

**Procedury ochrony dzieci przed treściami szkodliwymi w Internecie oraz
utrwalonymi w innej formie**

I. Niebezpieczne treści (materiały pornograficzne, promujące nienawiść, rasizm, ksenofobię, przemoc, zachowania autodestrukcyjne)

1. Treści nielegalne lub niezgodne z regulaminem danej strony zgłaszane są administratorom strony.
2. W przypadku zgłoszenia o dostępie do treści nieodpowiednich, administrator sieci ustala okoliczności zdarzenia, podejmując próbę ustalenia sprawcy i świadków incydentu, a także zabezpiecza dowody, konfiguruje zabezpieczenia sieci przedszkola, by na nowo zablokować dostęp do niewłaściwych treści. Z poczynionych ustaleń sporządza notatkę służbową.
3. Jeśli treści niebezpieczne dotyczą osób niezwiązanych ze przedszkolem, dyrektor zgłasza zdarzenie odpowiednim służbom (sądowi rodzinnemu lub Policji), przekazując zabezpieczone materiały.
4. Jeśli uczestnikami zdarzenia są wychowankowie, ze sprawcą i ofiarą przeprowadzona jest rozmowa (oddzielnie) psychologa/pedagoga na temat emocji, jakie może budzić materiał, do jakich zachowań zachęca, omówione zostają także konsekwencje łamania regulaminu.
5. Powiadomieni zostają rodzice/opiekunowie prawni, których informuje się o poczynionych ustaleniach i dalszych działaniach przedszkola (zastosowane kary regulaminowe/środki oddziaływania wychowawczego, powiadomienie organów ścigania, wsparcie psychologiczno - pedagogiczne).
6. Współpraca z organami ścigania lub sądem rodzinnym obligatoryjnie musi zaistnieć w przypadku naruszenia zakazu rozpowszechniania materiałów pornograficznych z udziałem małoletniego (osoby poniżej 18 roku życia – art. 202 § 3 kodeksu karnego) oraz nawołujących do nienawiści na tle różnic narodowościowych, etnicznych, rasowych, wyznaniowych (art. 256 i art. 257 kodeksu karnego).

II. Naruszenie prywatności

1. Informacja o zagrożeniu naruszeniem prywatności w przedszkolu powinna zostać niezwłocznie przekazana osobie odpowiedzialnej za ID i dyrektorowi, którzy podejmują natychmiastowe

działania w celu zabezpieczenia danych i ograniczenia dalszego dostępu do informacji niejawnych.

2. Następnie należy ustalić okoliczności zdarzenia, poprzez dokładne udokumentowanie pozyskanych informacji i skontaktować się z ekspertem ds. bezpieczeństwa cyfrowego.
3. W przypadku poważniejszych zagrożeń i w sytuacji, gdy naruszenie prywatności jest spowodowane przez osoby spoza placówki, należy nawiązać współpracę z organami ścigania.
4. Osoba odpowiedzialna za ID powiadamia osoby dotknięte zdarzeniem (których dane osobowe wyciekły) o sytuacji, by podjęły indywidualne środki zaradcze.

III. Cyberprzemoc

1. Wychowanek, który stał się ofiarą lub świadkiem cyberprzemocy (wyśmiewania, poniżania przy użyciu technologii cyfrowych, obraźliwych komentarzy, rozpowszechniania wizerunku, manipulowania zdjęciami itp.) powinien zgłosić sytuację do wychowawcy lub psychologa/pedagoga. Zgłoszenia może dokonać także świadek cyberprzemocy.
2. Przedstawiciel personelu, do którego dotarła informacja próbuje ustalić okoliczności zdarzenia, zebrać dowody w postaci zrzutów ekranu, wiadomości, komentarzy, zdjęć, adresów stron internetowych. Zebrane materiały przekazywane są osobie wskazanej w osobie odpowiedzialnej za ID.
3. O zdarzeniu poinformowani zostają rodzice.
4. Psycholog/Pedagog udziela pomocy psychologiczno – pedagogicznej ofierze, wyjaśniając również kolejne etapy postępowania.
5. Jeśli sprawcą jest wychowanek, psycholog/pedagog powinien przeprowadzić z nim rozmowę, w wyniku której ustali, czy istnieją przesłanki do zgłoszenia sprawy do sądu rodzinnego lub Policji (przestępstwa ścigane z urzędu), czy wystarczające będzie zastosowanie kar regulaminowych/ środków oddziaływania wychowawczego.