Szkolny Plan Zapewnienia Bezpieczeństwa Cyfrowego

I. Wprowadzenie

II. Rodzaje cyberzagrożeń

III. Działania interwencyjne w przypadku wystąpienia zagrożenia bezpieczeństwa cyfrowego

IV. Procedury wobec poszczególnych incydentów zagrożenia bezpieczeństwa cyfrowego

- Dostęp do treści szkodliwych i nielegalnych
- Zagrożenia prywatności
- Cyberprzemoc
- Seksting, prowokacyjne zachowania i aktywność seksualna
- Nawiązywanie niebezpiecznych kontaktów w Internecie: uwodzenie, zagrożenie pedofilią
- Infoholizm: nadmierne korzystanie z Internetu

Szkolny Plan Zapewnienia Bezpieczeństwa Cyfrowego powstał zgodnie z zaleceniami Ministerstwa Edukacji Narodowej oraz w oparciu o Poradnik „Bezpieczna Szkoła: Zagrożenia i zalecane działania profilaktyczne w zakresie bezpieczeństwa fizycznego i cyfrowego uczniów”.

I. Wprowadzenie

Cel główny:

- Zapewnienie bezpieczeństwa uczniom w środowisku cyfrowym - wprowadzenie działań profilaktycznych, stworzenie procedur postępowania na wypadek pojawienia się cyberzagrożeń.

Zadania:

- Uświadomienie uczniów w temacie cyberzagrożeń, prowadzenie działań profilaktycznych, mających na celu zapewnienie bezpieczeństwa cyfrowego w szkole.

Cele szczegółowe:

- Zapewnienie aktualnej wiedzy na temat korzystania z zasobów Internetu.
- Kształtowanie postaw odpowiedzialnej aktywności w środowisku cyfrowym.
- Zapewnienie spójności prawidłowych zachowań w szkole, w przestrzeni publicznej i w domu rodzinnym.

II. Rodzaje cyberzagrożeń

Cyberzagrożenia można podzielić na:

1. Kontakty z nieodpowiednimi treściami (cyberpornografia, cyberprostytucja, seksting, sponsoring, treści propagujące niezdrowy tryb życia).
2. Niebezpieczne działania (cyberprzemoc, samobójstwa, które są inspirowane wpływem sieci).
3. Niebezpieczne kontakty (child grooming = uwodzenie dzieci online, cyberpedofilia).
4. Naruszenie prywatności (cyberstalking).
5. Zagrożenia seksualne (cyberseks, seksting).
6. Zespół uzależnienia od Internetu.
7. Cyberprzestępczość (kradzież danych osobowych, fałszywe pliki cookies zawierające szkodliwe oprogramowanie, ataki hakerskie (min. na sieci społecznościowe), tabnabbing = fałszywe witryny internetowe, clickjacking = maskowanie odnośnika w celu kliknięcia w link podsunięty przez przestępcę, zagrożenia systemów mobilnych).

III. Działania interwencyjne w przypadku wystąpienia zagrożenia bezpieczeństwa cyfrowego

1. W przypadku wystąpienia incydentu naruszenia bezpieczeństwa w cyberprzestrzeni, naruszenia prawa, należy szybko zidentyfikować problem, określić szkodliwe lub niezgodne z prawem zachowania. Rozwiązanie ma być adekwatne do poziomu zagrożenia, jakie wywołało w szkole.

2. Zadaniem Dyrektorów szkół oraz nauczycieli jest uwzględnienie kontekstu indywidualnych przypadków, a także ich szkolnego oraz środowiskowego tła i reagowanie adekwatne do poziomu odpowiedzialności i winy ucznia.

3. Działania interwencyjne dzielą się na:

- działania wobec aktu/zdarzenia - opis przypadku, ustalenie okoliczności zdarzenia, zabezpieczenie dowodów oraz monitoring pointerwencyjny,
- działania wobec uczestników zdarzenia (ofiara - sprawca - świadek, rodzice),
- działania wobec instytucji/organizacji/służb pomocowych i współpracujących – policji, wymiaru sprawiedliwości, służb społecznych.

