

Zespół Szkolno-Przedszkolny nr 14  
Szkoła Podstawowa nr 28 w Gliwicach

---

## PROCEDURY REAGOWANIA W PRZYPADKU WYSTĄPIENIA W SZKOLE ZAGROŻEŃ BEZPIECZEŃSTWA CYFROWEGO

1. Podstawowe działania na rzecz bezpieczeństwa cyfrowego w szkole, wdrażane w sytuacji wystąpienia.
2. Dostęp do treści szkodliwych, niepożądanych, nielegalnych – procedura reagowania.

DOSTĘP DO TREŚCI SZKODLIWYCH, NIEPOŻĄDANYCH, NIELEGALNYCH	
Podstawy prawne uruchomienia procedury	Kodeks karny, Statut szkoły
Rodzaj zagrożenia objętego procedurą	Zagrożenie łatwym dostępem do treści szkodliwych, niedozwolonych, nielegalnych i niebezpiecznych dla zdrowia (pornografia, treści obrazujące przemoc, hate i promujące działania szkodliwe dla zdrowia i życia dzieci, popularyzujące ideologię faszystowską i działalność niezgodną z prawem, nawoływanie do samookaleczeń i samobójstw, korzystanie ze środków psychoaktywnych).
Telefony alarmowe	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 elektornicznej lub wydruku. 2. W przypadku sytuacji (1) rozwiązanie leży po stronie szkoły, zaś (2) należy rozważyć zgłoszenie incydentu na Policję
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 (wychowca-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.

**Zespół Szkolno-Przedszkolny nr 14  
Szkoła Podstawowa nr 28 w Gliwicach**

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 podejrzenia popełnienia czynu karalnego należy powiadomić policję.

### 3. Cyberprzemoc – procedura reagowania

CYBERPRZEMOC	
Podstawy prawne uruchomienia procedury	Kodeks Karny, Statut szkoły.
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.
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 i materiały związane z aktem cyberprzemocy.
Identyfikacja sprawcy(-ów)	Jeśli ustalenie sprawcy nie jest możliwe 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. Pedagog szkolny przeprowadza rozmowę z uczniem, próbuje rozwiązać sytuację konfliktową.
Aktywności	W pierwszej kolejności należy udzielić wsparcia ofierze. W działaniu wobec

**Zespół Szkolno-Przedszkolny nr 14  
Szkoła Podstawowa nr 28 w Gliwicach**

wobec ofiar zdarzenia	ofiary należy także włączyć rodziców/opiekunów prawnych ofiary – na bieżąco informować o sytuacji, pamiętając o podmiotowym traktowaniu dziecka.
Aktywność wobec świadków	Należy zadbać o bezpieczeństwo świadków zdarzenia, zwłaszcza jeśli byli oni ujawniającymi cyberprzemoc.
Współpraca z Policją i sądami rodzinnymi	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). Za zgłoszenie odpowiada dyrektor szkoły.

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

<b>NARUSZENIA PRYWATNOŚCI DOTYCZĄCE NIEODPOWIEDNIEGO BĄDŹ NIEZGODNEGO Z PRAWEM WYKORZYSTANIA DANYCH OSOBOWYCH LUB WIZERUNKU DZIECKA I PRACOWNIKA SZKOŁY</b>	
Podstawy prawne uruchomienia procedury	Kodeks Karny (art. 190a par. 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. Należy zwrócić uwagę, że podszywanie się pod inną osobę, wykorzystywanie jej wizerunku lub danych osobowych w celu wyrządzenia jej szkody osobistej lub majątkowej jest w świetle polskiego prawa przestępstwem. Często naruszenia prywatności łączy się z cyberprzemocą.
<b>SPOSÓB POSTĘPOWANIA W PRZYPADKU WYSTĄPIENIA ZAGROŻENIA</b>	
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.
Opis okoliczności, analiza, zabezpieczenie dowodów	W pierwszej kolejności należy zabezpieczyć dowody nieodpowiedniego lub niezgodnego z prawem działania – w formie elektronicznej (email, sms, zrzut ekranu, konserwacja w komunikatorze).

**Zespół Szkolno-Przedszkolny nr 14**  
**Szkoła Podstawowa nr 28 w Gliwicach**

---

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	Gdy sprawcą jest incydentu jest uczeń szkoły, należy wobec niego – w porozumieniu z rodzicami – podjąć działania profilaktyczne , zmierzające do uświadomienia nieodpowiedniego i nielegalnego charakteru czynów, jakich dokonał.
Aktywności wobec ofiar zdarzenia	Otoczenie opieką ofiary incydentu w porozumieniu z rodzicami/prawnymi opiekunami. Powiadomienie o interwencji w celu usunięcia skutków działania sprawcy. Jeśli kradzież tożsamości, bądź naruszenie dobrego wizerunku ofiary jest znane tylko jej i rodzicom, szkoła winna zapewnić poufność działań.
Aktywności wobec świadków	Gdy kradzież tożsamości, bądź naruszenie dobrego wizerunku ofiary jest znane szerszemu gronu uczniów szkoły, należy podjąć wobec nich działania wychowawcze.