

Plan zapewnienia bezpieczeństwa cyfrowego

oprac. Monika Markowska

Podstawowym elementem cyfrowego bezpieczeństwa w szkołach jest wiedza i świadomość **uczniów**, ale także **nauczycieli i rodziców** na temat możliwych zagrożeń i ryzyka związanego z korzystaniem z Internetu i nowoczesnych narzędzi cyfrowych.

Profilaktyka

- Upowszechnianie wśród dzieci i młodzieży wiedzy o bezpieczeństwie.
- Kształtowanie właściwych postaw wobec zagrożeń.
- Aktywna profilaktyka powinna być prowadzona wobec i z udziałem wszystkich członków społeczności szkolnej
 - uczniów i ich rodziców oraz nauczycieli i innych pracowników placówki.

Netykieta – zasady dobrego zachowania w Internecie

- Nie flejmuj, czyli: nie obrażaj drugich.
- Nie staraj się na siłę zostać "pępkiem świata".
- Nie wysyłaj łańcuszków szczęścia i SPAM-u.
- Pamiętaj, że znajomi mają prawo do prywatności.
- Pamiętaj, że każdy może Cię znaleźć. Policja i mama również.
- Przestrzegaj prawa - adresy IP mogą być śledzone.
- Swoje opinie wyrażaj kulturalnie. Szanuj poglądy drugich.
- Sprawdzaj pisownię i podawaj źródła swoich informacji.
- Zwracaj uwagę prywatnie (nie w otwartym profilu przyjaciela!).

Przykłady zagrożeń

- Niebezpieczne treści.
- Hejt i fake news.
- Uzależnienie od Internetu.
- Phishing i spearphishing.
- Niebezpieczne kontakty w Sieci.
- Cyberprzemoc.

Niebezpieczne treści

- Takie, które mogą stanowić zagrożenie dla rozwoju dzieci. To nie tylko **pornografia** – to również treści **brutalne, obrzydliwe** czy promujące **niebezpieczne dla zdrowia zachowania**.

Hejt

- **Czyli mowa nienawiści** - to nieprzyjemne, obraźliwe wpisy pod filmami, zdjęciami czy postami.
- Co trzeci nastolatek spotkał się z mową nienawiści, a prawie 9% doświadczyło jej osobiście - wynika z badań **EU Kids online 2018**, prowadzonych pod kierownictwem prof. UAM Jacka Pyżalskiego w partnerstwie z Fundacją Orange. Mowa nienawiści i agresja stały się poważnym problemem.

Fake newsy

Fake newsy to nieprawdziwe informacje, które mogą mieć poważne konsekwencje i stają się plagą, a jej ofiarami padają zarówno dzieci, jak i dorośli.

Uzależnienie - podtypy

- **Uzależnienie od sieci** - przymus ciągłego śledzenia tego, co się dzieje w sieci.
- **Przeciążenie informacyjne** - gorączkowe przerzucanie informacji, udział w kilku listach dialogowych jednocześnie.
- **Uzależnienie od komputera** - przymus spędzania czasu z komputerem, nie ważne co się robi, ale komputer musi być włączony.
- **Erotomania internetowa** - nałogowe poszukiwanie materiałów pornograficznych i rozmowy o tematyce seksualnej w specjalnych chat-roomach).
- **Socjomania internetowa** - uzależnienie od kontaktów z ludźmi przez Internet z równoczesnym zanikiem kontaktów bezpośrednich.

Phishing i spearphishing

- Sytuacje, w której oszuści (hakerzy) wzbudzają nasze zaufanie po to, aby wyłudzić dane (np. hasło i login do facebooka) lub pieniądze, przesyłając maile czy sms-y.
- W **spearphishingu** hakerzy wysyłają informacje dostosowane do zainteresowań adresata.

Niebezpieczne kontakty w Sieci

- Uwodzenie dziecka (grooming).
- Wyłudzenie od dziecka materiałów z jego udziałem o charakterze seksualnym i erotycznym.
- Angażowanie w rozmowy o seksie.
- Wyłudzenie danych osobowych lub innych informacji w celach popełnienia przestępstwa przeciwko dziecku, rodzinie lub innym osobom.
- Nakłanianie dziecka do podejmowania zachowań zagrażających jego zdrowiu, a nawet życiu (np. zażywanie narkotyków, namawianie do samookaleczeń).

Cyberprzemoc

W przypadku dzieci i młodzieży **cyberprzemoc** to najczęściej przemoc rówieśnicza przy użyciu internetu i telefonów komórkowych. Jest to jedno z poważniejszych i bardziej powszechnych zagrożeń, z jakimi mogą mieć kontakt młodzi ludzie.

Formy cyberprzemocy

- Publikowanie ośmieszających filmów lub zdjęć.
- Publikowanie wulgarnych, prześmiewczych lub pełnych nienawiści i agresji komentarzy i wpisów.
- Włamania na konta serwisów społecznościowych.
- Nękanie telefonami i SMS-ami.
- Podszywanie się pod inne osoby.
- Wykluczanie ze społeczności internetowych.

Gdzie kryje się niebezpieczeństwo?

- Gry komputerowe.
- Czaty i komunikatory internetowe.
- Portale społecznościowe.

