

Cyberprzemoc i bezpieczeństwo cyfrowe

Pełny program warsztatowy o rozpoznawaniu krzywdzenia w sieci, bezpiecznej interwencji, ochronie dowodów, prywatności i odporności cyfrowej. Kurs uczy decyzji i komunikacji — nie zbiera ani nie analizuje rzeczywistych wiadomości dzieci.

Program: 120 minut

Odbiorcy: **Młodzież, rodzice, nauczyciele i dydakcja**

Przegląd źródeł: 12.10.2026

Zakres i odpowiedzialność: szkolenie stanowi materiał autorski Fundacji WHITE-RED. Nie jest opinią prawną, dokumentem zatwierdzonym przez MEN ani gwarancją gotowości placówki. Wymaga dopasowania do wieku i sytuacji uczestników, regulacji prawnych oraz lokalnych procedur. Ćwiczenia dotyczą wyłącznie sytuacji fikcyjnych i nie zbierają informacji o uczniach.

Cele i efekty kształcenia

1. Odróżnić konflikt, nieporozumienie i powtarzalne nękanie oraz rozpoznać groźby wymagające pilnej interwencji.
2. Umieć powstrzymać dalsze rozpowszechnianie krzywdzącego materiału i zapewnić wsparcie.
3. Wyznaczyć role rodzica, wychowawcy, pedagoga, administratora IT i dyrektora.
4. Przeprowadzić profilaktyczne ćwiczenie bez publikowania danych, zrzutów ekranu i wizerunków uczniów.

Plan przeprowadzenia szkolenia

Etap zajęć	Planowany czas
Otwarcie, zasady bezpieczeństwa i cele	10 min
Sześć modułów merytorycznych	65 min
Praca w grupach i studia przypadków	20 min
Quiz, omówienie i decyzje do wdrożenia	15 min
Podsumowanie i karta kontroli	10 min

Czasy orientacyjne. Szkolenie może być prowadzone z przerwą i dostosowane do kompetencji odbiorców.

MODUŁ 01 / 06

01. Mapa ryzyk i mechanizm cyberprzemocy

Krzywdzenie może mieć postać uporczywego poniżania w grupie, podszywania się, gróźb, publikowania treści ośmieszających lub wykluczania z komunikacji. Ocena nie powinna opierać się wyłącznie na liczbie wiadomości: znaczenie mają kontekst, relacja stron, skala rozpowszechnienia, wcześniejsze zachowania i bezpieczeństwo osoby pokrzywdzonej. Jednorazowa groźba również może wymagać pilnego działania.

W rozmowie z młodzieżą oddzielamy ocenę zachowania od etykietowania człowieka. Zamiast pytać „kto jest winny?”, najpierw ustalamy, czy ktoś pozostaje w niebezpieczeństwie, czego potrzebuje i jaka dorosła osoba może pomóc. Mechanizmy udostępniania, komentowania i „żartowania” mogą eskalować krzywdę, dlatego także pozornie bierny odbiorca odpowiada za decyzję, czy materiał rozpowszechniać.

Wnioski do zastosowania

- Rozpoznaj role: osoba pokrzywdzona, sprawca zachowania, świadek, zaufany dorosły.
 - Zaznacz, kiedy konflikt wymaga wsparcia wychowawczego, a kiedy pilnego alarmowania.
 - Zastąp słowo „donoszenie” pojęciem zgłoszenia w trosce o bezpieczeństwo.
-

MODUŁ 02 / 06

02. Pierwsza rozmowa i ochrona dziecka

Dorosły powinien wysłuchać spokojnie, nie obiecywać absolutnej tajemnicy i nie żądać natychmiastowego pokazywania wszystkich prywatnych rozmów. Dobre otwarcie brzmi: „Dziękuję, że mi o tym mówisz. Chcę zadbać o twoje bezpieczeństwo. Ustalimy, komu muszę przekazać informacje, żeby uzyskać pomoc”. Zamiast szczegółowego przesłuchania stosujemy pytania otwarte i minimum niezbędnych faktów.

Priorytetem jest przerwanie krzywdzenia, wsparcie i powstrzymanie wtórnej wiktymizacji. Nie organizujemy publicznego „wyjaśniania” na forum klasy, nie konfrontujemy uczestników na siłę i nie zawstydzamy rodziców. Szkoła działa w ramach swoich standardów ochrony małoletnich, a w sytuacji bezpośredniego zagrożenia życia lub zdrowia wzywa 112.

