PROCEDURY REAGOWANIA W PRZYPADKU ZAGROŻEŃ BEZPIECZEŃSTWA CYFROWEGO

1. Zapewnienie bezpieczeństwa ucznia w sieci

1. Wszystkie komputery, z których korzystają uczniowie są zabezpieczone odpowiednim oprogramowaniem utrudniającym uczniom dostęp do treści niepożądanych.

2. Uczniowie mogą korzystać z Internetu wyłącznie pod kontrolą nauczyciela.

3. Nauczyciel nadzorujący pracę ucznia z komputerem powinien posiadać odpowiednie kwalifikacje.

4. W trakcie zajęć uczniowie mają obowiązek:

a) przestrzegać zasad ograniczonego zaufania przede wszystkim wobec nowo poznanych osób,

b) nie przekazywać danych osobowych,

c) nie otwierać poczty elektronicznej bez zgody nauczyciela,

d) nie korzystać z komunikatorów,

e) nie zapisywać na dysku komputerów ściągniętych z Internetu plików graficznych, muzycznych, filmowych itp.,

f) nie umieszczać treści obraźliwych na stronach www (księgi gości itp.) i na dysku komputera,

g) przestrzegać etykiety,

h) w razie wystąpienia sytuacji kłopotliwej, niejasnej zwrócić się do nauczyciela o pomoc.

5. Nauczyciel ma obowiązek uświadomić uczniom zagrożenia związane z Internetem.

6.Wszystkie incydenty, które nauczyciel uzna za szkodliwe, ma obowiązek zgłosić dyrektorowi/wicedyrektorowi Ośrodka oraz odpowiednim organizacjom i instytucjom zajmującym się ściganiem przestępstw internetowych.

2. Reagowanie w sytuacji cyberprzemocy

1) Procedura interwencyjna powinna obejmować:

a) udzielenie wsparcia ofierze przemocy,

b) zabezpieczenie dowodów i ustalenie okoliczności zdarzenia,

c) wyciągnięcie konsekwencji wobec sprawcy przemocy oraz praca nad zmianą postawy ucznia.

2) Ustalenie okoliczności zdarzenia.

2.1. Jeśli wiedzę o zajściu posiada nauczyciel nie będący wychowawcą, powinien przekazać informację wychowawcy klasy, który informuje o fakcie pedagoga lub psychologa oraz dyrektora/ wicedyrektora.

2.2. Pedagog/psycholog i dyrektor wspólnie z wychowawcą dokonują analizy zdarzenia i planują dalsze postępowanie w celu ustalenia okoliczności zdarzenia oraz ewentualnych świadków.

3) Zabezpieczenie dowodów.

3.1. Wszelkie dowody cyberprzemocy nauczyciel/ wychowawca zabezpiecza i rejestruje. Następnie zapoznaje wszystkie zaangażowane w sprawę osoby: dyrektora/ wicedyrektora, pedagoga/psychologa, rodziców, w przypadku złamania prawa - policję.

3.2. Należy zanotować datę i czas otrzymania materiału, treść wiadomości oraz, jeśli to możliwe, dane nadawcy (nazwę użytkownika, adres e-mail, numer telefonu komórkowego, itp.) lub adres strony www, na której pojawiły się szkodliwe treści czy profil.

4) Identyfikacja sprawcy.

4.1. Szkoła podejmuje działania mające na celu identyfikację sprawcy cyberprzemocy.

4.2. W sytuacji kiedy ustalenie sprawcy nie jest możliwe, należy powiadomić dostawcę usługi w celu usunięcia z sieci kompromitujących lub krzywdzących materiałów. Do podjęcia takiego działania zobowiązuje administratora serwisu art. 14 Ustawy z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną.

4.3. W przypadku, gdy zostało złamane prawo, a tożsamości sprawcy nie udało się ustalić należy bezwzględnie skontaktować się z policją.