Jaką pomoc powinna zaoferować szkoła gdy dziecko stało się ofiarą przemocy

- **Poinformowanie rodziców** dziecka o problemie i okazanie im wsparcia i pomocy ze strony szkoły. W rozmowie z nimi pedagog lub wychowawca przedstawiają kroki, jakie zostały podjęte w celu wyjaśnienia zajścia oraz zapewnienia bezpieczeństwa poszkodowanemu uczniowi, a także, jeśli to wskazane, proponuje rodzicom i dziecku pomoc specjalisty (psychologa, pedagoga).

- **Wsparcie psychologiczne** (poradę, jak ma się zachować, aby zapewnić sobie poczucie bezpieczeństwa i nie doprowadzić do eskalacji prześladowania).
- Po zakończeniu interwencji należy **monitorować** sytuację ucznia sprawdzając, czy nie są wobec niego podejmowane dalsze działania przemocowe bądź odwetowe ze strony sprawcy.

Procedury bezpieczeństwa cyfrowego w szkołach

- Ministerstwo Edukacji Narodowej opublikowało zbiór rekomendacji i zaleceń dotyczących bezpieczeństwa w szkołach, którym istotną częścią są rekomendacje odnośnie procedur reagowania w przypadku zagrożenia bezpieczeństwa cyfrowego oraz procedury reagowania w szkole w przypadku wystąpienia incydentu zagrożenia.
- [Procedury_bezpieczenstwa_cyfrowego_w_szkole_rekomendacje](#)

Procedury reagowania w przypadku wystąpienia w szkole zagrożeń bezpieczeństwa cyfrowego - infografiki

Źródło: Cyfrowobezpieczni.pl [online], [dostęp: 17 stycznia 2020].
Dostępny w Internecie: <<https://www.cyfrowobezpieczni.pl/procedury-bezpieczenstwa-cyfrowego-w-szkolach>>.

Przemoc, pornografia, sekty,
 popularyzacja faszyzmu,
 nawoływanie do samokaleczeń,
 werbunek do organizacji
 terrorystycznych, promowanie
 korzystania z narkotyków.



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.



PROCEDURY REAGOWANIA W PRZYPADKU WYSTĄPIENIA W SZKOLE ZAGROŻEN BEZPIECZYSTWA CYFROWEGO

CYBERPRZEMOC

PRZYJĄCIE ZGŁOSZENIA I USTALENIE OKOLICZNOŚCI ZDARZENIA

- Wysłuchaj ze spokojem osoby zgłaszającej**
Działaj z empatią. Podążaj za motywacją i zgłoszenie sprawy jest sposobem cyfrowym, który może być wykorzystany przez ofiarę do wywołania lub zmiany sytuacji (niekiedy).
- Oceń, czy zdarzenie wyczerpuje znamiona cyberprzemocy**
Czy jest to naradyt uderzeniem (dotyczy to do skutków psychicznych), dotknięciem prywatności, nie dozwolone z użyciem danych itp. (dotyczy to do skutków psychicznych).
- Unikaj działań wtórnie stygmatyzujących**
To ważne dla ofiary, jak i dla sprawcy. Nie wywołuj wtórnie z użyciem danych itp. (dotyczy to do skutków psychicznych).
- Ustal charakter zdarzenia**
Sprawdź, czy ma to charakter przestępstwa, czy może być to czyn przestępstwa, czy może być to czyn przestępstwa, czy może być to czyn przestępstwa.

OPIS OKOLICZNOŚCI NA LUBO, ZARZĄDZENIE DOWODÓW

- Zabezpiecz wszystkie dowody**
Przeanalizuj dane dowodowe, aby być w stanie udowodnić, że doszło do zdarzenia, jakieś dane zostały, jakieś dane zostały, jakieś dane zostały.
- Zadbaj o bezpieczeństwo osób zaangażowanych w problem**
Przeanalizuj dane dowodowe, aby być w stanie udowodnić, że doszło do zdarzenia, jakieś dane zostały, jakieś dane zostały, jakieś dane zostały.

IDENTYFIKACJA SPRAWCY

- Skontaktuj się z Policją**
Jeśli ustalono sprawcę, nie należy się wahać i zgłosić sprawę do policji.

AKTYWNOŚCIOWE DZIAŁANIE

- Bezwzględnie zgłoś rozpowszechnianie nagich zdjęć osób poniżej 18 roku życia**
(art. 207 par. 2 KR)
- Rozmowa pedagoga szkolnego ze sprawcą**
Rozmowa ta ma służyć ustaleniu okoliczności zdarzenia, jego wspólnej analizie (w tym np. przestępstwa) i podjęciu działań naprawczych w celu uspokojenia ofiary.
- Określ „cyberprzemoc” w wewnętrznych przepisach szkoły**
Szkoła może być stroną odpowiedzialną za bezpieczeństwo ucznia. Warto więc rozważyć wprowadzenie do regulaminu szkoły przepisów dotyczących cyberprzemocy.
- Udziel wsparcia ofierze**
Ofiara zdarzenia może czuć się zagrożona i musi czuć wsparcie ze strony szkoły. Warto więc rozważyć wprowadzenie do regulaminu szkoły przepisów dotyczących cyberprzemocy.

AKTYWNOŚCIOWE DZIAŁANIE

- Włącz w działania rodziców/opiekunów ofiary**
Wykorzystaj do tego wszystkie dostępne narzędzia i metody. Nie należy się wahać i zgłosić sprawę do policji.
- Pomóż ofierze w zabezpieczeniu dowodów**
To ważne dla ofiary, aby móc udowodnić, że doszło do zdarzenia, jakieś dane zostały, jakieś dane zostały, jakieś dane zostały.
- Zaproponuj pomoc specjalisty oraz możliwość zgłoszenia sprawy Policji**
W trakcie rozmowy z ofiarą i rodzicami warto rozważyć zgłoszenie sprawy do policji.
- Monitoruj sytuację**
Pomóż ofierze nie czuć się zagrożoną i musi czuć wsparcie ze strony szkoły. Warto więc rozważyć wprowadzenie do regulaminu szkoły przepisów dotyczących cyberprzemocy.