Wnioski do zastosowania

- Powiedz, co zrobisz teraz, kto będzie poinformowany i kiedy wrócisz z informacją.
 - Nie uzależniaj pomocy od posiadania zrzutów ekranu.
 - Zaplanuj wsparcie psychologiczno-pedagogiczne w kompetentnym zespole.
-

MODUŁ 03 / 06

03. Informacja, dowody i prywatność

Dokumentacja powinna być adekwatna do celu, sporządzana w bezpiecznym systemie placówki i udostępniana tylko osobom uprawnionym. Wystarczy często zapis chronologii, adresu strony, identyfikacji platformy oraz tego, kto i kiedy zgłosił problem; zakres dalszych materiałów oceniają właściwe osoby. Nie wykorzystujemy do ćwiczeń rzeczywistych treści dzieci ani nie tworzymy ich kopii w DSS.

Szczególną ostrożność zachowujemy wobec materiałów przedstawiających intymność małoletnich. Nie pobieramy ich, nie przesyłamy między pracownikami i nie używamy jako „dowodów szkoleniowych”. Należy przerwać obieg, zabezpieczyć bezpieczeństwo dzieci i skorzystać z właściwej procedury oraz uprawnionych organów. Samodzielne śledztwo cyfrowe prowadzone przez szkołę może zaszkodzić osobom pokrzywdzonym i naruszyć ich prawa.

Wnioski do zastosowania

- Nie publikuj treści zajęcia w klasowych komunikatorach.
 - Ustal odrębne role dla opieki nad dzieckiem i zarządzania informacją.
 - Dostęp do dokumentacji uzasadnij rzeczywistą potrzebą służbową.
-

MODUŁ 04 / 06

04. Higiena konta i reakcja na nadużycia

Unikalne hasła, uwierzytelnianie wieloskładnikowe, aktualizacje i rozważne korzystanie z linków ograniczają ryzyko przejęcia konta. Uczymy rozpoznawania próśb o kody uwierzytelniające, fałszywych formularzy i podszywania się pod znajomych. W przypadku naruszenia konta właściwe są procedury platformy, zmiana haseł z bezpiecznego urządzenia i wsparcie administratora systemów szkolnych.

Oddzielamy incydent techniczny od przemocy interpersonalnej: zgłoszenie phishingu do właściwego zespołu nie zastępuje pomocy poszkodowanemu uczniowi. Osobą odpowiedzialną za bezpieczeństwo systemów nie musi być osoba prowadząca działania pedagogiczne. Ważne jest ustalenie bezpiecznego punktu kontaktu w placówce i prawidłowego kanału do CERT Polska, gdy dotyczy to incydentu cyberbezpieczeństwa.

Wnioski do zastosowania

- Zastosuj ćwiczenie na fikcyjnej wiadomości, nie na realnej skrzynce pocztowej.
 - Wprowadź zasadę „nie przekazuję kodu logowania nawet znajomemu”.
 - Opracuj z uczniami trzy pytania kontrolne: kto prosi, dlaczego, co się stanie z danymi?
-

MODUŁ 05 / 06

05. Postępowanie zespołu i komunikacja z rodziną

Dyrektor zatwierdza odpowiedzialność i zasady eskalacji; wychowawca lub pedagog organizuje wsparcie; rodzice otrzymują rzetelne, proporcjonalne informacje. Nie wszystkie szczegóły dotyczące innych dzieci mogą być przekazywane każdej rodzinie. Jeżeli zachodzi podejrzenie przestępstwa, zagrożenie bezpieczeństwa lub krzywdzenie, uruchamia się odpowiednie procedury i organy.

Komunikacja nie może sugerować, że sama blokada konta rozwiązała problem. Należy sprawdzić, czy nękanie ustało, czy osoba pokrzywdzona ma wsparcie, czy nie pojawiła się nowa forma przemocy oraz czy działania profilaktyczne są bezpieczne i adekwatne. Publiczna informacja szkoły powinna być oparta na faktach i chronić prywatność. Zasady NASK z października 2026 r. akcentują odpowiedzialność za słowa i obrazy.