5) Działania wobec sprawcy cyberprzemocy:

5.1. W przypadku, gdy sprawca cyberprzemocy jest znany i jest on wychowankiem Ośrodka, pedagog/ psycholog przeprowadza rozmowę z uczniem, której celem jest wyjaśnienie okoliczności zdarzenia, jego przyczyn, ustalenia sposobów rozwiązania sytuacji problemowej, omówienia konsekwencji.

5.2. Jeśli w zdarzeniu brała udział większa grupa uczniów, należy rozmawiać z każdym z nich z osobna, zaczynając od lidera grupy.

5.3. Nie należy konfrontować sprawcy i ofiary cyberprzemocy.

5.4. Wychowawca informuje rodziców/ opiekunów prawnych sprawcy o przebiegu zdarzenia i zapoznaje z materiałem dowodowym, a także o decyzji w sprawie dalszego postępowania i podjętych środkach dyscyplinarnych wobec ich dziecka.

5.5. We współpracy z rodzicami/ prawnymi opiekunami wychowawca opracowuje kontrakt dla dziecka, określającego zobowiązania ucznia, rodziców/ prawnych opiekunów i przedstawiciela szkoły oraz konsekwencje nieprzestrzegania przyjętych wymagań.

6) Zastosowanie środków dyscyplinarnych wobec sprawcy cyberprzemocy

6.1. Wobec sprawcy cyberprzemocy stosuje się kary zawarte w statucie Ośrodka.

6.2. Podejmując decyzję o rodzaju kary należy wziąć pod uwagę:

a) rozmiar i rangę szkody,

b) czas trwania prześladowania,

c) świadomość popełnianego czynu,

d) motywację sprawcy,

e) rodzaj rozpowszechnianego materiału.

7. Działania wobec ofiary cyberprzemocy

7.1. Ofiara cyberprzemocy otrzymuje w szkole wsparcie psychologiczne udzielane przez pedagoga/psychologa.

7.2. Po zakończeniu interwencji wychowawca wraz z osobą udzielającą pomocy monitorują sytuację ucznia sprawdzając, czy nie są wobec niego podejmowane dalsze działania przemocowe bądź odwetowe ze strony sprawcy.

8. Sporządzenie dokumentacji z zajścia

8.1. Wychowawca, pedagog/psycholog zobowiązany jest do sporządzenia notatki służbowej z rozmów ze sprawcą, poszkodowanym, ich rodzicami oraz świadkami zdarzenia. Dokument powinien zawierać datę i miejsce rozmowy, personalia osób biorących w niej udział i opis ustalonego przebiegu wydarzeń.

8.2. Jeśli zostały zabezpieczone dowody cyberprzemocy, należy je również włączyć do dokumentacji (wydruki, opis, itp.).

9) Powiadomienie sądu rodzinnego

9.1. Jeśli rodzice/ prawni opiekunowie sprawcy cyberprzemocy odmawiają współpracy, a uczeń nie zaniechał dotychczasowego postępowania, dyrektor Ośrodka pisemnie informuje o zaistniałej sytuacji sąd rodzinny, szczególnie jeśli do szkoły napływają informacje o innych przejawach demoralizacji dziecka.

9.2. W sytuacji, gdy wykorzystane zostaną wszystkie dostępne środki wychowawcze (rozmowa z rodzicami, konsekwencje regulaminowe wobec ucznia, spotkania z pedagogiem, itp.), a ich zastosowanie nie przynosi pożądanych rezultatów, dyrektor powinien zwrócić się do sądu rodzinnego z zawiadomieniem o podjęcie odpowiednich środków wynikających z ustawy o postępowaniu w sprawach nieletnich.

9.3. W przypadku szczególnie drastycznych aktów cyberprzemocy - z naruszeniem prawa, dyrektor Ośrodka zobowiązany jest zgłosić te fakty policji i do sądu rodzinnego.