4. Procedura reakcji w przypadku wystąpienia zagrożenia bezpieczeństwa cyfrowego:

- rozmowa uczestników zdarzenia z Dyrektorem szkoły,
- powiadomienie rodziców/opiekunów poszkodowanego dziecka oraz rodziców/opiekunów sprawcy zdarzenia,
- działania wychowawcze i wyciągnięcie konsekwencji wobec sprawcy,
- powiadomienie policji/sądu rodzinnego w przypadku naruszenia prawa,
- udzielenie uczestnikom zdarzenia wsparcia psychologicznego.

5. Niezbędna jest współpraca szkoły z zewnętrznymi instytucjami/organizacjami/służbami pomocowymi w przypadku naruszenia przepisów prawa przez uczniów lub osoby spoza szkoły. Szkoła współpracuje z:

- policją i sądami rodzinnymi,
- służbami społecznymi i placówkami specjalistycznymi,
- dostawcami usług internetowych oraz operatorami telekomunikacyjnymi.

6. Sprawców wszystkich rodzajów zagrożeń bezpieczeństwa cyfrowego w szkole należy objąć poniższymi działaniami:

- sprawca musi otrzymać komunikat o braku akceptacji dla działań jakich dokonał,
- musi poznać możliwe skutki i konsekwencje swojego postępowania (np. wynikające ze Statutu szkoły i/lub Regulaminu szkoły lub kontraktu),
- powinien zostać wezwany do zaprzestania podejmowania podobnych działań w przyszłości oraz usunięcia skutków swoich dotychczasowych działań (np. publikacji na portalu społecznościowym),
- powinien zostać objęty pomocą psychologiczno-pedagogiczną by podobne zdarzenia nie miały miejsca w przyszłości,
- w przypadku, kiedy sprawców jest więcej, należy z każdym z nich rozmawiać osobno,

- decyzję o konsekwencjach zdarzenia dla sprawcy, powinna podejmować Rada Pedagogiczna lub wyznaczony przez Dyrektora szkoły Zespół ds. cyberzagrożeń,
- decyzję przekazywać powinien Dyrektor szkoły.

7. Celem sankcji wobec sprawcy jest zatrzymanie jego działań i zapewnienie poczucia bezpieczeństwa ofierze oraz zmiana postawy sprawcy. Sankcje mają na celu także pokazanie społeczności szkolnej, że działania sprawcy nie będą tolerowane i że szkoła jest w stanie skutecznie zareagować w tego rodzaju sytuacjach.

8. Rola pedagoga szkolnego lub psychologa szkolnego ogranicza się do podjęcia interwencji oraz udzielenia pomocy psychologiczno-pedagogicznej. Pedagog szkolny oraz psycholog szkolny nie wchodzą w skład Zespołu ds. cyberzagrożeń.

9. Decyzję o konsekwencjach dla sprawcy zdarzenia podejmuje powołany przez Dyrektora szkoły Zespół, po poznaniu się ze wszystkimi okolicznościami zdarzenia, a przekazuje Dyrektor szkoły.

10. Sankcja wymierzona wobec sprawcy ma na celu zatrzymanie jego działań i zapewnienie poczucia bezpieczeństwa ofierze oraz wpływ na zmianę postawy sprawcy. Pokazanie społeczności szkolnej, że takie działania nie są tolerowane i że szkoła skutecznie reaguje w tego rodzaju sytuacjach.

11. Wpływ na decyzję o sankcjach ma:

- rozmiar i ranga szkody,
- czas trwania,
- świadomość popełnianego czynu,
- motywacja sprawcy.

12. Rodzice czy opiekunowie prawni sprawcy powinni zostać poinformowani o zdarzeniu, zapoznani z materiałami i przewidywanymi konsekwencjami oraz poinformowani o tym, że rodzice ofiary mają prawo zgłosić sprawę na policję.