Wnioski do zastosowania

- Przypisz jedną rolę do kontaktu z rodzicami, drugą do ochrony informacji.
 - Oceń ponownie bezpieczeństwo po kilku dniach i uzgodnionym okresie obserwacji.
 - Unikaj publicznej prezentacji zgłoszeń, nawet po anonimizacji pozornej.
-

MODUŁ 06 / 06

06. Profilaktyka trwała, a nie jednorazowa lekcja

Skuteczny program buduje język reagowania: rozpoznaj, nie rozpowszechniaj, poproś o pomoc, zadbaj o osobę pokrzywdzoną. Uczniowie powinni znać dostępne kanały wsparcia i rozumieć, że zgłoszenie może dotyczyć także zachowań poza budynkiem szkoły, jeżeli wpływają na ich bezpieczeństwo i funkcjonowanie.

W starszych klasach warto analizować odpowiedzialność świadka, ekonomię uwagi i mechanizm viralowego udostępniania; w młodszych — korzystać z prostych fikcyjnych ilustracji i krótkich zdań. Rodzice otrzymują nie listę aplikacji do zakazania, lecz praktyczny schemat spokojnej rozmowy. Efektem szkolenia jest umiejętność wskazania jednej bezpiecznej ścieżki pomocy i jednej rzeczy, której nie wolno robić.

Wnioski do zastosowania

- Zaplanuj krótkie przypomnienie za miesiąc.
 - Zbierz anonimową informację, czy uczniowie wiedzą, komu zgłaszać problem.
 - Nie przechowuj odpowiedzi uczestników w publicznym narzędziu.
-

MATERIAŁ DLA PROWADZĄCEGO

Warsztat praktyczny

Instrukcja

W grupach po 3–4 osoby przeanalizuj fikcyjną wiadomość: „ktoś udostępnił obraźliwy mem o osobie z klasy”.

Oczekiwany rezultat

Grupa przygotowuje dwuminutową rozmowę pomocową, trzy kroki nieeskalowania i mapę ról szkoły.

Kryteria oceny

Prowadzący ocenia: bezpieczeństwo, brak obwiniania pokrzywdzonego, ochronę informacji i konkretny kanał wsparcia.

Zasada etyczna: bez odgrywania przemocy, ujawniania własnych doświadczeń, diagnozowania uczestników ani zbierania historii konkretnych uczniów.

Dwa studia przypadków do dyskusji

STUDIUM PRZYPADKU / 1

Fikcyjna sytuacja

W komunikatorze klasowym pojawia się zmanipulowana grafika dotycząca ucznia. Kilka osób przekazało ją dalej. Uczeń nie chce rozmawiać na forum klasy.

Pytania do dyskusji

Jak zapewnić mu wsparcie bez wymuszania relacji? Jak ograniczyć dystrybucję i wyznaczyć osoby odpowiedzialne?

Proponowany tok rozumowania

Najpierw zapewnij bezpieczny kontakt i niepowielanie treści. Oddziel pomoc pedagogiczną od prowadzenia dokumentacji; uruchom procedurę szkoły i ponownie oceń sytuację.

To model dydaktyczny; faktyczne działania muszą uwzględniać aktualne procedury i stan sprawy.

STUDIUM PRZYPADKU / 2

Fikcyjna sytuacja

Nauczyciel otrzymuje od ucznia informację o groźbach przesyłanych przez fałszywe konto. Nie wiadomo, czy groźba jest aktualna.

Pytania do dyskusji

Co jest kwestią pilności, a co potwierdzenia? Dlaczego nie należy prowadzić samodzielnej identyfikacji sprawcy?

Proponowany tok rozumowania

Ustal, czy istnieje bezpośrednie zagrożenie i w razie potrzeby wzywaj 112. Przekaż minimum faktów uprawnionym osobom i służbom; nie inicjuj publicznego „dochodzenia”.

To model dydaktyczny; faktyczne działania muszą uwzględniać aktualne procedury i stan sprawy.

SPRAWDZENIE WIEDZY

Test z omówieniem decyzji

Pięć pytań sprawdza zastosowanie zasad w fikcyjnych sytuacjach. Odpowiedzi pozostają wyłącznie w bieżącej stronie. Ocena nie jest egzaminem kwalifikacyjnym ani certyfikatem.