3. Reagowanie w sytuacji dostępu do treści szkodliwych, niepożądanych i nielegalnych.

Za treści szkodliwe, niedozwolone, nielegalne i niebezpieczne dla zdrowia uznaje się pornografię, treści obrazujące przemoc i promujące działania szkodliwe dla zdrowia i życia dzieci, popularyzujące ideologię faszystowską i działalność niezgodną z prawem, nawoływanie do samookaleczeń i samobójstw, korzystanie z narkotyków; niebezpieczeństwo werbunku dzieci i młodzieży do organizacji nielegalnych i terrorystycznych.

1) Ustalenie okoliczności zdarzenia, zabezpieczenie dowodów.

1.1. W przypadku pozyskania wiedzy o wystąpieniu zagrożenia dostępem do w/w treści, które można bezpośrednio powiązać z wychowankami Ośrodka, należy zabezpieczyć dowody w formie elektronicznej (pliki z treściami niedozwolonymi, zrzuty ekranu, zapisy rozmów w komunikatorach, e-maile,) znalezione w Internecie lub komputerze dziecka.

1.2. Zabezpieczenie dowodów leży po stronie rodziców dziecka. W czynnościach tych może wspomagać przedstawiciel Ośrodka, posiadający odpowiednie kompetencje techniczne.

1.3. Jeżeli treści szkodliwe, niedozwolone, nielegalne i niebezpieczne dla zdrowia nie mają związku z uczniami szkół Ośrodka, należy rozważyć zgłoszenie incydentu na policję oraz zgłosić go do serwisu Dyżurnet (dyzurnet.pl).

2) Identyfikacja sprawców.

2.1. Na podstawie zgromadzonych dowodów, należy zidentyfikować twórców treści oraz osoby, które udostępniły je dziecku.

2.2. Konieczne jest poinformowanie rodziców dzieci, uczestniczących w zdarzeniu, o sytuacji i roli ich dzieci.

3) Postępowania wobec sprawców zdarzenia.

3.1. W przypadku udostępniania przez ucznia treści szkodliwych, niedozwolonych/ nielegalnych i niebezpiecznych dla zdrowia należy przeprowadzić z nim rozmowę wychowawczą.

3.2. W sytuacji upowszechniania przez sprawców treści nielegalnych należy złożyć zawiadomienie o zdarzeniu na policję.

4) Postępowanie wobec ofiar zdarzenia.

4.1. Ofiary i świadkowie zdarzenia powinni być otoczeni opieką psychologiczno - pedagogiczną.

4.2. W trakcie rozmowy z dzieckiem należy ustalić okoliczności uzyskania przez ofiarę podejmowane działania i formę wsparcia dziecka.

5)Postępowanie wobec świadków zdarzenia.

5.1. W przypadku, gdy informacja na temat zdarzenia dotrze do środowiska rówieśniczego ofiary (klasy, szkoły, grupy wychowawczej), wskazane jest podjęcie działań edukacyjnych i wychowawczych.

6) Współpraca z instytucjami.

6.1. W sytuacji 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/ prawnymi opiekunami dziecka - niezwłocznie powiadomić policję.

6.2. Jeżeli ofiara potrzebuje opieki psychologicznej, decyzja o kontakcie z psychologiem i skierowaniu na terapię musi zostać podjęta w porozumieniu z rodzicami/ prawnymi opiekunami dziecka.

4. Reagowanie w sytuacji naruszenia prywatności dotyczącea nieodpowiedniego bądź niezgodnego z prawem wykorzystania danych osobowych lub wizerunku dziecka i pracownika szkoły.

Do najczęstszych form wyłudzenia lub kradzieży danych należy: przejęcie profilu na portalu społecznościowym w celu dyskredytacji lub naruszenia dobrego wizerunku ofiary (np. publikacja zdjęć intymnych bądź montowanych), szantażu (w celu uzyskania korzyści finansowych w zamian za niepublikowanie zdjęć bądź treści naruszających dobry wizerunek ofiary), dokonania zakupów i innych transakcji finansowych (np. w sklepach internetowych na koszt ofiary), uzyskania korzyści (np. usługi premium SMS).

1) Ustalenie okoliczności zdarzeni.

1.1. W przypadku, gdy sprawcą jest uczeń kolega ofiary ze szkoły czy klasy, uczniowie lub rodzice winni skontaktować się z dyrektorem Ośrodka, wychowawcą luklasy lub grupy

1. 2. W przypadku, gdy do naruszenia prywatności uczniów dochodzi ze strony dorosłych osób trzecich, rodzice/ prawni opiekunowie winni skontaktować się bezpośrednio z policją i powiadomić o tym Dyrektora/wicedyrektora Ośrodka

2) Analiza zdarzenia, zabezpieczenie dowodów.

2.1. Nauczyciel zabezpiecza dowody nieodpowiedniego lub niezgodnego z prawem działania w formie elektronicznej (e-mail, zrzut ekranu, konwersacja w komunikatorze lub SMS).

2.2. Równolegle dokonuje zmian tych danych identyfikujących, które zależą od ofiary, tj. haseł i loginów lub kodów dostępu do platform i portali internetowych, tak aby uniemożliwić kontynuację procederu naruszania prywatności - w działaniu tym ucznia i/lub jego rodzica powinien wspierać ASI.

2.3. W przypadku naruszenia dobrego wizerunku ofiary, należy wyjaśnić te działania i usunąć ich skutki.

2.4. Likwidacja stron internetowych czy profili w portalach społecznościowych, która wymagać będzie interwencji w zebrane dowody musi odbywać się za zgodą policji (o ile została powiadomiona).

2.5. Szczególnej uwagi wymagają incydenty kradzieży tożsamości w celu posłużenia się nią np. podczas zakupu towarów online lub dokonania transakcji finansowych. W tym przypadku należy skontaktować się ze sklepem lub pożyczkodawcą i wyjaśnić charakter zdarzenia.

3) Identyfikacja sprawców.

3.1. W przypadku, gdy dowody jasno wskazują na konkretnego sprawcę oraz na spełnienie przesłanki, iż sprawca zmierzał do wyrządzenia ofierze szkody majątkowej lub osobistej, należy je zabezpieczyć i przekazać policji. W przypadku, gdy trudno to ustalić, identyfikacji dokonać winna policja.

3.2. W przypadku znanego sprawcy, który jednak nie działał z powyższych pobudek, pracownicy Ośrodka powinni dążyć do rozwiązania problemu w ramach działań wychowawczo – edukacyjnych uzgodnionych z rodzicami/prawnymi opiekunami.

4) Postępowania wobec sprawców zdarzenia.

4.1. Gdy sprawcą incydentu jest wychowanek Ośrodka, należy wobec niego – w porozumieniu z rodzicami – podjąć działania wychowawcze (m.in. przeprosiny złożone osobie poszkodowanej), zmierzające do uświadomienia nieodpowiedniego i nielegalnego charakteru czynów, jakich dokonał.

4.2. Celem działań powinno być nabycie odpowiedniej wiedzy przez ucznia na temat wagi poszanowania prywatności w codziennym życiu, zmiana jego postawy na akceptującą szacunek dla wizerunku i prywatności. Działania takie należy podjąć niezależnie od powiadomienia policji/sądu rodzinnego.

4.3. Dyrektor Ośrodka podejmuje decyzję w sprawie powiadomienia o incydencie policji, biorąc pod uwagę wiek sprawcy, jego dotychczasowe zachowanie, postawę po odkryciu incydentu oraz opinie wychowawcy i pedagoga/psychologa.

4. 4. Przed podjęciem decyzji o zgłoszeniu incydentu na policję należy rozważyć, czy istnieją dowody, iż uczeń - sprawca zmierzał do wyrządzenia ofierze szkody majątkowej lub osobistej.

5) Postępowanie wobec ofiar zdarzenia.

5.1. Ofiary incydentów należy otoczyć – w porozumieniu z rodzicami - opieką pedagogiczno-psychologiczną i powiadomić o działaniach podjętych w celu usunięcia skutków działania sprawcy.

