**Procedura postępowania w przypadku wystąpienia cyberprzemocy**

**w Zespole Szkół im. Jadwigi Grodzkiej w Łęczycy**

Procedury opracowano na podstawie dokumentu Bezpieczna Szkoła wydanego przez Departament Wychowania i Kształcenia Integracyjnego Ministerstwa Edukacji Narodowej jako zbiór rekomendacji i wytycznych dla dyrektorów szkół i organów prowadzących szkoły, do realizacji począwszy od września 2017r**.**

**1. Podstawowe działania na rzecz bezpieczeństwa cyfrowego w szkole.**

Systematycznie prowadzone działania profilaktyczne w znacznej mierze ograniczają zakres zagrożeń uczniów występujących w cyberprzestrzeni, nie są jednak w stanie ich całkowicie wyeliminować.   
**W przypadkach wystąpienia incydentu naruszenia bezpieczeństwa, zwłaszcza wobec naruszenia prawa, działania szkoły cechować powinna otwartość w działaniu, szybka identyfikacja problemu - określenie szkodliwych lub niezgodnych z prawem zachowań -   
i jego rozwiązywanie adekwatnie do poziomu zagrożenia, jakie wywołało w szkole.**

Zagrożenia bezpieczeństwa cyfrowego w szkole oraz problemy ucznia w świecie cyfrowym mogą mieć różnorodny charakter. Warto przy tym podkreślić, iż nie istnieje „złota recepta”, którą zastosować można we wszystkich przypadkach wystąpienia zagrożeń spowodowanych przez uczniów. Dyrektor i nauczyciele uwzględniają kontekst indywidualnych przypadków,   
a także ich szkolne i środowiskowe tło i starają się reagować adekwatnie do poziomu odpowiedzialności i winy ucznia.

**Obligatoryjne działania interwencyjne**, będące następstwem wystąpienia zagrożenia, dzielimy na 3 grupy:

1) **działania wobec aktu/zdarzenia** - opis przypadku, ustalenie okoliczności zdarzenia, zabezpieczenie dowodów oraz monitoring pointerwencyjny

2) **działania wobec uczestników zdarzenia** (ofiara **-** sprawca **-** świadek, rodzice)

3) **działania wobec instytucji/organizacji/służb pomocowych i współpracujących** – Policji, wymiaru sprawiedliwości, służb społecznych.

**Na każdą procedurę reakcji na wystąpienie danego typu zagrożenia cyberbezpieczeństwa w szkole muszą składać się działania podjęte przez dyrekcję szkoły oraz nauczycieli, pedagogów/psychologów szkolnych.**

**Działania wobec zdarzenia** polegają przede wszystkim na zachowaniu (nie usuwaniu) dokumentacji cyfrowej: wiadomości sms, e-maili, nagrań z poczty głosowej telefonu, komentarzy w serwisie społecznościowym, zapisów w blogu i plików filmów wideo. O ile to możliwe, należy także zarchiwizować treść rozmów w komunikatorach oraz linki (konkretne adresy URL) oraz danych o potencjalnym sprawcy. Każde zdarzenie wymaga udokumentowania w stosownym protokole.

Przez **działania na rzecz uczestników zdarzenia** rozumie się aktywności podejmowane wobec **ofiar** (osób poszkodowanych), **sprawców** i **świadków zdarzenia.** W szkole osobami poszkodowanymi będą w przeważającym odsetku przypadków dzieci (nieletni). Dlatego jako kolejną grupę pośrednich uczestników zdarzenia wyróżniamy ich rodziców.

Standardowa procedura reakcji w przypadku wystąpienia zagrożenia bezpieczeństwa cyfrowego zaprezentowana jest poniżej:

1. **Rozmowa uczestnika zdarzenia z kierownictwem szkoły**
2. **Powiadomienie rodziców/opiekunów poszkodowanego dziecka**
3. **Działania wychowawcze i wyciągnięcie konsekwencji wobec sprawcy**
4. **Powiadomienie Policji/ sądu rodzinnego w przypadku naruszenia prawa**
5. **Udzielenie uczestnikom zdarzenia wsparcia psychologicznego**

*Źródło: Agnieszka Wrońska, Zuzanna Polak,* Standard bezpieczeństwa online placówek oświatowych, str.25 *NASK, 2015*

**Działania szkoły adresowane do instytucji i organizacji zewnętrznych** są niezbędne w przypadku naruszenia przepisów prawa przez uczniów lub osoby spoza szkoły5.   
Pośród nich należy wyróżnić szczególnie współpracę z: (1) Policją i sądami rodzinnymi,   
(2) służbami społecznymi i placówkami specjalistycznymi oraz (3) dostawcami usług internetowych oraz operatorami telekomunikacyjnymi.

