, samobójstw, zażywania szkodliwych substancji itp.), zachęcające do nietolerancji, wrogości czy nienawiści, pornografia dziecięca;
- **niebezpieczne kontakty, uwodzenie w internecie (child grooming);**
- **seksting, prowokacyjne zachowania i aktywność seksualna** jako źródło dochodu osób nieletnich;
- **ryzykowne zachowania**, w tym podejmowanie wyzwań online;
- **agresja elektroniczna** – różnego rodzaju działania agresywne realizowane za pomocą współczesnych technologii komunikacyjnych mające na celu dyskredytowanie jednej czy wielu osób (szczególną formą agresji elektronicznej jest cyberprzemoc rówieśnicza);
- **nadużywanie internetu** – rozumiane jako nadmierne i/lub dysfunkcyjne używanie internetu związane z czasem, jak i intensywnością korzystania z sieci oraz potrzebą korzystania z sieci z jednoczesną utratą kontroli nad planowanym czasem aktywności online. Wiąże się to często z zaniedbywaniem innych aspektów życia.

ZAGROŻENIA TECHNOLOGICZNE W CYBERPRZESTRZENI, TAKIE JAK:

- **szkodliwe oprogramowanie (malware)** takie jak: wirusy, konie trojańskie, ransomware itp.,
- **zagrożenie poprzez surfowanie (drive by download)** - ściąganie szkodliwego oprogramowania poprzez kontakt z zarażonymi serwisami WWW,
- **BOTnety**, czyli sieci atakujących komputerów, przejętych przez cyberprzestępców,
- **ataki typu blokowanie usług (DoS),**
- **ataki socjotechniczne (phishing),**
- **włamania na strony internetowe lub do wewnętrznych systemów komputerowych.**

W przypadkach wystąpienia incydentu naruszenia bezpieczeństwa, zwłaszcza wobec naruszenia prawa, działania szkoły cechuje otwartość w działaniu, szybka identyfikacja problemu i jego rozwiązywanie adekwatnie do poziomu zagrożenia, jakie wywołało w szkole.

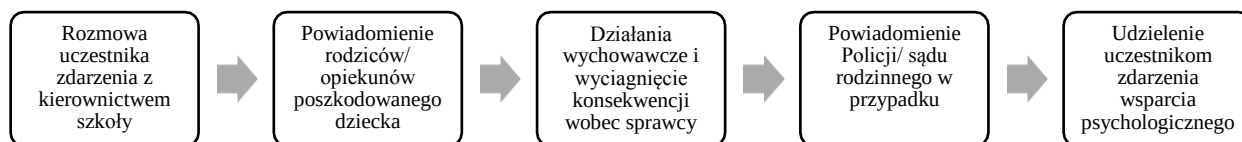
1. Obligatoryjne działania interwencyjne, będące następstwem wystąpienia zagrożenia, zawsze podzielić można na 3 grupy:

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

2. 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.

3. Przez działania na rzecz uczestników zdarzenia rozumie się aktywności podejmowane wobec **ofiar** (osób poszkodowanych), **sprawców** i **świadków zdarzenia**.

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



5. Działania szkoły adresowane do instytucji i organizacji zewnętrznych są niezbędne w przypadku naruszenia przepisów prawa przez uczniów lub osoby spoza szkoły. Pośród nich należy wyróżnić szczególnie współpracę z: Policją i sądami rodzinnymi, służbami społecznymi i placówkami specjalistycznymi oraz dostawcami usług internetowych oraz operatorami telekomunikacyjnymi.

6. Modele współpracy ze służbami społecznymi wobec e-problemów

Współpraca lokalnych instytucji i organizacji ma wiele wymiarów, może obejmować różne formy:

- **informacyjną**, która polega na przekazywaniu wiadomości o programach, rozwiązaniach itp.,
- **organizacyjną**, która polega w szczególności na: tworzeniu lub współtworzeniu i aktywnym udziale w pracach wspólnych zespołów o charakterze inicjatywnym i doradczym;
- **szkoleniową**, która polega na szkoleniu rodziców, ale także na doskonaleniu warsztatu pracy pedagoga, nauczyciela informatyki, wychowawców i nauczycieli.

7. **Działania, instytucji** wielu poziomów, zwłaszcza lokalnych we współpracy z rodzicami, mogą dotyczyć różnych zagadnień (obszarów działania), przyjmować mniej lub bardziej sformalizowany charakter.

Najważniejsze obszary działania służb społecznych w obliczu e-problemów:



8. Zespół do spraw bezpieczeństwa online w szkole tworzą nauczyciel informatyki i pedagog szkolny.

Zadania zespołu:

Zadania zespołu koncentrują się nie tylko na ustaleniu okoliczności zdarzenia, przerwaniu aktu oraz dokumentacji zdarzenia, ale przede wszystkim na udzieleniu wsparcia ofierze oraz wyciągnięciu konsekwencji wobec sprawcy przemocy. Zadania i procedury tej grupy muszą być znane wszystkim członkom społeczności szkolnej. Ustalenia zespołu oraz planowane przez niego podjęcie kolejnych działań przebiega w ścisłej współpracy z rodzicami osoby małoletniej zaangażowanej w zdarzenie. Obowiązkiem jest sporządzenie dokumentacji z zebranego i analizowanego materiału: opis przebiegu zdarzenia, osoby uczestniczące, zabezpieczone dowody, zastosowane środki wychowawcze i dyscyplinarne, notatki służbowe członków zespołu z rozmów ze sprawcą, poszkodowanym, ich rodzicami oraz świadkami zdarzenia. Zawierają informację o miejscu rozmowy, personalia osób biorących w niej udział oraz opis ustalonego przebiegu wydarzeń. Dokumentacja prowadzona jest z poszanowaniem prywatności osób uczestniczących w zdarzeniu wraz z zapewnieniem niezbędnej poufności przechowywanych i przetwarzanych danych.