5. 2. Jeśli kradzież tożsamości, bądź naruszenie dobrego wizerunku ofiary, jest znane tylko jej i rodzicom, pracownicy Ośrodka powinni zapewnić poufność działań.

6) Postępowanie wobec świadków.

6.1. Gdy kradzież tożsamości, bądź naruszenie dobrego wizerunku ofiary jest znane szerszemu gronu uczniów, należy podjąć wobec nich działania wychowawcze, zwracające uwagę na negatywną ocenę naruszania wizerunku ucznia – koleżanki lub kolegi oraz ryzyko popełnienia czynu karalnego.

7) Współpraca z instytucjami.

7.1. Gdy naruszenie prywatności, czy wyłudzenie lub kradzież tożsamości skutkują wyrządzeniem ofierze szkody majątkowej lub osobistej, rodzice uczniów winni o nim powiadomić policję.

7.2. W przypadku konieczności podejmowania dalszych działań pomocowych wobec ofiary, można skierować ucznia, za zgodą i we współpracy z rodzicami, do placówki specjalistycznej np. terapeutycznej.

5. Postępowanie w sytuacji zagrożenia dla zdrowia dzieci w związku z nadmiernym korzystaniem z Internetu

Za treści szkodliwe i niebezpieczne dla zdrowia uznaje się infoholizm (siecioholizm) – nadmierne, obejmujące niekiedy niemal całą dobę korzystanie z zasobów Internetu i gier komputerowych (najczęściej sieciowych) oraz portali społecznościowych przez dzieci.

1) Przyjęcie zgłoszenia i ustalenie okoliczności zdarzenia.

1.1. Infoholizm stwierdza najczęściej rodzic dziecka. W przypadku konieczności podejmowania dalszych działań pomocowych można skierować ucznia, za zgodą i we współpracy z rodzicami, do placówki specjalistycznej, np. terapeutycznej.

1.2. Nauczyciele w szkole powinni zainteresować się przypadkami dzieci nieangażujących się w życie klasy, a poświęcających wolne chwile na kontakt online lub przychodzących do szkoły po nieprzespanej nocy.

3) Opis okoliczności, analiza, zabezpieczenie dowodów.

3.1. W przypadku pozyskania wiedzy o wystąpieniu zagrożenia reakcjapracowników Ośrodka powinna polegać na ustaleniu skutków zdrowotnych i psychicznych, jakie nadmierne korzystanie z zasobów Internetu wywołało u dziecka (np. gorsze oceny w nauce, niedosypianie, niedojadanie, rezygnacja z dawnych zainteresowań, załamanie się relacji z rodziną czy rówieśnikami).

3.2. Celem ustaleń jest wybór odpowiedniej ścieżki rozwiązywania problemu - z udziałem specjalistów (lekarzy, terapeutów) lub bez. W początkowej fazie popadania w uzależnienie od Internetu należy koncentrować się na wsparciu udzielonym w rodzinie i w Ośrodku (psycholog/pedagog, wychowawca).

4) Aktywności wobec ofiar zdarzenia.

4.1. W przypadku nadmiernego korzystania z Internetu przez uczniów należy otoczyć zindywidualizowaną opieką psychologiczno - pedagogiczną osobę, której problem dotyczy. Pierwszym jej etapem powinna być rozmowa ze specjalistą, która pozwoli zdiagnozować poziom zagrożenia, określić przyczyny popadnięcia w nałóg (np. sytuacja domowa, brak sukcesów edukacyjnych, izolacja w środowisku rówieśniczym) i ukazać specyfikę przypadku. Każdy uczeń, u którego podejrzewa się nałóg korzystania z Internetu powinno zostać profesjonalnie zdiagnozowane przez psychologa.

4.2. W trakcie wsparcia należy zapewnić komfort psychiczny - o jego sytuacji i specyfice uwarunkowań osobistych muszą zostać powiadomieni wszyscy uczący go i oceniających nauczycieli.