Sprawców wszystkich rodzajów zagrożeń bezpieczeństwa cyfrowego w szkole należy objąć , co najmniej poniższymi działaniami:

1) Sprawca musi otrzymać od przedstawicieli szkoły komunikat o braku akceptacji dla działań, jakich dokonał. W trakcie takiej rozmowy uczeń powinien poznać możliwe skutki swojego postępowania, a także konsekwencje, jakie mogą zostać wobec niego wyciągnięte (np. wynikające z statutu i/lub regulaminu szkoły lub wprowadzonego kontraktu-umowy). W trakcie rozmowy sprawca powinien zostać wezwany do zaprzestania podejmowania podobnych działań w przyszłości, w tym usunięcia skutków swoich działań (np. publikacji w portalu społecznościowym). Sprawca powinien również zostać objęty odpowiednią pomocą psychologiczną-pedagogiczną w celu zrozumienia konsekwencji jego zachowania oraz zmianie postawy i dalszego postępowania. Jeśli sprawców jest więcej, to z każdym z nich należy rozmawiać osobno.

2) Należy zadbać o to, żeby osoba reprezentująca szkołę (psycholog/pedagog, wychowawca) ograniczała się do podjęcia interwencji, a nie wymierzała karę. Decyzję o tym, jaką karę wymierzyć sprawcy, powinna podejmować rada pedagogiczna (po poznaniu wszystkich okoliczności zdarzenia), a przekazywać dyrektor szkoły. Ważne jest zatem oddzielenie osoby psychologa/pedagoga, nawiązującego relację z uczniem, od organu wymierzającego karę.

Celem sankcji wobec sprawcy jest przede wszystkim: 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 sytuacji. Podejmując decyzję o sankcjach, należy wziąć pod uwagę:

**- rozmiar i rangę szkody** –np. czy w przypadku cyberprzemocy materiał został upubliczniony w sposób pozwalający na dotarcie do niego wielu osobom (określa to rozmiar upokorzenia, jakiego doznaje ofiara), czy trudno jest wycofać materiał z sieci itp.

- **czas trwania prześladowania** –czy było to długotrwałe działanie, czy pojedynczy incydent

**- świadomość popełnianego czynu** –czy działanie było zaplanowane, a sprawca był świadomy, że postąpił nagannie np. czy wie, że wyrządza krzywdę koledze, jak wiele wysiłku włożył w ukrycie swojej tożsamości itp.

- **motywację sprawcy** –należy sprawdzić, czy działanie sprawcy nie jest działaniem odwetowym w odpowiedzi na uprzednie doświadczenia sprawcy.

Aktywność wobec sprawcy powinna także obejmować rozmowę z jego rodzicami lub opiekunami prawnymi –powinni oni zostać poinformowani o zdarzeniu, zapoznani z materiałami oraz decyzją na temat dalszego postępowania ze sprawcą (np. na temat sankcji). Warto, aby rodzice współpracowali ze szkołą w zakresie rozwiązywania sytuacji kryzysowej, aby stali się jej sojusznikami a nie przeciwnikami. Rodzice sprawcy powinni również zostać poinformowani, że rodzice ofiary mają prawo zgłosić sprawę na Policję.

Jeśli sprawca pochodzi spoza szkoły, należy zapewnić bezpieczeństwo ofierze i poinformować ją (jej rodziców) o przysługujących jej prawach (np. zgłoszenie popełnienie przestępstwa na Policję). Jeśli sprawca jest z innej szkoły, należy rozważyć nawiązanie współpracy między placówkami i wspólne rozwiązanie kryzysowej sytuacji.

**2. Procedury na wypadek wystąpienia zagrożeń bezpieczeństwa cyfrowego.**

Wyróżnia się 2 podstawowe zagrożenia bezpieczeństwa cyfrowego w środowisku szkolnym, którym przypisano opracowane według jednego standardu opisu procedury reagowania.