13. W przypadku, gdy sprawca pochodzi spoza szkoły, należy zapewnić bezpieczeństwo ofierze i poinformować ją oraz rodziców/prawnych opiekunów o przysługujących jej prawach zgłoszenia przestępstwa na policję. Należy nawiązać współpracę między placówkami do której uczęszcza lub znajduje się sprawca i wspólnie rozwiązać kryzysową sytuację.

14. Telefony/ kontakty alarmowe krajowe:

- Zgłaszanie nielegalnych treści: dyzurnet@dyzurnet.pl, tel.801615 005
- Policja 997 lub 112
- Telefon Zaufania dla Dzieci i Młodzieży - 116 111
- Telefon dla Rodziców i Nauczycieli w sprawie Bezpieczeństwa Dzieci – 800 100 100, dyzurnet@dyzurnet.pl

IV. Procedury wobec poszczególnych incydentów zagrożenia bezpieczeństwa cyfrowego

Kontakty z nieodpowiednimi treściami (cyberpornografia, cyberprostytucja, seksting, sponsoring, treści propagujące niezdrowy tryb życia)

Podstawy prawne: Kodeks karny, art. 200 § 1–5 kk, art. 200a kk, art. 200b kk, art. 202 § 1-4b, art. 256 kk, art. 257.I.

Dostęp do treści szkodliwych i nielegalnych

1. Należy zabezpieczyć szkodliwe treści w formie dowodów elektronicznych z pomocą rodziców/prawnych opiekunów oraz w razie konieczności przedstawiciela szkoły, który posiada odpowiednie kompetencje techniczne.

2. Jeżeli dane treści można powiązać bezpośrednio z uczniami jednej szkoły - rozwiązanie leży po stronie szkoły, a o danym zdarzeniu i roli uczniów powinni zostać poinformowani wszyscy rodzice/prawni opiekunowie. Jeżeli natomiast treści nielegalne lub szkodliwe nie mają związku z uczniami danej szkoły - należy rozważyć poinformowanie policji (numer alarmowy: 112, 997) oraz serwisu www.dyzurnet.pl

3. W przypadku, gdy w udostępnianiu szkodliwych lub nielegalnych treści biorą udział inni rówieśnicy, konieczne jest poinformowanie wszystkich rodziców/prawnych opiekunów o danym zajściu. W przypadku upowszechnienia przez sprawcę treści nielegalnych (np. dziecięcej pornografii) konieczne jest zawiadomienie policji.

4. Uczniów (ofiary i świadków) należy otoczyć opieką psychologiczno-pedagogiczną. Należy ustalić okoliczności uzyskania szkodliwych treści oraz zadbać o komfort psychiczny uczniów oraz poszanowanie ich poufności oraz podmiotowości (takie zdarzenie może mieć bardzo silny wpływ na ich psychikę). Należy uzgodnić z rodzicami/ prawnymi opiekunami formy działania oraz wsparcia uczniów oraz sposób w jaki doszło do incydentu.

5. Jeżeli informacje o incydencie dotrą do środowiska ucznia (klasa, szkoła), należy podjąć działania edukacyjne i wychowawcze.

6. W przypadku 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.

7. Jeżeli zaistnieje potrzeba skorzystania przez ofiarę za specjalistycznej opieki psychologicznej, decyzja o jej udzieleniu powinna zostać podjęta w porozumieniu z jego rodzicami/prawnymi opiekunami.

Zagrożenia prywatności

Podstawy prawne: Kodeks karny, art.190a, RODO

Zagrożenie prywatności polega na naruszeniu prywatności dziecka lub pracownika szkoły poprzez nieodpowiednie lub niezgodne z prawem wykorzystanie danych osobowych lub wizerunku dziecka i pracownika szkoły. Jest to często przejęcie profilu na portalu społecznościowym w celu dyskredytacji lub naruszenia wizerunku ofiary, szantażowania, dokonania zakupów i innych transakcji finansowych, podszywanie się pod inną osobę

lub wykorzystywanie jej wizerunku czy danych. Działania te są przestępstwem na podstawie art.190a § 2 Kodeksu karnego.