1. Co jest właściwe po otrzymaniu obraźliwego materiału?

Przesłać go całej klasie

Nie rozpowszechniać i zgłosić bezpieczną drogą

Wysłać do wszystkich rodziców

2. Czy brak zrzutu ekranu pozwala odmówić pomocy?

Nie, bezpieczeństwo oceniamy niezależnie od kompletności materiałów

Tak, dowód jest konieczny

Tylko rodzic może zgłosić

3. Jak należy postąpić z intymnym materiałem dotyczącym małoletniego?

Pobrać do prezentacji

Przekazać między nauczycielami

Nie kopiować ani rozpowszechniać; użyć właściwej ścieżki interwencji

4. Kto powinien wyznaczyć zakres komunikacji szkoły?

Uprawnione osoby zgodnie z procedurą

Dowolny członek grupy rodziców

Administrator publicznego forum

5. Jaki jest cel ponownej kontroli?

Sprawdzenie, czy nękanie ustało i pomoc działa

Zwiększenie liczby formularzy

Zamknięcie bez rozmowy

KARTA PRACY DYREKTORA / KOORDYNATORA

Lista kontrolna wdrożenia

Wykorzystaj na warsztacie lub wydrukuj. Zaznaczenie pozycji nie potwierdza samo w sobie prawnej zgodności placówki.

- ☐ Czy szkoła ma bezpieczny kanał informowania o cyberprzemocy?
- ☐ Czy personel wie, czego nie kopiować i nie rozpowszechniać?
- ☐ Czy przygotowano zasady reagowania na groźby i eskalację?

- ☐ Czy role pedagoga, dyrektora i administratora IT są rozdzielone?
- ☐ Czy dzieci znają przynajmniej dwie osoby, u których mogą szukać wsparcia?
- ☐ Czy ustalono sposób ponownej oceny po interwencji?
- ☐ Czy szkolenie stosuje wyłącznie fikcyjne treści?
- ☐ Czy rodzice znają zakres i ograniczenia komunikacji szkoły?

Sprawdził(a): Data:

Kolejny przegląd: Odpowiedzialna rola:

.....

Otwórz plan naprawczy w centrum dyrektora →

Wskazówki metodyczne i dostosowanie do odbiorców

- Klasy I–III: proste scenki słowne i karty „powiedz zaufanemu dorosłemu”; bez odgrywania przemocy.
- Klasy IV–VIII: analiza bezpiecznych wyborów świadka i granic prywatności; bez prawdziwych rzutów ekranu.
- Rodzice: krótka rozmowa w parach o pierwszym zdaniu, które chcą powiedzieć dziecku.
- Kadra/dyrekcja: sprawdzenie procedury zgłoszeń i ról, bez zbierania danych o rzeczywistych przypadkach.

Zasady prowadzenia

Na początku zajęć prowadzący informuje, że nikt nie musi opowiadać o własnych doświadczeniach. Przewidziane są alternatywne formy udziału, przerwa i możliwość skierowania uczestnika do zaufanej osoby. Każda analiza dotyczy neutralnego scenariusza. Instruktor wskazuje, które działania mają charakter organizacyjny, a które wymagają profesjonalnych kwalifikacji lub decyzji właściwych organów.

WERYFIKOWALNA WARSTWA MERYTORYCZNA

Źródła i charakter powołanych materiałów

Wskazane dokumenty stanowią punkty odniesienia do daty przeglądu 12.10.2026. Przed formalnym wdrożeniem regulaminu lub procedury należy sprawdzić aktualny tekst prawa i rozwiązania właściwe dla placówki.

1. CERT Polska — portal poradnictwa i reagowania na incydenty ↗

Źródło eksperckie z zakresu cyberbezpieczeństwa

2. MEN — „Wiedza moją Tarczą”, poradniki I–III oraz IV–VII, 8.10.2026 ↗

Materiały dydaktyczne; źródło zaleceń, nie akt prawny

3. MEN — Bezpieczna szkoła: bezpieczeństwo fizyczne i cyfrowe ↗

Poradnik metodyczny z 2020 r.; wymagane sprawdzenie aktualności szczegółów

4. Ministerstwo Sprawiedliwości — wytyczne standardów ochrony dzieci ↗

Wytyczne wdrożeniowe; nie zastępują tekstu ustawy

5. NASK — odpowiedzialne informowanie o przemocy w szkołach, 9.10.2026 ↗

Materiał ekspercki i etyczny; nie podstawa prawna

6. MEN — numery wsparcia dla uczniów, 8.10.2026 ↗

Oficjalna lista numerów alarmowych i pomocowych

Klasyfikacja: tekst ustawy = podstawa prawna; poradnik MEN, MS, RCB, NASK, RPD = źródło urzędowe lub eksperckie; scenariusze, testy i lista kontrolna = autorska metodyka Fundacji WHITE-RED. Szkolenie nie zostało zatwierdzone lub certyfikowane przez wskazane instytucje.