|  |  |
| --- | --- |
| 1. | Dostęp do treści szkodliwych, niepożądanych i nielegalnych |
| Podstawy prawne uruchomienia procedury | Kodeks Karny, Statut szkoły |
| Rodzaj zagrożenia objętego procedurą | Zagrożenie łatwym dostępem do treści szkodliwych, niedozwolonych, nielegalnych i niebezpiecznych dla zdrowia (pornografia, 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, korzystania z narkotyków; niebezpieczeństwo werbunku dzieci i młodzieży do organizacji nielegalnych i terrorystycznych) |
| Telefony/kontakt alarmowe krajowe | Zgłaszanie nielegalnych treści:  dyzurnet@dyzurnet.pl, tel. 801 615 005, Policja 997 |
| Sposób postępowania w przypadku wystąpienia zagrożenia | |
| Opis okoliczności, analiza, zabezpieczenie dowodów | Reakcja szkoły w przypadku pozyskania wiedzy o wystąpieniu zagrożenia będzie zależna od tego, czy: (1) treści te można bezpośrednio powiązać z uczniami danej szkoły, czy też (2) treści nielegalne lub szkodliwe nie mają związku z uczniami danej szkoły, lecz wymagają kontaktu szkoły z odpowiednimi służbami.  W pierwszej kolejności należy zabezpieczyć dowody w formie elektronicznej (pliki z treściami niedozwolonymi, zapisy rozmów w komunikatorach, e-maile, zrzuty ekranu), znalezione w Internecie lub w komputerze dziecka. Zabezpieczenie dowodów jest zadaniem rodziców lub opiekunów prawnych dziecka, w czynnościach tych może wspomagać ich przedstawiciel szkoły posiadający odpowiednie kompetencje techniczne. W przypadku sytuacji (1) rozwiązanie leży po stronie szkoły, zaś (2) należy rozważyć zgłoszenie incydentu na Policję oraz zgłosić go do serwisu Dyżurnet (dyzurnet.pl). |
| Identyfikacja sprawcy(ów) | W identyfikacji sprawców kluczowe znaczenie odgrywać będą zgromadzone dowody. W procesie udostępniania nielegalnych i szkodliwych treści małoletnim występują na ogół: twórca treści (np. pornografii) oraz osoby, która udostępniły je dziecku. Często osobami tymi są rówieśnicy – uczniowie tej samej szkoły czy klasy, dzieci sąsiadów. Konieczne jest poinformowanie wszystkich rodziców lub opiekunów dzieci uczestniczących w zdarzeniu o sytuacji i roli ich dzieci. |
| Działania wobec sprawców zdarzenia ze szkoły/spoza szkoły | W przypadku udostępniania (szerowania, dzielenia się) treści opisanych wcześniej jako szkodliwych/niedozwolonych/ nielegalnych i niebezpiecznych dla zdrowia przez ucznia należy przeprowadzić z nim rozmowę na temat jego postępowania  i w jej trakcie uzmysłowić mu szkodliwość prowadzonych przez niego działania. Działania szkoły powinny koncentrować się jednak na aktywnościach wychowawczych. W przypadku upowszechniania przez sprawców treści nielegalnych  (np. pornografii dziecięcej) należy złożyć zawiadomienie  o zdarzeniu na Policję. |
| Aktywności wobec ofiar zdarzenia | Dzieci - ofiary i świadków zdarzenia – należy od pierwszego etapu interwencji - otoczyć opieką psychologiczno-pedagogiczną. Rozmowa z dzieckiem powinna się odbywać  w warunkach jego komfortu psychicznego, z poszanowaniem poufności i podmiotowości ucznia ze względu na fakt, iż kontakt z treściami nielegalnymi może mieć bardzo szkodliwy wpływ na jego psychikę. W jej trakcie należy ustalić  okoliczności uzyskania przez ofiarę dostępu do ww. treści.  Należy koniecznie powiadomić ich rodziców lub opiekunów prawnych o zdarzeniu i uzgodnić z nimi podejmowane działania i formy wsparcia dziecka. Działania szkoły w takich przypadkach powinna cechować poufność i empatia  w kontaktach z wszystkimi uczestnikami zdarzenia oraz udzielającymi wsparcia.  W przypadku kontaktu dziecka z treściami szkodliwymi należy dokładnie zbadać sposób, w jaki nastąpił kontakt dziecka z nimi. Poszukiwanie przez dziecko tego typu treści w sieci lub podsuwanie ich dziecku przez innych może być oznaką niepokojących incydentów ze świata rzeczywistego.  Np. kontakty z osobami handlującymi narkotykami czy proces rekrutacji do sekty lub innej niebezpiecznej grupy. |
| Aktywności wobec świadków | W przypadku, gdy informacja na temat zdarzenia dotrze do środowiska rówieśniczego ofiary – w klasie, czy szkole, wskazane jest podjęcie działań edukacyjnych i wychowawczych. |
| Współpraca z Policją i sądami rodzinnymi | 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 dziecka - niezwłocznie powiadomić Policję |
| Współpraca ze służbami i placówkami specjalistycznymi | Kontakt z treściami szkodliwymi lub niebezpiecznymi może wywołać potrzebę skorzystania przez ofiarę ze specjalistycznej opieki psychologicznej. Decyzja o takim kontakcie  i skierowaniu na terapię musi zostać podjęta w porozumieniu  z rodzicami/opiekunami prawnymi dziecka |