Sposób postępowania w przypadku wystąpienia zagrożenia:

1. W pierwszej kolejności należy zabezpieczyć dowody nieodpowiedniego działania (e-mail, zrzut ekranu, adres strony internetowej, SMS, konwersacja w komunikatorze) oraz dokonać zmian danych identyfikujących, które należą do ofiary (hasła, loginy).

2. Jeżeli sprawcą naruszenia prywatności jest uczeń - osoba pokrzywdzona/rodzice powinni zgłosić się do Dyrektora szkoły, wychowawcy lub osoby odpowiedzialnej za koordynowanie działań związanych z bezpieczeństwem cyfrowym na terenie szkoły. Jeżeli zebrane dowody jednoznacznie wskazują na to, iż sprawca dążył do wyrządzenia ofierze szkody majątkowej lub osobistej, należy je zabezpieczyć i przekazać policji.

3. W przypadku gdy sprawcą naruszenia prywatności jest osoba dorosła lub osoba trzecia, rodzice powinni skontaktować się bezpośrednio z policją i powiadomić szkołę.

4. Jeżeli sprawcą incydentu jest uczeń szkoły, należy skonsultować się z rodzicami i podjąć wobec niego działania wychowawcze, które uświadomią mu charakter jego nieodpowiedzialnych i nielegalnych czynów. Osoba poszkodowana winna otrzymać zadośćuczynienie. Działania te szkoła powinna podjąć niezależnie od powiadomienia policji lub sądu, gdyż celem nadrzędnym jest trwała zmiana postawy ucznia na prezentującą szacunek wobec cudzego wizerunku i prywatności.

5. Dyrekcja powinna podjąć decyzję w sprawie powiadomienia policji w oparciu o rodzaj czynu, wiek sprawcy, jego dotychczasowe zachowanie, postawę po odkryciu incydentu, opinie wychowawcy i pedagoga szkolnego.

6. Nieletnia ofiara incydentu powinna być otoczona (w porozumieniu z rodzicami/opiekunami prawnymi) opieką psychologiczno-pedagogiczną. Należy ją również powiadomić o działaniach podjętych w celu usunięcia skutków działania sprawcy (usunięcie z Internetu nieodpowiednich treści, zablokowanie konta w serwisie społecznościowym).

7. W sytuacji gdy o danym zajściu (kradzież tożsamości, naruszenie dobrego imienia) wiedzą tylko ofiara, jej rodzice i szkoła, władze szkolne powinny zapewnić poufność działań.

8. W przypadku naruszenia dobrego imienia ofiary w gronie uczniów, należy podjąć wobec nich działania wychowawcze - negatywna ocena narażania na uszczerbek wizerunku ucznia oraz odpowiedzialność prawna.

9. W przypadku gdy naruszenie prywatności lub wyłudzenie czy kradzież tożsamości skutkują wyrządzeniem ofierze szkody majątkowej lub osobistej, rodzice ucznia powinni o tym fakcie powiadomić policję.

10. W razie konieczności ofiarę można skierować (za zgodą i we współpracy z rodzicami/prawnymi opiekunami) do placówki specjalistycznej.

Cyberprzemoc

Podstawy prawne: Kodeks karny: art.190 § 1–2, art. 190a § 1–3, art. 212 § 1–2, art. 256, art. 267 § 1–4, art. 268a.

Cyberprzemoc to seria agresywnych zachowań z użyciem technologii informacyjnych i komunikacyjnych, celowo i regularnie skierowanych przeciwko bezbronnej osobie. Podstawowe formy to: nękanie, straszenie, szantażowanie z użyciem sieci, publikowanie lub rozsyłanie ośmieszających, kompromitujących informacji, zdjęć, filmów. Może też być bardziej zawoalowana: polegać na wykluczeniu z grupy, manipulowaniu czy nienawiązywaniu relacji. 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:

1. Z należytym spokojem należy wysłuchać osobę, która zgłasza akt cyberprzemocy i okazać jej wsparcie w atmosferze bezpieczeństwa oraz miejscu, zapewniającym intymność. Należy zebrać informację dotyczącą zdarzenia, sporządzić notatkę oraz określić czy faktycznie posiada ono znamiona cyberprzemocy.

2. Należy ustalić czynności i charakter zdarzenia: zabezpieczyć dowody związane z aktem cyberprzemocy (np. kopia materiałów wraz z datą i kopią jej otrzymania, zapisać dane nadawcy, adresy stron www, historię połączeń itd.).

3. Na podstawie zebranych informacji i materiałów dowodowych należy w miarę możliwości zidentyfikować sprawcę. Ofiara często domyśla się kto stosuje wobec niej cyberprzemoc. Jeżeli ustalenie sprawcy nie jest możliwe, a w ocenie nauczycieli jest to konieczne, należy skontaktować się z policją. Należy pamiętać, że czyny karalne ścigane z urzędu powinny być niezwłocznie zgłoszone na policję lub do prokuratury. Dotyczy to sytuacji takich jak rozpowszechnianie zdjęć lub filmów z udziałem osoby nieletniej, mających cechy pornograficzne, czy publikowanie materiałów prezentujących seksualne wykorzystywanie nieletnich.

4. Działania wobec sprawców cyberprzemocy ze szkoły:

- pedagog przeprowadza rozmowę dyscyplinującą dotyczącą nagannego zachowania ucznia. Ma ona na celu ustalenie okoliczności zdarzenia, analizę zaistniałej sytuacji (powodów i motywów działania) oraz próbę naprawienia sytuacji konfliktowej,
- sprawcy cyberprzemocy powinna być wymierzona kara, którą przewidują wewnętrzne przepisy szkoły (Statut szkoły, regulaminy).

5. Działania wobec sprawcy cyberprzemocy spoza szkoły — w sytuacji, gdy sprawca jest nieznany, podstawowe działanie polega na: przerwaniu aktu cyberprzemocy (zawiadomieniu administratora serwisu w celu usunięcia materiału po wcześniejszym zabezpieczeniu dowodów) oraz ewentualnym zgłoszeniu sprawy Policji.

6. Szkoła powinna powiadomić odpowiednie służby (np. sąd rodzinny), gdy wykorzysta wszystkie dostępne jej środki wychowawcze (rozmowa z rodzicami, konsekwencje z statutu wobec ucznia) i interwencje pedagogiczne, a ich zastosowanie nie przyniosą niepożądanych rezultatów (zmiany w zachowaniu ucznia).

7. Kontaktu z policją wymagają wszelkie sytuacje, w których zostało naruszone prawo (np. groźby karalne, świadome publikowanie nielegalnych treści rozpowszechnianie nagich zdjęć z udziałem małoletnich). Za zgłoszenie odpowiada Dyrektor szkoły.

8. Działania wobec ofiar zdarzenia:

- udzielenie wsparcia ofierze przez specjalistów pomocy psychologiczno-pedagogicznej — musi się ona czuć bezpieczna i otoczona opieką dorosłych,
- poinformowanie ucznia o krokach, jakie może podjąć szkoła i sposobach, w jaki może zapewnić mu bezpieczeństwo,
- omówienie strategii postępowania wobec sprawcy (np. zerwanie kontaktu ze sprawcą, niepodejmowanie agresywnej konfrontacji itp.),
- monitorowanie sytuacji, np. zwrócenie uwagi, czy nie są podejmowane wobec niej dalsze działania przemocowe, obserwowanie, jak sobie radzi w grupie po ujawnieniu incydentu cyberprzemocy,
- włączenie rodziców/opiekunów prawnych w działania wobec ofiary – trzeba na bieżąco ich informować o sytuacji, zaproponować pomoc specjalisty (np. psycholog szkolny, poradnia psychologiczno-pedagogiczna) oraz przekazać informację o możliwości zgłoszenia sprawy policji.

Seksting, prowokacyjne zachowania i aktywność seksualna

Podstawy prawne: Kodeks karny – art. 191a, art. 202 § 1–4c.

Seksting to przesyłanie wiadomości drogą elektroniczną w formie wiadomości MMS lub z wykorzystaniem różnych aplikacji i komunikatorów albo publikowanie np. na portalach (społecznościowych) prywatnych treści, głównie zdjęć lub filmów, o kontekście seksualnym, erotycznym. Występują 3 rodzaje sekstingu:

1. Wymiana materiałów o charakterze seksualnym następuje tylko w ramach związku między dwojgiem rówieśników. Materiały nie uległy rozprzestrzenieniu dalej. Należy wezwać uczniów do dyrekcji szkoły, gdzie przedstawione im zostaną dowody ich aktywności. Konieczne jest również przeprowadzenie rozmów w obecności rodziców uczniów oraz uświadomienie, że rozpowszechnianie materiałów dalej jest nielegalne i będzie miało ostrzejsze konsekwencje, w tym prawne.

2. Materiały o charakterze seksualnym zostały rozesłane większej liczbie osób, jednak nie dochodzi do cyberprzemocy na tym tle. Młodzież traktuje materiał jako formę wyrażenia siebie. Należy powiadomić policję lub sąd rodzinny ze względu na pornograficzny charakter materiałów. Wszelkie działania wobec sprawców incydentu powinny być podejmowane w porozumieniu z ich rodzicami lub opiekunami prawnym.

3. Materiały zostały rozesłane większej liczbie osób (bez względu na intencje) i na tym tle dochodzi do cyberprzemocy. Należy zastosować procedury dotyczące cyberprzemocy. Każdy z tych rodzajów sekstingu uruchamia zmodyfikowane procedury reagowania. Za każdym razem, niezależnie od zakresu negatywnych zachowań, należy udzielić uczniom wsparcia pedagogicznego i psychologicznego oraz współpracować z rodzicami uczniów.

W przypadku publikacji lub upowszechniania zdjęć o charakterze pornografii dziecięcej, jako wykroczenie ścigane z urzędu Dyrektor jest zobowiązany jest do powiadomienia o tym zdarzeniu policji lub sądu rodzinnego.

Kontakt ofiar z placówkami specjalistycznymi może okazać się konieczny w indywidualnych przypadkach. O skierowaniu do nich decyzję powinien podjąć psycholog czy pedagog szkolny wspólnie z rodzicami/opiekunami prawnymi ofiary.

Nawiązywanie niebezpiecznych kontaktów w Internecie – uwodzenie, zagrożenie pedofilią

Podstawy prawne: Kodeks karny, art. 200, art. 200a. § 1 i 2, art. 286 § 1.

Niebezpieczne kontakty w Internecie to m.in. kontakt osób dorosłych z małoletnimi w celu: wyłudzenia poufnych informacji lub własności (danych, pieniędzy, cennych przedmiotów rodzinnych), nawiązania kontaktów seksualnych, szantażu, chęci kidnappingu lub skłonienia do zachowań niebezpiecznych dla zdrowia i życia.

1. Osobami najczęściej zgłaszającymi omawiany problem są rodzice/opiekunowie prawni lub osoby, zajmujące się ściganiem „pedofili". W pierwszym przypadku informacja trafia najpierw do szkół, w drugim – na policję. Zdarza się, że informacja uzyskiwana jest ze środowiska rówieśników ofiary.

2. W działaniach szkoły kluczowym znaczeniem jest czas reakcji, czyli szybkie przeciwdziałanie zagrożeniu ze względu na szkodliwe konsekwencje realizacji kontaktu *online*, przeradzającego się w zachowania w świecie rzeczywistym gdyż istnieje duże prawdopodobieństwo zagrożenia życia lub zdrowia dziecka oraz przymus realizacji czynności seksualnych.

3. Należy zawiadomić policję o wystąpieniu zdarzenia, udzielić wszelkiego możliwego wsparcia organom ścigania, m.in. zabezpieczyć i przekazać zebrane dowody (tj. zapisy rozmów w komunikatorach, na portalach społecznościowych; zrzuty ekranowe, zdjęcia, wiadomości e-mail).

4. Nie należy podejmować aktywności zmierzających do kontaktu ze sprawcą. Zadaniem szkoły jest zebranie dowodów i opieka nad ofiarą i ewentualnymi świadkami.

5. W przypadku reakcji na zagrożenie, zaobserwowania antyzdrowotnych i zagrażających życiu zachowań, ofiarę należy objąć pomocą psychologiczno-pedagogiczną, zapewnić komfort psychiczny i poczucie bezpieczeństwa. Do pomocy powinny być zaangażowane osoby do których ofiara ma zaufanie np. wychowawca, pedagog szkolny, psycholog szkolny. Należy również upewnić się, że kontakt ofiary ze sprawcą został przerwany. Wszelkie działania szkoły wobec dziecka winny być uzgadniane z rodzicami/opiekunami prawnymi i inicjowane za ich zgodą.

6. Trzeba zbadać sytuację domową dziecka i zastanowić się czy nie tkwi w niej źródło poszukiwania kontaktów w Internecie.

7. Jeżeli zgłaszającym zagrożenie lub jego świadkiem był rówieśnik ofiary, należy również objąć go opieką psychologiczną, pozytywnie wzmacniając jego reakcję na zdarzenie we współpracy z rodzicami/opiekunami prawnymi.

8. W przypadku, kiedy doszło do naruszenia prawa (uwiedzenie dziecka do lat 15) szkoła ma obowiązek powiadomić policję lub sąd rodzinny. W porozumieniu z rodzicami/opiekunami prawnymi rekomenduje się skierowanie ofiary na terapię do placówki specjalistycznej opieki psychologicznej.

Nadmierne korzystanie z INTERNETU

Podstawy prawne: Ustawa z dnia 14 grudnia 2016 r. Prawo oświatowe Dz.U.2020, poz.910, z późn. zm.

Infoholizm (siecioholizm) to nadmierne, obejmujące niekiedy niemal całą dobę, korzystanie z zasobów internetu i gier komputerowych oraz portali społecznościowych przez dzieci. Jego negatywne efekty to: pogarszanie się stanu zdrowia fizycznego, psychicznego, zaniedbywanie codziennych czynności oraz osłabianie relacji rodzinnych i społecznych.

Sposób postępowania w przypadku wystąpienia zagrożenia:

1. W przypadku wystąpienia nadmiernego korzystania z komputera lub podejrzeń infoholizmu konieczne jest podjęcie działań pomocowych – skierowanie ucznia do placówki specjalistycznej za zgodą rodziców/prawnych opiekunów.

2. Szkoła wraz z rodzicami powinna ustalić skutki zdrowotne i psychiczne wywołane przez nadmierne korzystanie z zasobów Internetu (np. gorsze wyniki w nauce, niedosypianie, niedojadanie...) - ma to na celu wybór odpowiedniej ścieżki rozwiązania problemu.

3. Nauczyciele powinni zwrócić uwagę na dzieci nieangażujące się w życie klasy i poświęcające wolny czas na kontakt online lub przychodzącymi do szkoły po nieprzespanej nocy.

4. Osoba, która ma problem z infoholizmem powinna zostać otoczona zindywidualizowaną opieką pedagoga/psychologa szkolnego, który powinien przeprowadzić z nią (i rodzicami) wywiad w celu określenia sytuacji i wstępnego ustalenia poziomu zagrożenia, a następnie proponuje się kontakt ze specjalistą. Dziecku należy zapewnić komfort psychiczny, a o jego sytuacji i specyfice uwarunkowań osobistych powinni wiedzieć wszyscy uczący i oceniający go nauczyciele. Należy również omówić wspólne rozwiązanie danej sytuacji z rodzicami/prawnymi opiekunami ucznia.

5. W przypadku zdiagnozowania przez psychologa uzależnienia od Internetu, uczeń powinien zostać skierowany (w porozumieniu z rodzicami/prawnymi opiekunami) na program terapeutyczny do specjalnej placówki specjalistycznej.

6. Jeśli inni uczniowie są świadkami problemu, należy zwrócić ich uwagę na negatywne skutki nadmiernego korzystania z zasobów Internetu oraz zaapelować o wsparcie ucznia dotkniętego problemem.