AKTYWNOŚCIOWE DZIAŁANIE

- Zadbaj o bezpieczeństwo świadków zdarzenia**
Zadbaj o bezpieczeństwo świadków zdarzenia, aby nie czuli się zagrożeni i mogli udowodnić, że doszło do zdarzenia, jakieś dane zostały, jakieś dane zostały, jakieś dane zostały.

WSPÓŁPRACA Z POLICJĄ

- Skontaktuj się z Policją**
Jeśli ustalono sprawcę, nie należy się wahać i zgłosić sprawę do policji.

WSPÓŁPRACA Z DOSTAWCAMI INTENETU

- Skontaktuj się z dostawcą usługi w celu usunięcia z sieci kompromitujących lub krzywdzących materiałów**
Skontaktuj się z dostawcą usługi w celu usunięcia z sieci kompromitujących lub krzywdzących materiałów.

PODSZTYWY PRAWNE: Kodeks Karny, Statut szkoły, Regulamin szkoły
KONTAKTY ALARMOWE: Telefon Zaufania do Dział II Ministerstwa - 116 111; Telefon do Rzecznika i Komisji ds. spraw o bezpieczeństwo Dział II - 000 100 100, naj bliższa komisja

Dotyczące nieodpowiedniego lub niezgodnego z prawem wykorzystania danych osobowych lub wizerunku dziecka i pracownika szkoły (przestępstwo).



PROCEDURY REAGOWANIA W PRZYPADKU WYSTĄPIENIA W SZKOLE ZAGROZEŃ BEZPIECZEŃSTWA CYFROWEGO

NARUSZENIA PRYWATNOŚCI DOTYCZĄCE NIEODPOWIEDNIEGO BĄDŹ NIEZGODNEGO Z PRAWEM WYKORZYSTANIA DANYCH OSOBOWYCH LUB WIZERUNKU DZIECKA I PRACOWNIKA SZKOŁY

PRZYJĘCIE ZGROŻENIA I USTALENIE OKREŚLONOŚCI ZAGROŻENIA

Skontaktuj się z dyrektorem szkoły, wychowawcą lub Szkolnym Mentorem Bezpieczeństwa Cyfrowego

Gdy sprawca jest osobą znaną ofiarze z wirtualnej czy rzeczywistej sfery, zwróć się do niego.

Rodzice winni skontaktować się bez pośrednio z Policją i powiadomić o tym szkołę

W przypadku, gdy chodzi o nieznajomą przestępcę – jak na przykład kradzież, wglądanie w dane osobiste, wykorzystanie wizerunku dziecka – skontaktuj się z innymi osobami, które mogą być świadkami.

Ustal szczegóły sprawy, zbierz wszystkie informacje

Jeżeli nie jesteś ofiarą sprawy, bądź to w imieniu dziecka, ze sprawcą, jeżeli nie jest to osoba znaną ofiarze, bądź to w imieniu ofiary, bądź to w imieniu rodziców ofiary. Samo podjęcie się pod afisz nie jest karalne.

OPIS OKREŚLONOŚCI

Zabezpiecz dowody

Zgromadź materiały, które mogą być dowodem na naruszenie praw dziecka lub pracownika szkoły – w formie elektronicznej (e-mail, strona internetowa, komunikacja w komunikatorze lub sms).

Dokonaj zmian danych identyfikujących

To powinno się odbyć przed udaniem się do Policji z doniesieniem.

Zmierzaj do wyjaśnienia działań i usunięcia ich skutków

Także tych wirtualnych w Internecie. Jeśli wykradłeś dane, usuń je z Internetu. Jeśli ktoś inny je udostępnił, usuń je z Internetu. Jeśli ktoś inny je udostępnił, usuń je z Internetu.

Skontaktuj się z podmiotem świadczącym usługi – sprzedawcą w celu wyjaśnienia charakteru zdarzenia

Jeżeli kradzież lub wandalizm dotyczyło konto w sklepie Internetowym, skontaktuj się z sprzedawcą.

Likwidacja stron internetowych czy profili w portalach społecznościowych

Dotyczy to stron, które zostały utworzone przez sprawcę lub osoby, które zostały utworzone przez sprawcę.

IDENTYFIKACJA SPRAWCY

Zabezpiecz i przekaz dowody policji

Gdy sprawca jest osobą znaną ofiarze, zwróć się do niego z prośbą o przekazanie dowodów. Jeśli sprawca jest osobą nieznaną ofiarze, zwróć się do niego z prośbą o przekazanie dowodów.

Identyfikacji sprawcy dokonuje Policja

AKTYWNOŚCI ODC SPRAWCY I DZIAŁANIA

Rozwiąż problem w ramach działań wychowawczo-odukacyjnych

Jeżeli sprawca jest osobą znaną ofiarze, zwróć się do niego z prośbą o rozwiązanie problemu. Jeśli sprawca jest osobą nieznaną ofiarze, zwróć się do niego z prośbą o rozwiązanie problemu.

Podejmij działania wychowawcze

Ustawienie sprawy do jego podjęcia jest obowiązkiem szkoły, rodziców, nauczycieli. Wskazanie na odpowiedzialność, jakie ciąży na sprawcy z tytułu naruszenia praw, może być skutkiem działań wychowawczych.

AKTYWNOŚCI ODC OFIAR ZIARZENIA

Powiadomienie o incydencie Policji

Decyzję podejmuje dyrekcja szkoły. Skontaktuj się z Policją, jeśli sprawca jest osobą nieznaną ofiarze, zwróć się do niego z prośbą o rozwiązanie problemu. Jeśli sprawca jest osobą znaną ofiarze, zwróć się do niego z prośbą o rozwiązanie problemu.



Otocz ofiary opieką

Zapewnij opiekę psychologiczną i prawno-odukacyjną ofiarze. Jeśli sprawca jest osobą znaną ofiarze, zwróć się do niego z prośbą o rozwiązanie problemu. Jeśli sprawca jest osobą nieznaną ofiarze, zwróć się do niego z prośbą o rozwiązanie problemu.

Zapewnij poufność działań

Zachowaj poufność informacji o sprawie. Jeśli sprawca jest osobą znaną ofiarze, zwróć się do niego z prośbą o rozwiązanie problemu. Jeśli sprawca jest osobą nieznaną ofiarze, zwróć się do niego z prośbą o rozwiązanie problemu.

AKTYWNOŚCI ODC WŁADZ

Podejmij działania wychowawcze

Jeżeli sprawca jest osobą znaną ofiarze, zwróć się do niego z prośbą o rozwiązanie problemu. Jeśli sprawca jest osobą nieznaną ofiarze, zwróć się do niego z prośbą o rozwiązanie problemu.

WSPÓŁPRACA Z POLICJĄ

Policję winni powiadomić rodzice dzieci

Gdy naruszenie prywatności, czy wglądanie lub kradzież danych osobowych, dotyczy dziecka, rodzice powinni powiadomić Policję.

WSPÓŁPRACA Z PLACÓWKAMI SPECJALISTYCZNYMI

Skieruj ucznia do placówki specjalistycznej

W przypadku konieczności podjęcia działań pomocowych w obszarze zdrowia psychicznego, skieruj ucznia do placówki specjalistycznej.



ZAGROŻENIA DLA ZDROWIA DZIECI W ZWIĄZKU Z NADMIERNYM KORZYSTANIEM Z INTERNETU

I PRZYJĄCIE ZGŁOSZENIA I USTALENIE ORODZINOŚCI ZDARZENIA

Infokhizm scharakteryzuj jako nadmierne lub szkodliwe korzystanie z zasobów Internetu i gier komputerowych (najczęściej sieciowych) i portali społecznościowych przez dzieci.

Monitorujcie w szkole powroty uczniów z domu, zwracając uwagę na zmiany w ich zachowaniu, w tym na zmniejszenie czasu spędzającego z rodziną, na zmniejszenie zainteresowania nauką.

II OPIS ORODZINOŚCI, ANALIZA ZAOPINIENIEŃ DORADCÓW

Ustal skłótki zdrowotne i psychiczne. Wywołane nadmiernym korzystaniem z zasobów Internetu i gier komputerowych objawy (np. zmęczenie, bóle głowy, zmniejszenie koncentracji, zmniejszenie zainteresowania nauką, zmniejszenie zainteresowania sportem, zmniejszenie zainteresowania innymi hobby).

Skoncentruj się na wsparciu udzielonym rodzinie i w szkole. Zapewnij opiekę i wsparcie psychologiczne. W przypadku konieczności skorzystaj z poradnictwa i pomocy specjalistów.

Wybierz odpowiednie rozwiązanie problemu. Zorganizuj dla pomocy specjalistów (kolory, terapeutów) lub inne – w zależności od sytuacji.

III AKTYWNOŚCIOWE DZIAŁANIE



Otocz indywidualizowaną opieką. Zapewnij wsparcie pedagogiczne i psychologiczne w szkole.

Rozmowa ze specjalistą. Rozmowa z rodzicami i nauczycielami o objawy i skutki nadmiernej gry komputerowej.

Profesjonalna diagnoza. Kierujcie dziecko do specjalisty (psychologa, psychiatry, terapeuty zajęciowego, terapeuty muzycznego, terapeuty zajęciowego, terapeuty zajęciowego, terapeuty zajęciowego).

Zapewnij komfort psychiczny. Powołaj komisję do oceny sytuacji i działań nauczycieli i rodziców i spróbuj znaleźć warunki do zmniejszenia nadmiernej gry komputerowej.

Synergiczne współdziałanie rodziców i szkoły. Działania te powinny być skierowane na zmniejszenie czasu spędzającego z zasobami Internetu i gier komputerowych. Działania te powinny być skierowane na zmniejszenie czasu spędzającego z zasobami Internetu i gier komputerowych.



Zwróć uwagę na negatywne aspekty nadmiernej gry komputerowej. Zapewnij o konkretnym wsparciu dla dziecka dotkniętego problemem, a także o informowaniu o tym wsparciu w przypadku wystąpienia kolejnych przypadków u innych dzieci.

IV WSPÓŁPRACA ZE SZKOŁAMI I PLACÓWKAMI SPECJALISTYCZNYMI



Skierowane do placówki specjalistycznej. W przypadku nadmiernej gry komputerowej skierujcie dziecko do placówki specjalistycznej.

Diagnoza i terapia lekarska. W przypadku konieczności skierujcie dziecko do lekarza.

Infokhizm (sieciokhizm) – nadmierne, obejmujące niekiedy niemal całą dobę korzystanie z zasobów Internetu i gier komputerowych (najczęściej sieciowych) i portali społecznościowych przez dzieci.

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).



NAWIĄZYWANIE NIEBEZPIECZNYCH KONTAKTÓW W INTERECIE - UWODZENIE, ZAGROŻENIE PEDOFILIA

PRZYJĘCIE ZGŁOSZENIA I USTALENIE OKOLICZNOŚCI ZDARZENIA

Osobom najpóźniej zgłaszającym mi oznaczony problem są rodzice opiekunowie prawni dziecka lub osoby z opisywanej sytuacji „poradnikiem pedofilii”. W pierwszym przypadku informacja trafiła najpóźniej do szkoły w drugim – do Policji. Zdaniem szkoły nie informacja uzyskana jest z telefonów ani wiadomości e-mail.

Czas reakcji ma kluczowe znaczenie

W przypadkach niebezpiecznych kontaktów inicjujących on w Internecie małe dzieci trudniej do zapamiętania jest i ich wola do tego, skontaktować się z innymi osobami.

OPIS OKOLICZNOŚCI, ANALIZA, ZAGROŻENIE DOWODOM

Zidentyfikuj i zabezpiecz dowody działania dorosłego sprawcy uwodzenia

Zbierz dowody dostępne w formie elektronicznej (raporty, wiadomości w komunikatorach, na portalach społecznościowych, strony stronach, zdjęcia, wiadomości e-mail).

Bezwzględnie zawiadom Policję o wystąpieniu zdarzenia

IDENTYFIKACJA SPRAWCY

Nie podejmuj samodzielnych działań w celu dotarcia do sprawcy

Udziel wszelkiego możliwego wsparcia organom ścigania

Zabezpiecz i przekaz zebrałe dowody



AKTYWNOŚCI W OBEC SPRAWCY

Nie podejmuj aktywności zmierzających bezpośrednio do kontaktu ze sprawcą

Zadaniem szkoły jest zebranie dowodów i opisać nad ofiarą i ew. świadczenia.

AKTYWNOŚCI W OBEC OFIAR ZDARZENIA



Zapewnij ofierze opiekę psychologiczną i poczucie bezpieczeństwa

Powiadom rodziców o możliwym związku zachowań antyzdrowotnych dzieci z inspiracją w Internecie

Zachowania takie jak np. samookaleczenia czy nazywanie substancji psychoaktywnych mogą być inicjowane i wzmacniane poprzez kontakty w Internecie.

Otocz ofiary pomocą psychologiczno-pedagogiczną

Zadaniem szkoły jest zebranie dowodów i opisać nad ofiarą i ew. świadczenia.

Zapewnij warunki komfortu psychicznego

Przygotuj do pracy ofiary i ich opiekunów, psycholog, osoby ze szkoły, do której dziecka ma szczególne zaufanie.

Użyj wszelkiej możliwej informacji o sprawcy i przekaz ją Policji

Należy sprawić, aby nie kontakt ofiary z e sprawcą został przerwany, a dziecko odzyskało poczucie bezpieczeństwa.

Analizuj sytuację domową dziecka

Należy mieć świadomość, że dziecko może być narażone na kontakt w Internecie. Dziecko należy odnieść do profesjonalnej opieki i terapii oraz w celu interwencji.

AKTYWNOŚCI W OBEC ŚWIADKÓW

Wszelkie działania szkoły w obec dziecka uzgadniaj z rodzicami/opiekunami prawnymi

Obejmij zgłaszającego opieką psychologiczną

Jedną z głównych ról szkoły jest zapewnić ofiarze, nauczycielom i rodzicom opiekę psychologiczną.

WSPÓŁPRACA Z POLICJĄ I SĄDAMI RODZINNYMI

Powiadom Policję lub sąd rodzinny

Jest to obowiązek szkoły. W przypadkach naruszenia prawa – szczególnie w przypadku uwodzenia dziecka do lat 15.

WSPÓŁPRACA Z PRACOWNIKAMI SPECJALISTYCZNYMI



Sklaruj ofertę do placówki specjalistycznej opieki psychologicznej

W przypadkach uwodzenia małoletnich przez osoby dorosłe rekomenduje się – w porozumieniu z rodzicami/opiekunami prawnymi – skierowanie ofiary na terapię.

Prowokacyjne zachowania i aktywność seksualna jako źródło dochodu osób nieletnich - przesyłanie drogą elektroniczną lub publikowanie w portalach (społecznościowych) prywatnych treści, głównie zdjęć, o kontekście seksualnym, erotycznym i intymnym.



SEKSTING, PROWOKACYJNE ZACHOWANIA I AKTYWNOŚĆ SEKSUALNA JAKO ŹRÓDŁO DOCHODU OSÓB NIELETNICH

PRZYJĘCIE ZGŁOSZENIA I USTALENIE ODDUCZNOŚCI ZA REZONA



Zygnień dokonując głośno nadciagając się do dziecka. Czasami informacja dociera do szkoły bezpośrednio od ofiary lub z grona bliskich znajomych dziecka. W trudnych wypadkach pracownicy szkoły sami identyfikują takie zdarzenia w sieci. Czasami zgłoszenia dokonują ofiary lub osoby je znające.

Zachowaj daleko posuniętą dyskrecję i profesjonalną reakcję

Szczególnie w środowisku rówieśniczym ofiary. Wywołują tego delikatny charakter sprawy, a także potencjalna powściągnięcie sprawy.

OPIS ODDUCZNOŚCI, ANALIZA, ZARZĄCZENIE DOWODÓW

Wyróżniamy 3 podstawowe rodzaje sekstingu:

Rodzaj 1.

Wytworzone materiały o charakterze seksualnym nagrywane są w ramach związku między innymi nieintencjonalnie, nie są w pełni przemyślane, nie są w pełni profesjonalne.

Rodzaj 2.

Materiały o charakterze seksualnym zostały narobione w wyniku działań osób, jednak nie dochodzi do ich rozpowszechnienia na tym etapie. Wówczas materiały mogą być usunięte z sieci.

Rodzaj 3.

Materiały zostały narobione w wyniku działań osób w celu uzyskania korzyści na nich opartych (np. w postaci pieniędzy, jakichkolwiek korzyści).

IDENTYFIKACJA SPRAWCY

Zabezpiecz dowody

Przebieg sprawy zależy, czy zostały udokumentowane dowody. Dotyczy to przede wszystkim ofiar. Dotyczy to przede wszystkim ofiar. Dotyczy to przede wszystkim ofiar.

AKTYWNOŚĆ OŚC SPRAWCÓW Z DZIECIEM

Rodzaj 1.

Osoba dokonująca przesyłania materiałów w sposób psychologicznie i emocjonalnie wywołujący u ofiary poczucie zagrożenia, aby osoba przesyłała materiały.

Rodzaj 2.

Niekiedy z tego typu materiałów mogą być wykonane kopie, które mogą być wykorzystane do celów dowodowych.

Rodzaj 3.

Materiały zostały przesyłane w celu uzyskania korzyści na nich opartych (np. w postaci pieniędzy, jakichkolwiek korzyści).

Wezwij sprawców do dyrekcji szkoły

Przebieg sprawy zależy, czy zostały udokumentowane dowody. Dotyczy to przede wszystkim ofiar. Dotyczy to przede wszystkim ofiar.

AKTYWNOŚĆ OŚC OFIAR ZDARZENIA

Działaj w porozumieniu z rodzicami lub opiekunami prawnymi sprawców



Otocz wszechstronną, dyskretną opieką psychologiczno-pedagogiczną

Przeprowadź rozmowę na temat identyfikacji potencjalnego sprawcy

AKTYWNOŚĆ OŚC ŚWIADKÓW



Podjęj działania wychowawcze

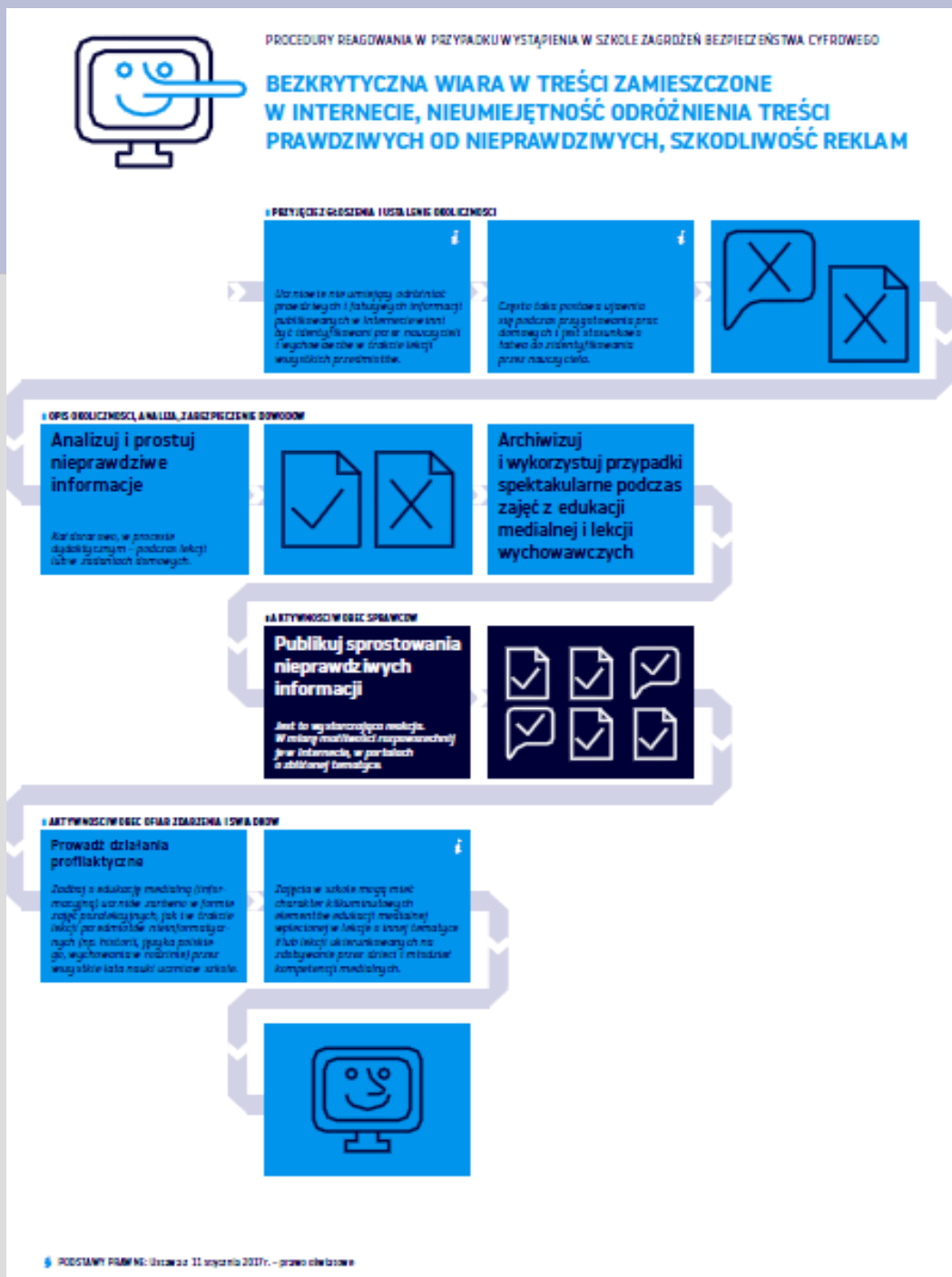
WSPÓŁPRACA Z POLICJĄ I SĄDAMI RODZINNymi

Powiadom Policję lub sąd rodzinny

WSPÓŁPRACA Z PRACOWNIKAMI SPECJALISTYCZNYMI

Skontaktuj się z placówkami specjalistycznymi

Nieumiejętność odróżnienia treści prawdziwych od nieprawdziwych, bezkrytyczne uznawanie za prawdę tez publikowanych w forach internetowych, kierowanie się informacjami zawartymi w reklamach.





ŁAMANIE PRAWA AUTORSKIEGO

PRZYJĘCIE ZGŁOSZENIA I USUŁENIE DROGOMIĘDZYSKOWE

Zdobądź dane z materiału zgłoszonego w sposób nieformalny (np. ustnie, telefonicznie, pocztą elektroniczną) lub formalny (w postaci doprecyzowania adresu poczty lub innego adresu elektronicznego np. wiadomości z Polityj lub prokuratury).

Utwórz formalny ślad
W przypadku przyjęcia zgłoszenia dokonaj go w sposób nieformalny (np. ustnie, telefonicznie, pocztą elektroniczną) lub formalny (w postaci doprecyzowania adresu poczty lub innego adresu elektronicznego np. wiadomości z Polityj lub prokuratury).

Unikaj wdawania się w argumentację, pochopnego przyznawania roszczeń lub spełniania żądań, pływaniowania domniemych sprawców, itd.

Uzyskaj fachową pomoc prawną

Nie występuj w roli sędziego
W przypadku naruszeń dokonanych przez uczniów, dochodzenie należy prowadzić osobno i niezależnie.

Nie występuj w roli sędziego
W przypadku naruszeń dokonanych przez uczniów, dochodzenie należy prowadzić osobno i niezależnie.

Skup się na roli edukacyjno-wychowawczej
Zajmij się przede wszystkim edukacją i wychowaniem, a nie dochodzeniem roszczeń.

Zweryfikuj wszystkie informacje podane przez zgłaszającego lub inną osobę
Sprawdź, czy okoliczności podane w zgłoszeniu faktycznie miały miejsce i czy powołane na dowody nie zostały zmanipulowane.

Zbierz informacje
Sprawdź, czy osoba dokonująca zgłoszenia jest do tego uprawniona (czy faktycznie przysługują jej prawa autorskie do danego utworu, czy posiada w danej dziedzinie wiedzę itp.).

Zbierz informacje
Sprawdź, czy osoba dokonująca zgłoszenia jest do tego uprawniona (czy faktycznie przysługują jej prawa autorskie do danego utworu, czy posiada w danej dziedzinie wiedzę itp.).

Dochodzenie naruszeń praw autorskich może prowadzić do odpowiedzialności cywilnej i karnej, a także do odpowiedzialności administracyjnej.

Szkola nie powinna wyřęcać Policji i prokuratury ani też wkraczać w ich kompetencje

Szkola powinna skupić się na roli wychowawczej i edukacyjnej
Wykorzystaj do tego wszystkie dostępne narzędzia (np. zajęcia, projekty, konkursy, itp.) i nie zapominaj o roli wychowawczej i edukacyjnej.

Szkola powinna podjąć działania o charakterze edukacyjno-wychowawczym
Wykorzystaj do tego wszystkie dostępne narzędzia (np. zajęcia, projekty, konkursy, itp.) i nie zapominaj o roli wychowawczej i edukacyjnej.

Rozważ możliwość wystąpienia w roli mediatora
Jeżeli osoba, której prawa autorskie zostały naruszone, jest uczniem, należy ustalić z nim porozumienie lub inne kompromisowe rozwiązanie powstałego sporu.

Pomóż sprawcy zaniechania naruszeń i naprawienia ich skutków

Zbierz zeznania lub zadbaj, aby zostały one zebrane przez uprawnione organy.
Skontaktuj się z policją.

Współpraca z policją
Uprawniony może samodzielnie zgłosić sprawę do policji lub skierować ją do policji.

Współpraca z szeregami społecznymi
Rozważ z organizacjami społecznymi lub warsztatami z zakresu prawa autorskiego w Internecie.

Współpraca z dostawcami internetu
Skontaktuj się z dostawcą internetu, aby poinformować go o naruszeniu i poprosić o wyłączenie dostępu do stron, które są źródłem naruszeń.

Ryzyko poniesienia odpowiedzialności cywilnej lub karnej z tytułu naruszenia prawa autorskiego albo negatywnych skutków pochopnego spełnienia nieuzasadnionych roszczeń (tzw. copyright trolling).



ZAGROŻENIA BEZPIECZEŃSTWA TECHNICZNEGO SIECI, KOMPUTERÓW I ZASOBÓW ONLINE

PRZYJĘCIE ZGŁOSZENIA I USTALENIE OBECNOŚCI ZDARZENIA

Zgłoś incydent osobie odpowiedzialnej za infrastrukturę cyfrową szkoły oraz dyrekcji

Alaczkwie zdarzenie ma złośliwy i zabezpieczenie przez specjalistę danej firmy w formie elektronicznej.

OPIS OBECNOŚCI, ANALIZA, ZAPROPOZYCIE DZIAŁAŃ

W innych przypadkach skontaktuj się z firmą, która świadczy usługi IT, aby uzyskać wsparcie techniczne i zaplanować działania naprawcze.

IDENTYFIKACJA SPRAWCY

Pozostaw specjalistom identyfikację sprawców ataku

Powiadom Policję
W sytuacji, gdy incydent spowodował atak na dane osobiste lub dane innej osoby, powiadom Policję o zdarzeniu.

AKTYWNOŚCI W OBLICZNIU

Podejmij działania wychowawcze i powiadom rodziców
Jeśli sprawa dotyczy danych osobowych, powiadom rodziców.

AKTYWNOŚCI W OBLICZNIU

Powiadom społeczność szkolną
Zaprezentuj podjęte działania, tak przynależące do społeczności szkolnej.

WSPÓŁPRACA Z POLICJĄ I SĄDAMI

Zgłoś incydent na Policję
W przypadku wystąpienia strat materialnych danej osoby, powiadom Policję o zdarzeniu.

WSPÓŁPRACA Z SPECJALISTYCZNYMI FIRMAMI

Skorzystaj z zewnętrznego wsparcia eksperckiego
W przypadku złośliwych ataków na dane osobiste lub dane innej osoby, skorzystaj z zewnętrznego wsparcia eksperckiego.

Zagrożenia bezpieczeństwa technicznego sieci, komputerów i zasobów online.

Warto odwiedzić:

- **Dziecko w Sieci** - kampania „Chroń dziecko w Sieci” przestrzeganie przed konsekwencjami kontaktów dzieci w wieku przedszkolnym i wczesnoszkolnym ze szkodliwymi treściami w Internecie.

- **NASK** – państwowy instytut badawczy nadzorowany przez Ministerstwo Cyfryzacji, prowadzi działalność związaną z bezpieczeństwem Internetu.

- **Saferinternet** – działania na rzecz bezpieczeństwa dzieci i młodzieży korzystających z Internetu i nowych technologii.

- **Fundacja Dajemy Dzieciom Siłę** - pomoc dla dzieci, które doświadczyły przemocy.

- **Dyżurnet.pl**- zgłaszanie nielegalnych treści w Internecie, szczególnie związanych z seksualnym wykorzystywaniem dzieci.

- **Telefon zaufania dla dzieci i młodzieży**

- **Telefon dla rodziców i nauczycieli**

- **Fundacja Orange** - działa na rzecz nowoczesnej edukacji.

- **Sieciaki** - portal edukacyjny
- **Necio.pl** - portal edukacyjny

Bibliografia:

- 116111.pl [online], [dostęp: 17 stycznia 2020]. Dostępny w Internecie: <<https://116111.pl/mlodziez>>.
- Bezpiecznaszkola.men.gov.pl [online], [dostęp: 17 stycznia 2020]. Dostępny w Internecie: <<https://bezpiecznaszkola.men.gov.pl/bezpieczna-szkola-zagrozenia-i-zalecane-dzialania-profilaktyczne-w-zakresie-bezpieczenstwa-fizycznego-i-cyfrowego-uczniow/>>.
- *Bezpieczna szkoła: zagrożenia i zalecane działania profilaktyczne w zakresie bezpieczeństwa fizycznego i cyfrowego uczniów*, MEN, Warszawa 2017.
- Cyfrowobezpieczni.pl [online], [dostęp: 17 stycznia 2020]. Dostępny w Internecie: <https://www.cyfrowobezpieczni.pl/procedury-bezpieczenstwa-cyfrowego-w-szkolach>.
- Dyżurnet.pl [online], [dostęp: 17 stycznia 2020]. Dostępny w Internecie: <<https://dyzurnet.pl/>>.
- Fdds.pl [online], [dostęp: 17 stycznia 2020]. Dostępny w Internecie: <https://fdds.pl/o-nas/>.
- Fundacja.orange.pl [online], [dostęp: 17 stycznia 2020]. Dostępny w Internecie: <<https://fundacja.orange.pl/>>.
- Nask.pl [online], [dostęp: 17 stycznia 2020]. Dostępny w Internecie: <<https://www.nask.pl/pl/dzialalnosc/projekty/safer-internet/3427,Safer-Internet.html>>.
- *Rodzice Nastolatków 3.0: raport z ogólnopolskiego badania społecznego*, pod red. R. Lange, NASK, Warszawa 2019.
- Saferinternet.pl [online], [dostęp: 17 stycznia 2020]. Dostępny w Internecie: <https://www.saferinternet.pl/>.
- *Standard bezpieczeństwa online placówek oświatowych*, pod red. J. Lizut, Fundacja Odkrywców Innowacji, Warszawa 2015.