|  |  |
| --- | --- |
| 2. | Cyberprzemoc |
| Podstawy prawne uruchomienia procedury | Kodeks Karny, Statut szkoły |
| Rodzaj zagrożenia objętego procedurą | Cyberprzemoc –przemoc z użyciem technologii informacyjnych  i komunikacyjnych, głównie Internetu oraz telefonów komórkowych. Podstawowe formy zjawiska to 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. Do działań określanych mianem cyberprzemocy wykorzystywane są głównie: poczta elektroniczna, czaty, komunikatory, strony internetowe, blogi, serwisy społecznościowe, grupy dyskusyjne, serwisy SMS i MMS |
| Telefony/kontakt alarmowe krajowe | Telefon Zaufania dla Dzieci i Młodzieży -116 111  Telefon dla Rodziców i Nauczycieli w sprawie Bezpieczeństwa Dzieci – **800 100 100,** dyzurnet@dyzurnet.pl |
| Sposób postępowania w przypadku wystąpienia zagrożenia | |
| **Przyjęcie zgłoszenia i ustalenie okoliczności zdarzenia** | Reakcja szkoły w przypadku pozyskania wiedzy o wystąpieniu zagrożenia będzie zależna od tego, czy: (1) treści te można bezpośrednio powiązać z uczniami danej szkoły, czy też (2) treści nielegalne lub szkodliwe nie mają związku z uczniami danej szkoły, lecz wymagają kontaktu szkoły z odpowiednimi służbami.  W pierwszej kolejności należy zabezpieczyć dowody w formie elektronicznej (pliki z treściami niedozwolonymi, zapisy rozmów w komunikatorach, e-maile, zrzuty ekranu), znalezione w Internecie lub w komputerze dziecka. Zabezpieczenie dowodów jest zadaniem rodziców lub opiekunów prawnych dziecka, w czynnościach tych może wspomagać ich przedstawiciel szkoły posiadający odpowiednie kompetencje techniczne. W przypadku sytuacji (1) rozwiązanie leży po stronie szkoły, zaś (2) należy rozważyć zgłoszenie incydentu na Policję oraz zgłosić go do serwisu Dyżurnet (dyzurnet.pl). |
| Opis okoliczności, analiza, zabezpieczenie dowodów | Należy zabezpieczyć wszystkie dowody związane z aktem cyberprzemocy (np. zrobić kopię materiałów, zanotować datę i czas otrzymania materiałów, dane nadawcy, adresy stron www, historię połączeń, etc.). W trakcie zbierania materiałów należy zadbać o bezpieczeństwo osób zaangażowanych w problem. |
| Identyfikacja sprawcy(ów) | Identyfikacja sprawcy(ów) często jest możliwa dzięki zebranym materiałom –wynikom rozmów z osobą zgłaszającą, z ofiarą, analizie zebranych materiałów. Ofiara często domyśla się, kto stosuje wobec niego cyberprzemoc.  Jeśli ustalenie sprawcy nie jest możliwe, a w ocenie kadry pedagogicznej jest to konieczne, należy skontaktować się z Policją. Bezwzględnie należy zgłosić rozpowszechnianie nagich zdjęć osób poniżej 18 roku życia (art. 202 par. 3 KK) |
| Aktywności wobec sprawców zdarzenia ze szkoły/spoza szkoły | Gdy sprawca cyberprzemocy jest znany i jest on uczniem szkoły, pedagog szkolny powinien przeprowadzić z nim rozmowę o jego zachowaniu. Rozmowa taka ma służyć ustaleniu okoliczności zdarzenia, jego wspólnej analizie (w tym np. przyjrzeniu się przyczynom), a także próbie rozwiązania sytuacji konfliktowej (w tym sposobów zadośćuczynienia ofiarom cyberprzemocy).  Cyberprzemoc powinna podlegać sankcjom określonym w wewnętrznych przepisach szkoły (m. in. w statucie, kontrakcie, regulaminie). Szkoła moęe tu stosować konsekwencje przewidziane dla sytuacji „tradycyjnej” przemocy. Warto jednak rozszerzyć repertuar dostępnych środków, np. o czasowy zakaz korzystania ze szkolnej pracowni komputerowej w czasie wolnym i przynoszenia do szkoły akcesoriów elektronicznych (PSP, mp3) itp |