4.3. Konieczne jest powiadomienie rodziców/ prawnych opiekunów ucznia i omówienie z nimi wspólnych rozwiązań.

5) Aktywności wobec świadków.

5.1. Jeśli świadkami problemu są rówieśnicy ucznia, należy im w rozmowie zwrócić uwagę na negatywne aspekty nadmiernego korzystania z zasobów Internetu oraz zaapelować o codzienne wsparcie dla ucznia dotkniętego problemem.

6) Współpraca ze służbami i placówkami specjalistycznymi.

6. 1. W przypadku zdiagnozowania przez psychologa zaawansowanego uzależnienia od korzystania z zasobów Internetu uczeń powinien zostać skierowany, w bliskiej współpracy z rodzicami/ prawnymi opiekunami do placówki specjalistycznej oferującej program terapeutyczny z zakresu przeciwdziałania uzależnieniom.

6.2. W części przypadków może się okazać konieczna diagnoza i terapia lekarska.

6. Nawiązywanie niebezpiecznych kontaktów w Internecie - uwodzenie, zagrożenie pedofilią

1) Ustalenie okoliczności zdarzenia, zabezpieczenie dowodów:

1.1. Ważna w podejmowanych działaniach jest szybkość przeciwdziałania zagrożeniu ze względu na szkodliwe konsekwencje w świecie rzeczywistym.

1.2. Należy zidentyfikować i zabezpieczyć, w formie elektronicznej, dowody działania sprawcy oraz zawiadomić policję o wystąpieniu zdarzenia.

2) Identyfikacja sprawcy(-ów)

2.1. Ze względu na bezpieczeństwo nie należy podejmować samodzielnych działań w celu dotarcia do sprawcy, lecz udzielać wszelkiego możliwego wsparcia organom ścigania. Identyfikacja sprawcy wykracza poza kompetencje i możliwości pracowników Ośrodka.

3) Postępowanie wobec sprawców..

3.1. Nie należy podejmować aktywności zmierzających do kontaktu ze sprawcą.

3.2. Zadaniem pracowników Ośrodka jest zebranie dowodów oraz opieka nad ofiarą i świadkami.

4) Postępowanie wobec ofiar zdarzenia.

4.1. Pierwszą czynnością w ramach reakcji na zagrożenie jest otoczenie ofiary pomocą psychologiczno-pedagogiczną we współpracy z rodzicami/ prawnymi opiekunami.

4.2. W trakcie rozmowy z dzieckiem prowadzonej przez pracownika Ośrodka, do którego uczeń ma zaufanie, należy uzyskać wszelkie możliwe informacje o sprawcy i przekazać je policji.

4.3. Należy upewnić się, że kontakt ofiary ze sprawcą został przerwany, a uczeń odzyskał poczucie bezpieczeństwa. Dziecku należy udzielić profesjonalnej opieki terapeutycznej i/lub lekarskiej.

5) Postępowanie wobec świadków:

5.1. Jeżeli zgłaszającym zagrożenie był rówieśnik ofiary, należy również objąć go opieką psychologiczną.

6) Współpraca z instytucjami.

6.1. W przypadkach naruszenia prawa, obowiązkiem dyrektora Ośrodka jest powiadomienie policji lub sądu rodzinnego.

6. 2. Wskazane jest w porozumieniu z rodzicami – skierowanie ofiary na terapię do placówki specjalistycznej opieki psychologicznej.

7. Postępowanie w sytuacjach zagrożenia bezpieczeństwa technicznego sieci, komputerów i zasobów.

1. W przypadku wystąpienia incydentów zagrożenia bezpieczeństwa cyfrowego pracownik Ośrodka zobowiązany jest do zgłoszenia go osobie odpowiedzialnej za infrastrukturę cyfrową oraz dyrektorowi Ośrodka.

2. Kluczowe znaczenie ma zebranie i zabezpieczenie przez specjalistę dowodów w formie elektronicznej, z uwzględnieniem materialu umozliwiajacego identyfikację sprawcy.

3. Dyrektor Ośrodka zgłasza incydent na Policję.