Wyróżniono dziewięć podstawowych zagrożeń bezpieczeństwa cyfrowego w środowisku szkolnym:

- I. Dostęp do treści szkodliwych, niepożądanych i nielegalnych.
- II. Cyberprzemoc.
- III. Naruszenia prywatności dotyczące nieodpowiedniego bądź niezgodnego z prawem wykorzystania danych osobowych lub wizerunku dziecka i pracownika szkoły.
- IV. Zagrożenia dla zdrowia dzieci w związku z nadmiernym korzystaniem z Internetu.
- V. Nawiązywanie niebezpiecznych kontaktów w Internecie - uwodzenie, zagrożenie pedofilią, child grooming.
- VI. Seksting, prowokacyjne zachowania i aktywność seksualna jako źródło dochodu osób nieletnich.
- VII. Bezkrytyczna wiara w treści zamieszczone w Internecie, nieumiejętność odróżnienia treści prawdziwych od nieprawdziwych, szkodliwość reklam.
- VIII. Łamanie prawa autorskiego.
- IX. Zagrożenia bezpieczeństwa technicznego sieci, komputerów i zasobów online.

I. DOSTĘP DO TREŚCI SZKODLIWYCH, NIEPOŻĄDANYCH I NIELEGALNYCH

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 samookaleceń 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. 1. Zabezpieczyć dowody w formie elektronicznej (pliki z treściami niedozwolonymi, zapisy rozmów w komunikatorach, e-maile, zrzuty ekranu), znalezione w Internecie lub w komputerze dziecka. 2. Zabezpieczenie dowodów jest zadaniem rodziców dziecka, w czynnościach tych może wspomagać ich nauczyciel informatyki. 3. W przypadku sytuacji (1) rozwiązanie leży po stronie szkoły, zaś (2) należy rozważyć zgłoszenie incydentu na Policję oraz zgłosić go do serwisu dyzurnet.pl.
Identyfikacja sprawcy (-ów)	W identyfikacji sprawców kluczowe znaczenie odgrywać będą zgromadzone dowody. W procesie udostępniania nielegalnych i szkodliwych treści małoletnim występują na ogół: twórca treści oraz osoby, które udostępniły je dziecku. Konieczne jest poinformowanie wszystkich rodziców uczestniczących w zdarzeniu o sytuacji i roli ich dzieci.
Działania wobec sprawców zdarzenia ze szkoły/ spoza szkoły	1. W przypadku udostępniania treści wyżej opisanych przeprowadza się z nim rozmowę na temat jego postępowania i w jej trakcie uzmysłwić mu szkodliwość prowadzonych przez niego działań. 2. Działania szkoły koncentrują się na aktywnościach wychowawczych. 3. W przypadku upowszechniania przez sprawców treści nielegalnych należy złożyć zawiadomienie o zdarzeniu na Policję.
Aktywności wobec ofiar zdarzenia	1. Dzieci - ofiary i świadków zdarzenia – należy od pierwszego etapu interwencji - otoczyć opieką psychologiczno-pedagogiczną. Rozmowa z dzieckiem odbywa się w warunkach jego komfortu psychicznego, z poszanowaniem poufności i podmiotowości ucznia ze względu na fakt, iż kontakt z treściami nielegalnymi może mieć bardzo szkodliwy wpływ na jego psychikę. W jej trakcie ustala się okoliczności uzyskania przez ofiarę dostępu do ww. treści. 2. Należy koniecznie powiadomić ich rodziców o zdarzeniu i uzgodnić z nimi podejmowane działania i formy wsparcia dziecka. Działania szkoły w takich przypadkach cechuje poufność i empatia w kontaktach z wszystkimi uczestnikami zdarzenia oraz udzielającymi wsparcia.

Aktywności wobec świadków	W przypadku, gdy informacja na temat zdarzenia dotrze do środowiska rówieśniczego ofiary, podejmuje się działania edukacyjne i wychowawcze.
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	Kontakt z treściami szkodliwymi lub niebezpiecznymi może wywołać potrzebę skorzystania przez ofiarę ze specjalistycznej opieki psychologicznej. Decyzja o takim kontakcie i skierowaniu na terapię musi zostać podjęta w porozumieniu z rodzicami dziecka.

II. CYBERPRZEMOC

Rodzaj zagrożenia objętego procedurą	Cyberprzemoc – przemoc z użyciem technologii informacyjnych i komunikacyjnych, głównie Internetu oraz telefonów komórkowych. Podstawowe formy zjawiska to nękanie, straszenie, szantażowanie z użyciem sieci, publikowanie lub rozsyłanie ośmieszających, kompromitujących informacji, zdjęć, filmów z użyciem sieci oraz podszywanie się w sieci pod kogoś wbrew jego woli. Do działań określanych mianem cyberprzemocy wykorzystywane są głównie: poczta elektroniczna, czaty, komunikatory, strony internetowe, blogi, serwisy społecznościowe, grupy dyskusyjne, serwisy SMS i MMS
Telefony alarmowe	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	1. Przypadek cyberprzemocy może zostać ujawniony przez ofiarę, świadka. W każdym przypadku należy ze spokojem wysłuchać osoby zgłaszającej i okazać jej wsparcie. 2. Rozmowę należy przeprowadzić w miejscu bezpiecznym, zapewniającym ofierze/osobie zgłaszającej intymność. 3. W każdej sytuacji w trakcie ustalania okoliczności trzeba ustalić charakter zdarzenia (rozmiar i rangę szkody, jednorazowość /powtarzalność). 4. Trzeba dokonać oceny, czy zdarzenie wyczerpuje znamiona cyberprzemocy, czy jest np. niezbyt udanym żartem (wtedy trzeba podjąć działania profilaktyczne mające na celu nie dopuszczenie do eskalacji tego typu zachowań w stronę cyberprzemocy). 5. Realizując procedurę należy unikać działań, które mogłyby wtórnie stygmatyzować ofiarę lub sprawcę, np.: wywoływanie uczniów z lekcji, konfrontowanie ofiary i sprawcy, niewspółmierna kara.
Opis okoliczności, analiza, zabezpieczenie dowodów	Należy zabezpieczyć wszystkie dowody związane z aktem cyberprzemocy (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)	Identyfikacja sprawcy(ów) często jest możliwa dzięki zebranych materiałom – wynikom rozmów z osobą zgłaszającą, z ofiarą i analizie zabezpieczonych danych. 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	1. Gdy sprawca cyberprzemocy jest znany i jest on uczniem szkoły, pedagog szkolny przeprowadza z nim rozmowę o jego zachowaniu. Rozmowa taka ma służyć ustaleniu okoliczności zdarzenia, jego wspólnej analizie, a także próbie rozwiązania sytuacji konfliktowej.
Aktywności wobec ofiar zdarzenia	1. Należy udzielić wsparcia ofierze. Musi się ona czuć bezpieczna i zaopiekowana przez dorosłych. 2. Podczas rozmowy z uczniem należy okazać mu zrozumienie, podkreślić, że dobrze zrobił ujawniając sytuację i zapewnić go o pomocy ze strony szkoły. 3. Trzeba podkreślić, że placówka nie toleruje przemocy i że zostaną podjęte odpowiednie procedury interwencyjne. 4. Należy pomóc ofierze (rodzicom ofiary) w zabezpieczeniu dowodów i zadbanie o podstawowe zasady bezpieczeństwa online. 5. Należy monitorować sytuację ucznia, zwracać uwagę czy nie są podejmowane wobec niej dalsze działania przemocowe i obserwować, jak sobie radzi w grupie po ujawnionym incydencie cyberprzemocy. 6. W działania wobec ofiary należy także włączyć rodziców ofiary, informować ich na bieżąco o sytuacji dziecka. 7. W trakcie rozmowy z dzieckiem i jego rodzicami można zaproponować pomoc specjalisty (poradnia psychologiczno-pedagogiczna) oraz przekazać informację o możliwości zgłoszenia sprawy Policji.
Aktywności wobec świadków	Należy zadbać o bezpieczeństwo świadków zdarzenia, zwłaszcza, jeśli byli osobami ujawniającymi cyberprzemoc. W trakcie rozmowy ze świadkami należy okazać zrozumienie i empatię dla ich uczuć – obawy przed przypięciem łatki „donosiciela”, strachu przed staniem się kolejną ofiarą sprawcy itp.
Współpraca z Policją i sądami rodzinnymi	1. Samo wystąpienie zjawiska cyberprzemocy nie jest jednoznaczne z koniecznością zaangażowania Policji i sądu rodzinnego. 2. Kontakt z Policją wymagają wszelkie sytuacje, w których zostało naruszone prawo (np. groźby karalne, świadome publikowanie nielegalnych treści, rozpowszechnianie nagich zdjęć z udziałem małoletnich). 3. Szkoła powinna powiadomić odpowiednie służby (np. sąd rodzinny), gdy wykorzysta wszystkie dostępne jej środki wychowawcze (rozmowa z rodzicami, konsekwencje z statutu wobec ucznia) i interwencje pedagogiczne, a ich zastosowanie nie przynosi pożądanych rezultatów). 4. Za zgłoszenie powinien odpowiadać dyrektor szkoły.
Współpraca z dostawcami Internetu i teleoperatorami	Kontakt z dostawcą usługi może być wskazany w celu usunięcia z sieci kompromitujących lub krzywdzących materiałów. Do podjęcia takiego działania stymuluje administrator serwisu art. 14 Ustawy z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną.

III. 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 § 2)
Rodzaj zagrożenia objętego procedurą	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. Podsywanie 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, szantażu, dokonania zakupów i innych transakcji finansowych lub uzyskania korzyści. Często naruszenia prywatności łączy się z cyberprzemocą.
SPOSÓB POSTĘPOWANIA W PRZYPADKU WYSTĄPIENIA ZAGROŻENIA	
Przyjęcie zgłoszenia i ustalenie okoliczności zdarzenia	1. Gdy sprawcą jest uczeń - kolega ofiary ze szkoły czy klasy, uczniowie lub rodzice winni skontaktować się z dyrektorem szkoły, wychowawcą lub pedagogiem szkolnym. 2. 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).
Opis okoliczności, analiza, zabezpieczenie dowodów	1. W pierwszej kolejności należy zabezpieczyć dowody nieodpowiedniego lub niezgodnego z prawem działania - w formie elektronicznej (e-mail, zrzut ekranu, konwersacja w komunikatorze lub sms). 2. Równolegle należy dokonać zmian tych danych identyfikujących, które zależą od ofiary, tj. haseł i loginów, kodów dostępu do platform i portali internetowych, tak aby uniemożliwić kontynuację procederu naruszania prywatności. 3. Jeśli wykradzione dane zostały wykorzystane w celu naruszenia dobrego wizerunku ofiary, bądź w innych celach niezgodnych z prawem należy dążyć do wyjaśnienia tych działań i usunięcia ich skutków, także tych widocznych w Internecie. 4. Likwidacja stron internetowych czy profili w portalach społecznościowych, która wymagać będzie interwencji w zebrane dowody musi odbywać się za zgodą Policji.
Identyfikacja sprawcy(-ów)	1. W przypadku, gdy dowody jasno wskazują na konkretnego sprawcę oraz na spełnianie przesłanki, iż sprawca zmierzał do wyrządzenia ofierze szkody majątkowej lub osobistej należy je zabezpieczyć i przekazać Policji. 2. W przypadku, gdy trudno to ustalić, identyfikacji dokonać winna Policja. 3. W przypadku znanego sprawcy, który jednak nie działał z powyższych pobudek, szkoła powinna dążyć do rozwiązania problemu w ramach działań wychowawczo – edukacyjnych uzgodnionych z rodzicami.

Aktywności wobec sprawców zdarzenia ze szkoły/ spoza szkoły	Gdy sprawcą incydentu jest uczeń szkoły, należy wobec niego – w porozumieniu z rodzicami – podjąć działania wychowawcze, zmierzające do uświadomienia nieodpowiedniego i nielegalnego charakteru czynów, jakich dokonał. Działania takie szkoła winna podjąć niezależnie od powiadomienia Policji/ sądu rodzinnego. Dyrekcja szkoły podejmuje decyzje w sprawie powiadomienia 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.
Aktywności wobec ofiar zdarzenia	1. Ofiary incydentów należy otoczyć – w porozumieniu z rodzicami - opieką pedagogiczno-psychologiczną i powiadomić o możliwych działaniach podjętych w celu usunięcia skutków działania sprawcy. 2. 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 penalizacji.
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	W przypadku konieczności podejmowania dalszych działań pomocowych wobec ofiary, można skierować ucznia, za zgodą i we współpracy z rodzicami, do placówki specjalistycznej, np. terapeutycznej.

IV. 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)	<i>Infoholizm</i> (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	1. Infoholizm stwierdza najczęściej rodzic dziecka. Rzadziej zgłoszeń można się spodziewać od rówieśników dziecka nadmiernie korzystającego z Sieci. 2. W przypadku konieczności podejmowania działań pomocowych można skierować ucznia, za zgodą i we współpracy z rodzicami, do placówki specjalistycznej, np. terapeutycznej. 3. Nauczyciele w szkole także powinni zainteresować się przypadkami dzieci nieangażujących się w życie klasy, a poświęcającymi wolne chwile na kontakt online lub przychodzącymi do szkoły po nieprzespanej nocy.
Opis okoliczności, analiza, zabezpieczenie dowodów	Należy ustalić, jak nadmierne korzystanie z zasobów Internetu wpłynęło na dziecko (np. gorsze oceny w nauce, niedosypianie, niedojadanie, rezygnacja z dawnych zainteresowań, załamanie się relacji z rodziną czy rówieśnikami) w celu wyboru odpowiedniej ścieżki rozwiązywania problemu i wsparcia ucznia oraz jego rodziców.
Aktywności wobec ofiar zdarzenia	1. Osoba, której problem dotyczy, zostaje otoczona zindywidualizowaną opieką przez pedagoga szkolnego i wychowawcę. 2. Niezbędna jest współpraca rodzicami dziecka, w celu zagwarantowania powodzenia podejmowanych działań wspierających dziecko. 3. Każde dziecko, u którego podejrzewa się nałóg korzystania z Internetu powinno zostać profesjonalnie zdiagnozowane, warto w tym zakresie skorzystać z pomocy Poradni Psychologiczno-Pedagogicznej. 4. Dziecku w trakcie wsparcia należy zapewnić komfort psychiczny - o jego sytuacji i specyfice uwarunkowań osobistych muszą zostać powiadomieni wszyscy uczący go i oceniający nauczyciele.
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 u ucznia uzależnienia od korzystania z zasobów Internetu rodzic we współpracy ze szkołą powinien udać się z dzieckiem do placówki specjalistycznej oferującej program terapeutyczny z zakresu przeciwdziałania uzależnieniom.

**V. NAWIĄZYWANIE NIEBEZPIECZNYCH KONTAKTÓW W INTERNECIE –
UWODZENIE, ZAGROŻENIE PEDOFILIĄ, CHILD GROOMING**

Podstawy prawne uruchomienia procedury	Kodeks Karny, art. 200, 200a § 1 i 2, art. 286 § 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 (werbunku do sekty, grupy terrorystycznej lub promującej niebezpieczne zachowania) oraz wyłudzenia własności. W przypadkach niebezpiecznych kontaktów inicjowanych w Internecie może dochodzić do zagrożenia życia i zdrowia dziecka, szantażu i przymusu realizacji czynności seksualnych.
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	Osobami najczęściej zgłaszającymi omawiany problem są rodzice dziecka lub osoby zajmujące się „poszukiwaniem pedofili”. W pierwszym przypadku informacja trafia najpierw do szkół, w drugim - na Policję. Zdarza się, że informacja uzyskiwana jest ze środowiska rówieśników ofiary. Kluczowe znaczenie w działaniach szkoły ma czas reakcji - szybkość przeciwdziałania zagrożeniu ze względu na niezwykle szkodliwe konsekwencje realizacji kontaktu online.
Opis okoliczności, analiza, zabezpieczenie dowodów	Należy zidentyfikować i zabezpieczyć wszystkie dowody związane z działaniami sprawcy (zapisy rozmów w komunikatorach, na portalach społecznościowych, zrzuty ekranowe, zdjęcia, wiadomości e-mail). Jednocześnie – bezzwłocznie - należy dokonać zawiadomienia na 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.
Aktywności wobec ofiar zdarzenia	1. O możliwym związku takich zachowań dzieci z inspiracją w Internecie należy powiadomić rodziców. 2. W każdym przypadku próby nawiązania niebezpiecznego kontaktu należy we współpracy z rodzicami zapewnić ofierze poczucie bezpieczeństwa i opiekę psychologiczną. 3. Podobne wsparcie winno być udzielone w przypadku zaobserwowania antyzdrowotnych i zagrażających życiu zachowań uczniów (samookaleczenia, zażywanie substancji psychoaktywnych).

	4. W trakcie rozmowy z dzieckiem prowadzonej w warunkach komfortu psychicznego przez wychowawcę, pedagoga lub osobę ze szkoły, do której dziecko ma szczególne zaufanie, należy uzyskać wszelkie możliwe informacje o sprawcy i przekazać je Policji. 5. Dziecku należy udzielić profesjonalnej opieki terapeutycznej i/lub lekarskiej.
Aktywności wobec świadków	Jeżeli zgłaszającym zagrożenie był rówieśnik ofiary, należy również powiadomić o tym fakcie rodziców i objąć go opieką psychologiczno-pedagogiczną.
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 powinno się – w porozumieniu z rodzicami/opiekunami prawnymi – skierowanie ofiary na terapię do placówki specjalistycznej opieki psychologicznej.

VI. 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	<i>Seksting</i> - 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 głównie rodzice lub opiekunowie prawni dziecka - ofiary. Czasami informacja dociera do szkoły bezpośrednio od jej samej lub z grona bliskich znajomych dziecka. Delikatny charakter sprawy, a także potencjalna penalizacja sprawcy, wymagają zachowania daleko posuniętej dyskrecji i profesjonalnej reakcji.
Opis okoliczności, analiza, zabezpieczenie dowodów	Wyróżniamy 3 podstawowe rodzaje sekstingu, które skutkują koniecznością realizacji zmodyfikowanych procedur reagowania i zabezpieczenia materiałów elektronicznych: 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 zdjęcia. Jako, że seksting jest karalny, skrupulatność i wiarygodność dokumentacji ma duże znaczenie.
Aktywności wobec sprawców zdarzenia ze szkoły/ spoza szkoły	1. Zidentyfikowani małoletni sprawcy sekstingu winni zostać wezwani do dyrekcji szkoły, gdzie w obecności rodziców zostaną im przedstawione dowody ich aktywności. 2. Dalsze działania poza zapewnieniem wsparcia i opieki psychologiczno- pedagogicznej nie są konieczne, jednak istotne jest pouczenie sprawców zdarzenia, że rozpowszechnianie materiałów może być nielegalne i będzie miało konsekwencje prawne. 3. W przypadku uznania materiałów za pornograficzne, dyrektor placówki jest zobowiązany do zgłoszenia incydentu na Policję lub do sądu rodzinnego. 4. W sytuacji zaistnienia znamion cyberprzemocy, należy dodatkowo zastosować procedurę: Cyberprzemoc.
Aktywności wobec ofiar zdarzenia	1. Pierwszą reakcją szkoły i rodziców, obok dokumentacji dowodów, jest otoczenie wszechstronną, dyskretną opieką psychologiczno - pedagogiczną ofiary oraz zaproponowanie odpowiednich działań

	wychowawczych, w przypadku upublicznienia przypadku sekstingu w środowisku rówieśniczym. 2. Rozmowa na temat identyfikacji potencjalnego sprawcy jest realizowana w warunkach komfortu psychicznego dla dziecka – ofiary sekstingu, z szacunkiem dla jego indywidualności i przeżytego stresu.
Aktywności wobec świadków	Jeśli przypadek sekstingu zostanie upowszechniony w środowisku rówieśniczym – np. poprzez przesłanie MMS do uczniów tej samej szkoły lub klasy lub publikację w portalu społecznościowym, podejmuje się 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, 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. O skierowaniu do nich decyzję powinien podjąć pedagog szkolny wspólnie z rodzicami ofiary.

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

Podstawy prawne uruchomienia procedury	Ustawa z 14 grudnia 2016 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	Uczniowie nie umiejący odróżniać prawdy od fałszu informacji publikowanych w Internecie mogą być identyfikowani przez nauczycieli i wychowawców w trakcie lekcji wszystkich przedmiotów.
Opis okoliczności, analiza, zabezpieczenie dowodów	Posługiwanie się nieprawdziwymi informacjami zaczerpniętymi z Internetu w procesie dydaktycznym – podczas lekcji lub w zadaniach domowych, powinno być przeanalizowane i sprostowane przez nauczyciela.
Aktywności wobec sprawców zdarzenia ze szkoły/ spoza szkoły	Wystarczającą reakcją jest sprostowanie nieprawdziwych informacji.
Aktywności wobec ofiar zdarzenia i świadków	Szkoła prowadzi działania profilaktyczne - edukację medialną (informacyjną), np. w trakcie lekcji. Zajęcia w szkole mogą mieć charakter kilkuminutowych elementów edukacji medialnej wplecionej w lekcje o innej tematyce i/lub lekcji ukierunkowanych na zdobywanie przez dzieci i młodzież kompetencji medialnych.

VIII. ŁAMANIE PRAWA AUTORSKIEGO

Podstawy prawne uruchomienia procedury	Ustawa z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych Dz. U. z 2019 r. poz. 1231
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	W zależności od okoliczności oraz zaawansowania problemu, w którym doszło do ujawnienia sprawy, zdarzenie może zostać zgłoszone w sposób nieformalny (np. ustnie, pocztą elektroniczną) lub formalny (np. wezwania z Policji lub prokuratury). Przyjęcie zgłoszenia dokonanego w sposób nieformalny powinno zaowocować powstaniem notatki służbowej, zakomunikowania dyrektorowi szkoły w zależności od wagi sprawy. Szkoła może zetknąć się z problemem naruszenia praw autorskich jakim jest użycie materiałów prawnie chronionych na stronach internetowych szkoły, poza zakresem dozwolonego użytku, przez jej pracowników bądź uczniów. W przypadku naruszeń dokonanych dochodzenie roszczeń należy pozostawić osobom uprawnionym. Szkoła skupia się na swojej roli edukacyjno-wychowawczej poprzez organizację lekcji na temat praw autorskich.
Opis okoliczności, analiza, zabezpieczenie dowodów	Należy zweryfikować wszystkie informacje podawane przez zgłaszającego lub inne osoby i podjąć kontakt z odpowiednimi służbami celem ustalenia, czy okoliczności podane w zgłoszeniu faktycznie miały miejsce i czy powoływane tam dowody nie zostały zmanipulowane.
Identyfikacja sprawcy(-ów)	Szkoła powinna zgłosić zaistniałą sprawę odpowiednim instytucjom (policja, prokuratura) i skupić się na swojej roli wychowawczej i edukacyjnej, wykorzystując zaistniałą sytuację do przekazania wiedzy na temat tego, jak faktycznie prawo reguluje tę konkretną sytuację.
Aktywności wobec sprawców zdarzenia ze szkoły/ spoza szkoły	Szkoła podejmuje 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	Jeżeli osobą, której prawa autorskie naruszono, jest uczeń należy rozważyć możliwość wystąpienia szkoły w roli mediatora, aby stosownie do okoliczności ułatwić stronom ugodowe lub inne kompromisowe zakończenie powstałego sporu.
Aktywności wobec świadków	Stosownie do okoliczności, należy samodzielnie zebrać ich zeznania lub zadbać, aby zostały one zebrane przez uprawnione organy
Współpraca z Policją i sądami rodzinnymi	Ponieważ, co do zasady dochodzenie roszczeń z tytułu naruszeń zależy od decyzji uprawnionego, to uprawniony musi samodzielnie zdecydować czy zawiadamiać Policję lub składać powództwo. Stosownie do wskazanej wyżej roli mediatora, szkoła angażuje się natomiast przede wszystkim w ułatwianie zakończenia sporu bez takiej eskalacji.

Współpraca ze służbami społecznymi i placówkami specjalistycznymi	Szkoła organizuje szkolenie lub warsztaty z zakresu prawa autorskiego w Internecie dla wszystkich zainteresowanych osób w szkole.
Współpraca z dostawcami Internetu i teleoperatorami	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).

IX. ZAGROŻENIA BEZPIECZEŃSTWA TECHNICZNEGO SIECI, KOMPUTERÓW I ZASOBÓW ONLINE

Podstawy prawne uruchomienia procedury	Ustawa z dnia 14 grudnia 2016 r. - Prawo oświatowe Statut 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 zobowiązany jest do zgłoszenia go dyrekcji szkoły. Kluczowe znaczenie ma zebranie i zabezpieczenie przez specjalistę dowodów w formie elektronicznej.
Opis okoliczności, analiza, zabezpieczenie dowodów	Szczegółowy opis procedur reagowania na wystąpienie w szkole różnorodnych zagrożeń bezpieczeństwa cyfrowego zostaje zawarty w niniejszym dokumencie. W części przypadków szkoła poradzi sobie we własnym zakresie, w niektórych konieczne będzie skorzystanie z zewnętrznego wsparcia wyspecjalizowanych firm.
Identyfikacja sprawcy(-ów)	Identyfikację sprawców ataku należy pozostawić specjalistom. W sytuacji, gdy incydent spowodował 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 szkoły, o zaistniałej sytuacji należy powiadomić ich rodziców, zaś wobec nich podjąć działania wychowawcze. Jeżeli skutki ataku mają dotkliwy charakter, doprowadziły do zniszczenia mienia lub utraty istotnych danych, należy taki przypadek zgłosić na Policję.
Aktywności wobec świadków	O incydencie należy powiadomić społeczność szkolną i zaprezentować podjęte działania techniczne i wychowawczo-edukacyjne.
Współpraca z Policją i sądami rodzinnymi	W przypadku wystąpienia strat materialnych oraz utraty danych (szczególnie danych wrażliwych) należy zgłosić incydent na Policji.
Współpraca ze służbami społecznymi i placówkami specjalistycznymi	W przypadkach zaawansowanych awarii lub strat konieczne jest skorzystanie z zewnętrznego wsparcia eksperckiego, kontakt z serwisem twórcy oprogramowania lub zamówienie usługi w wyspecjalizowanej firmie.

NIELEGALNE TREŚCI

w szczególności treści pornograficzne
z udziałem osoby nieletniej



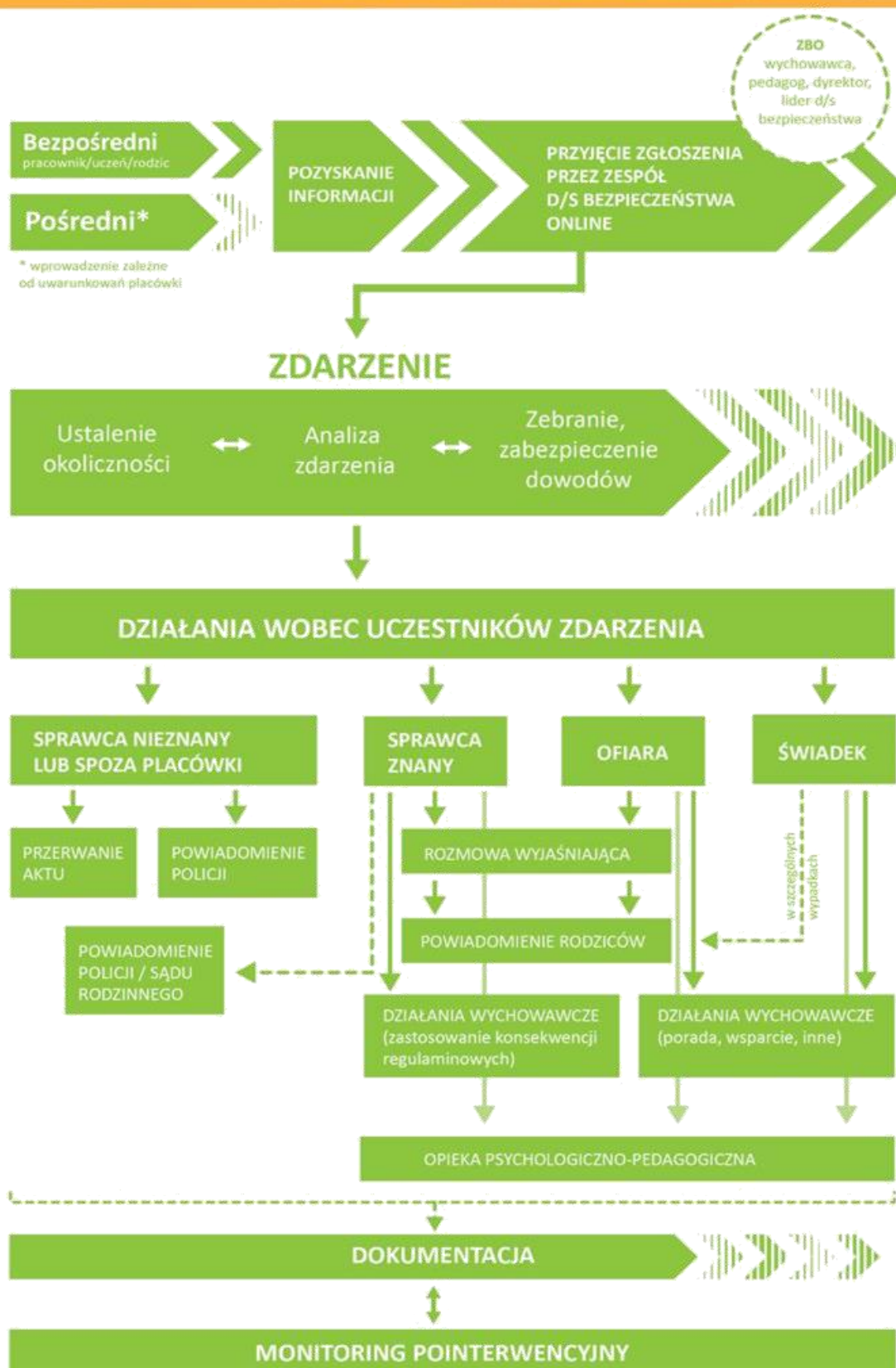
CYBERPRZEMOC



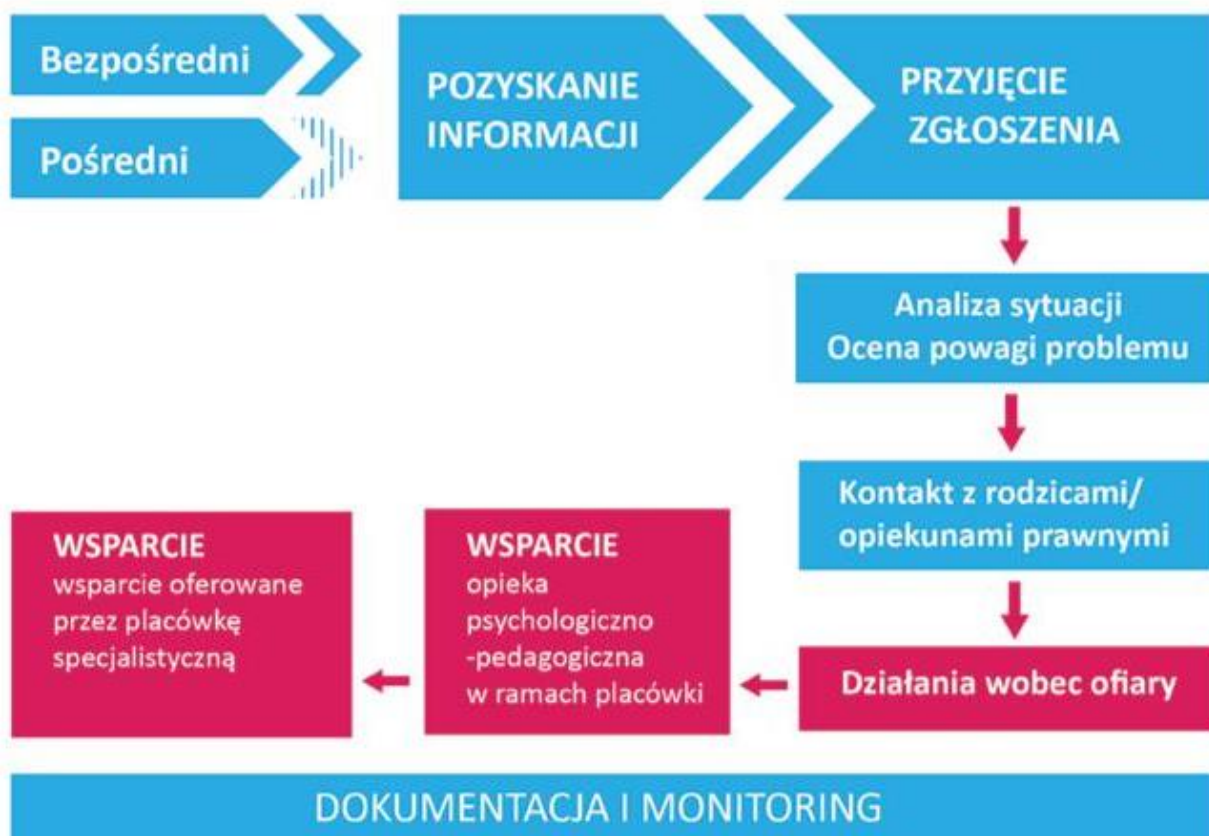
Możliwe naruszenie prawa

- groźba karna (art. 190 kk)
- uporczywe nękanie, podszywanie się (art. 190 a kk)
- zmuszanie do określonego działania (art. 191 kk)
- utrwalenie wizerunku nagiej osoby bez jej zgody, naruszenie intymności seksualnej (art. 191 a kk)
- zniesławienie (art. 212 kk)
- zniewaga (art. 216 kk)

SZKOLNY MODEL INTERWENCJI/PROCEDURY



NADMIERNE KORZYSTANIE Z INTERNETU/NOWOCZESNYCH TECHNOLOGII

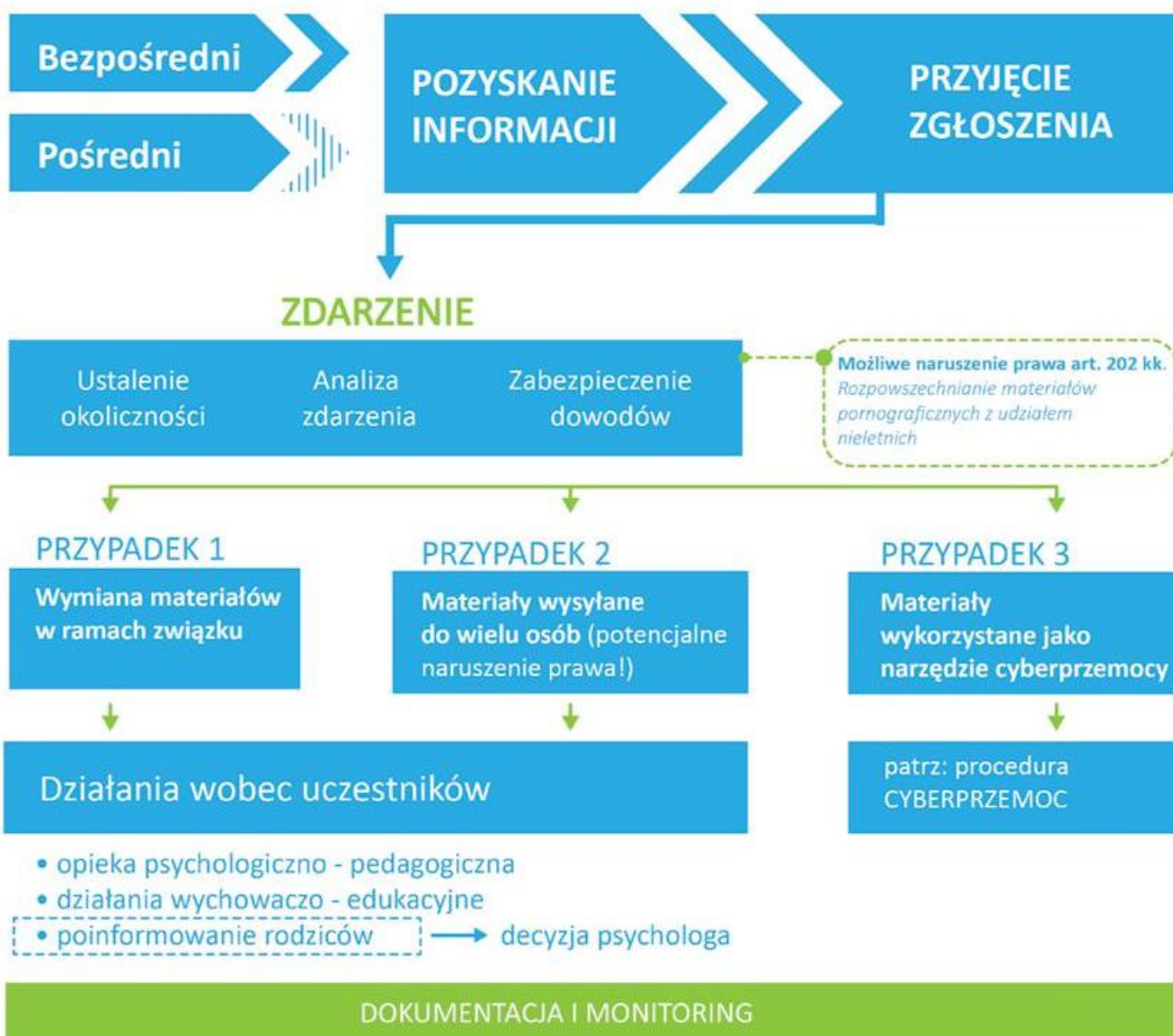


NIEBEZPIECZNE KONTAKTY CHILD GROOMING





SEKSTING



MODEL REAGOWANIA NA ZAGROŻENIA I INCYDENTY KOMPUTEROWE (TECHNOLOGICZNE)