| Aktywności wobec ofiar zdarzenia | W pierwszej kolejności należy udzielić wsparcia ofierze. Musi się ona czuć bezpieczna i zaopiekowana przez dorosłych. Na poczucie bezpieczeństwa dziecka wpływa fakt, że wie ono, iż szkoła podejmuje kroki w celu rozwiązania problemu.  Podczas rozmowy z uczniem –ofiarą cyberprzemocy –należy zapewnić go, z e nie jest winny zaistniałej sytuacji oraz że nikt nie ma prawa zachowywać się w ten sposób wobec niego, a także podkreślić, że dobrze zrobił ujawniając sytuację. Należy okazać zrozumienie dla jego uczuć, w tym trudności z ujawnieniem okoliczności wydarzenia, strachu, wstydu. Trzeba podkreślić ,  że szkoła nie toleruje przemocy i że zostaną podjęte odpowiednie procedury interwencyjne. Należy poinformować ucznia o krokach, jakie może podjąć szkoła i sposobach, w jaki może zapewnić mu bezpieczeństwo.  Należy pomóc ofierze (rodzicom ofiary) w zabezpieczeniu dowodów (to może być dla niej zadanie trudne zarówno ze względów technicznych, jak i emocjonalnych), zerwaniu kontaktu ze sprawcą, zadbaniu o podstawowe zasady bezpieczeństwa on-line (np. nieudostępnianie swoich danych kontaktowych, kształtowanie swojego wizerunku etc).  Pomoc ofierze nie może kończyć się w momencie zakończenia procedury. Warto monitorować sytuację, „czuwać” nad jej bezpieczeństwem, np. zwracać uwagę czy nie są podejmowane wobec niej dalsze działania przemocowe, obserwować jak sobie radzi w grupie po ujawnionym incydencie cyberprzemocy.  W działania wobec ofiary należy także włączyć rodziców/opiekunów ofiary –trzeba na bieżąco ich informować o sytuacji, pamiętając przy tym o podmiotowym traktowaniu dziecka –mówiąc mu o tym i starając się uzyskać jego akceptację dla udziału rodziców. Jeśli dziecko nie wyraz a zgody, należy omówić z nim jego obawy, a jeśli to nie pomaga powołać się na obowiązujące nas zasady i przekazać informację rodzicom.  W trakcie rozmowy z dzieckiem i/lub jego rodzicami/opiekunami, jeśli jest to wskazane, można zaproponować pomoc specjalisty (np. psycholog szkolny, poradnia psychologiczno-pedagogiczna) oraz przekazać informację o możliwości zgłoszenia sprawy Policji. |
| Aktywności wobec świadków | Należy zadbać o bezpieczeństwo świadków zdarzenia, zwłaszcza, jes li byli oni osobami ujawniającymi cyberprzemoc. W trakcie rozmowy ze świadkami należy okazać zrozumienie i empatię dla ich uczuć –obawy przed przypięciem łatki „donosiciela”, strachu przed staniem się kolejną ofiarą sprawcy itp. |
| Współpraca z Policją i sądami rodzinnymi | Samo wystąpienie zjawiska cyberprzemocy nie jest jednoznaczne z koniecznością zaangażowania Policji i sądu rodzinnego –procedura powinna umożliwiać rozwiązanie sytuacji problemowej na poziomie pracy wychowawczej szkoły. Szkoła powinna powiadomić odpowiednie służby (np. sąd rodzinny), gdy wykorzysta wszystkie dostępne jej środki wychowawcze (rozmowa z rodzicami, konsekwencje z statutu i/lub regulaminu wobec ucznia) i interwencje pedagogiczne, a ich zastosowanie nie przynosi pożądanych rezultatów (np. nie ma zmian postawy ucznia).  Kontaktu z Policją wymagają wszelkie sytuacje, w których zostało naruszone prawo (np. groz by karalne, świadome publikowanie nielegalnych treści, rozpowszechnianie nagich zdjęć z udziałem małoletnich). Za zgłoszenie powinien odpowiadać dyrektor szkoły. |
| **Współpraca z dostawcami Internetu i operatorami telekomunikacyjnymi** | Kontakt z dostawcą usługi może być wskazany w celu usunięcia z sieci kompromitujących lub krzywdzących materiałów. Do podjęcia takiego działania stymuluje administratora serwisu art. 14 Ustawy z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną |