Załącznik do Zarządzenia
Nr 2/2017/2018
Dyrektora
Szkoły Podstawowej
w Małogoszczu
z dnia 28 kwietnia 2018 r.

INFORMATOR WPROWADZANIA ZASAD BEZPIECZNEGO KORZYSTANIA Z INTERNETU ORAZ PROCEDURY DZIAŁAŃ SZKOŁY W MOMENCIE ICH ŁAMANIA PRZEZ UCZNIÓW

Wstęp

CYBERZAGROŻENIA I BEZPIECZEŃSTWO CYFROWE W SZKOLE

Dzisiejszy świat to świat cyfrowych technologii, informacji i usług, które stały się codziennością. Korzystamy z nich w pracy, szkole i życiu prywatnym. Wszystko to ma celu poprawić jakość naszego funkcjonowania i służyć pomocą. Jednak stanie się to dopiero wtedy, gdy będziemy z nowych technologii korzystać w sposób odpowiedzialny i znać zasady kierujące wirtualnym światem oraz konsekwencje nieprzestrzegania tych zasad.

W związku z postępem technologicznym nasza szkoła powinna w jak najszerszym stopniu wykorzystywać edukacyjne zasoby dostępne online – multimedialne treści, aplikacje, platformy i skojarzone z nimi interaktywne metody nauczania. Właściwe korzystanie z komputera i Internetu może być zatem bardzo pożyteczne i służyć uczniom jako pomoc edukacyjna, może być także świetną formą rozrywki, pod warunkiem jednak, że wszyscy będą korzystać z sieci rozważnie i z zachowaniem wszelkich zasad bezpieczeństwa.

I. Katalog zagrożeń

Korzystając z zasobów i możliwości jakie daje nam Internet warto na początek poznać niebezpieczeństwa płynące z sieci. Oto te najważniejsze:

- wirusy komputerowe
- hasła zapamiętywane w przeglądarce
- naruszenie prywatności, stalking
- hakerzy
- spam
- nieodpowiednie treści
- pedofilia
- bezpieczeństwo danych w sieci
- botnety
- fałszywe lajki i ciasteczka
- fałszywe oprogramowanie ochronne
- fałszywe witryny i wyłudzanie danych
- szyfrowanie danych bez naszej wiedzy
- wykradanie danych osobowych
- skrócone adresy
- literówki w adresach WWW
- otwarte sieci wi-fi
- ataki ukierunkowane
- niezaktualizowane oprogramowanie
- nadmierna wiara w odporność na zagrożenia.

Internet jest przydatnym do nauki, pracy i zabawy narzędziem. Niestety, jak każde narzędzie może być używane do dobrych jak i złych działań. Warto wiedzieć, jakie występują w nim zagrożenia i jak się zachować, kiedy na nie natrafimy.

Niebezpieczne kontakty - pamiętaj, że nie wszyscy w Internecie mają wobec Ciebie dobre zamiary, nawet jeśli tak mówią. W Internecie oszukiwać jest łatwiej niż w prawdziwym życiu. Nie wierz, we wszystko, co usłyszysz od osób, które znasz tylko w Internecie. Nie wolno się też z takimi osobami spotykać – ktoś może mówić, że ma tyle lat co Ty, a tak naprawdę jest dorosłą osobą!

Szkodliwe kontakty - zdarzyć się może, że ktoś obrazi Cię na czacie, wyśle nieprzyjemnego e-maila lub wiadomość na komunikatorze, a może po prostu pisze do Ciebie, choć Ty tego nie chcesz. Może to być ktoś, kto Cię zna, ale może też to być osoba nieznajoma, która uważa, że takie zachowanie to dobry żart. Zwykle ktoś taki myśli też, że w Internecie można robić, co się chce i nikt nie dowie się, kim jest. To nieprawda. W Internecie każdy zostawia ślady, po których policja może go znaleźć. Jeśli zdarzy Ci się, że internetowy kontakt sprawia Ci przykrość, powiedz o tym rodzicom lub zaufanej osobie dorosłej. Możesz również skontaktować się z helpline.org.pl.

Ujawnienie Twoich prywatnych danych - Twoje prywatne dane nie powinny wpaść w niepowołane ręce! Adres e-mail, numer telefonu, adres, zdjęcie czy różnego rodzaju hasła (do poczty, komunikatora, czatu) to informacje, które należy chronić w trosce o własne bezpieczeństwo. Przecież nie chcesz dostawać spamu lub żeby każdy wiedział, gdzie mieszkasz i mógł do Ciebie przyjść czy zmienił tak Twoje zdjęcie w komputerze, że będzie Ci przykro, będą się z Ciebie śmiać. To samo dotyczy danych Twoich kolegów i koleżanek – odmawiaj, jeśli ktoś Cię o to poprosi – nie chcesz, by im stało się coś złego.

Szkodliwe treści - to takie teksty, zdjęcia, filmy i nagrania, które są nielegalne lub przeznaczone tylko dla dorosłych. Kontakt z nimi może być dla Ciebie przykry, mogą Cię przestraszyć, zawstydzić lub spowodować, że poczujesz się źle. Pamiętaj, że możesz na nie natrafić zupełnie przypadkowo, to się zdarza i nie ma w tym Twojej winy. Jeśli zdarzyło Ci się napotkać w Internecie szkodliwe treści – powiedz o tym rodzicom lub zaufanej osobie dorosłej, a ona niech skontaktuje się z dyżurnet.pl, aby treści te zostały usunięte i nikomu już nie zagrażały.

Wirusy i złośliwe programy - wirusy i inne złośliwe programy mogą zniszczyć pliki na Twoim komputerze, albo sprawić, że korzystanie z niego będzie trudne lub nawet niemożliwe – przestanie działać tak, jak powinien. Nie ma całkowicie skutecznej ochrony przed wirusami i złośliwymi programami. Chronić należy się poprzez stosowanie antywirusa (pamiętaj o regularnym uaktualnianiu jego bazy – pozwoli mu to rozpoznawać nowe zagrożenia) i zapory sieciowej. Bardzo ważne jest również korzystanie tylko z tych programów, płyt, dyskietek i pendrive'ów, na których wiemy co się znajduje. Tę samą zasadę warto stosować również do nieznanych stron **internetowych.**

Spam - spam można porównać do ulotek zostawianych przed drzwiami lub wkładanych za wycieraczki samochodów. To wiadomości e-mail, które trafiają na Twoją skrzynkę, choć nie czekałeś na nie i nie są Ci potrzebne. Spam może przeszkadzać w znalezieniu w nim listu, na który czekasz, może też zawierać szkodliwe treści i wirusy. Dlatego warto korzystać w anty-spamu w poczcie, a swój adres e-mail chronić i nie podawać nikomu bez potrzeby, zwłaszcza w Internecie, gdzie każdy może go znaleźć.

Włamania - zdarzyć się może, że ktoś zobaczy, jakie hasło wpisujesz logując się na pocztę, do komunikatora czy na czacie. Może się też zdarzyć, że hasło jest bardzo proste i może je zgadnąć każdy, kto będzie miał trochę szczęścia lub dobrze Cię zna. Znając Twoje hasło, osoba taka może zrobić co tylko chce, a dla innych użytkowników Internetu wyglądać to będzie na Twoje działania. Aby uniknąć kłopotów i nieprzyjemności wymyślaj dobre hasła, to jest długie i skomplikowane. Nie używaj jako haseł imienia swojego, przyjaciela, czy zwierzaka, daty urodzenia itd. – te hasła są popularne i łatwo je odgadnąć.

II. Katalog zasad

1. Nigdy nie podawaj w Internecie swojego prawdziwego imienia i nazwiska. Posługuj się nickiem, czyli pseudonimem, internetową ksywką.

2. Nigdy nie podawaj osobom poznanym w Internecie swojego adresu domowego, numeru telefonu i innych tego typu informacji. Nie możesz mieć pewności, z kim naprawdę rozmawiasz!

3. Nigdy nie wysyłaj nieznajomym swoich zdjęć. Nie wiesz, do kogo naprawdę trafią.

4. Jeżeli wiadomość, którą otrzymałeś jest wulgarna lub niepokojąca, nie odpowiadaj na nią. Pokaż ją swoim rodzicom lub innej zaufanej osobie dorosłej.

5. Pamiętaj, że nigdy nie możesz mieć pewności, z kim rozmawiasz w Internecie. Ktoś, kto podaje się za twojego rówieśnika w rzeczywistości może być dużo starszy i mieć wobec ciebie złe zamiary.

6. Kiedy coś lub ktoś w Internecie cię przestraszy, koniecznie powiedz o tym rodzicom lub innej zaufanej osobie dorosłej.

7. Internet to skarbnica wiedzy, ale pamiętaj, że nie wszystkie informacje, które w nim znajdziesz muszą być prawdziwe! Staraj się zawsze sprawdzić wiarygodność informacji.

8. Szanuj innych użytkowników Internetu. Traktuj ich tak, jak chcesz, żeby oni traktowali Ciebie.

9. Szanuj prawo własności w Sieci. Jeżeli posługujesz się materiałami znalezionymi w Internecie, zawsze podawaj źródło ich pochodzenia.

10. Spotkania z osobami poznanymi w Internecie mogą być niebezpieczne! Jeżeli planujesz spotkanie z internetowym znajomym pamiętaj, aby zawsze skonsultować to z rodzicami. Na spotkania umawiaj się tylko w miejscach publicznych i idź na nie w towarzystwie rodziców lub innej zaufanej dorosłej osoby.

11. Uważaj na e-maile otrzymane od nieznanych Ci osób. Nigdy nie otwieraj podejrzanych załączników i nie korzystaj z linków przesłanych przez obcą osobę! Mogą na przykład zawierać wirusy. Najlepiej od razu kasuj maile od nieznajomych.

12. Pamiętaj, że hasła są tajne i nie powinno się ich podawać nikomu. Dbaj o swoje hasło, jak o największą tajemnicę. Jeżeli musisz w Internecie wybrać jakieś hasło, pamiętaj, żeby nie było ono łatwe do odgadnięcia i strzeż go jak oka w głowie.

13. Nie spędzaj całego wolnego czasu przy komputerze. Ustal sobie jakiś limit czasu, który poświęcasz komputerowi i staraj się go nie przekraczać.

14. Jeżeli prowadzisz w Internecie stronę lub bloga, pamiętaj, że mają do niej dostęp również osoby o złych zamiarach. Nigdy nie podawaj na swojej stronie adresu domowego, numeru telefonu, informacji o rodzicach, itp. Bez zgody rodziców nie publikuj też na niej zdjęć swoich, rodziny ani nikogo innego, kto nie wyrazi na to zgody.

15. Rozmawiaj z rodzicami o Internecie. Informuj ich o wszystkich stronach, które Cię niepokoją. Pokazuj im również strony, które Cię interesują i które często odwiedzasz.

16. Jeżeli twoi rodzice nie potrafią korzystać z Internetu, zostań ich nauczycielem. Pokaż im, jak proste jest serfowanie po Sieci. Zaproś ich na Twoje ulubione strony, pokaż im jak szukać w Internecie informacji.

17. Jeżeli chcesz coś kupić w Internecie, zawsze skonsultuj to z rodzicami. Nigdy nie podawaj numeru karty kredytowej i nie wypełniaj internetowych formularzy bez wiedzy i zgody rodziców.

18. W Sieci krąży coraz więcej wirusów, które mogą uszkodzić komputer. Dlatego koniecznie zainstaluj oprogramowanie antywirusowe. Porozmawiaj o tym z rodzicami i wspólnie wybierzcie, a następnie zainstalujcie odpowiedni program.

III. Działania wychowawcze i edukacyjne adresowane do uczniów

1. Zorganizowanie w szkole wydarzenia poświęconego tematyce bezpieczeństwa cyfrowego, przygotowanego przez uczniów dla całej społeczności szkolnej (np. apelu, przedstawienia teatralnego, happeningu, kampanii lokalnej).

2. Organizacja spotkań społeczności szkolnej z ekspertem tematyki korzystania z Internetu przez dzieci (edukatorem, nauczycielem, informatykiem, policjantem, itp.).

3. Przeprowadzenie lekcji wychowawczych oraz zajęć informatycznych na temat wybranego aspektu cyberbezpieczeństwa, adekwatnego do potrzeb i wyzwań klasy

i wieku uczniów. Sposób prowadzenia lekcji i ich tematyka muszą uwzględniać wiek i doświadczenia dzieci.

4. Organizacja Dnia Bezpieczeństwa Cyfrowego w szkole lub Dnia Bezpiecznego Internetu - wydarzenia dla całej społeczności szkolnej, otwartego na współudział rodziców/opiekunów prawnych uczniów, a także przedstawicieli lokalnego środowiska - władz oświatowych, organizacji pozarządowych, czy instytucji kultury. Do współorganizacji takiego dnia dyrekcja szkoły oraz lider tematyki bezpieczeństwa cyfrowego w szkole mogą zaprosić samorząd uczniowski, przewodniczących klas, czy radę rodziców. Na wydarzenie składać się mogą prelekcje i zajęcia praktyczne (warsztaty) w szkole, a także spotkania uświadamiające, dyskusje, happeningi, pikniki i inne formy popularyzacji tematyki cyberbezpieczeństwa.

5. Organizacja konkursów indywidualnych i grupowych na temat bezpieczeństwa cyfrowego (np. pozytywnego wykorzystania zasobów Internetu, sposobów radzenia sobie w sytuacjach zagrożenia) z nagrodami ufundowanymi przez radę rodziców i sponsorów.

6. Organizacja zajęć pozalekcyjnych dla uczniów o tematyce informatycznej (np. programowanie, robotyka, projektowanie graficzne, szkolne radio lub telewizja) z obligatoryjnym uwzględnieniem komponentu edukacji w zakresie bezpieczeństwa cyfrowego, a także kształtujących miękkie kompetencje medialne i cyfrowe (np. tworzenie własnego wizerunku cyfrowego, współpraca grupowa poprzez sieć, skuteczne szukanie informacji, odróżnianie fałszu od prawdy w sieci, prawo autorskie, bezpieczeństwo w sieci, itp).

7. Realizacja projektów edukacyjnych uwzględniających nowe technologie informacyjno - komunikacyjne oraz tematykę bezpieczeństwa cyfrowego, finansowanych ze środków unijnych, kuratoriów i fundacji prywatnych.

8. W codziennej pracy dydaktycznej należy dążyć do włączania tematyki bezpieczeństwa cyfrowego w nauczanie przedmiotów nie-informatycznych, a także wzmacniać zainteresowania uczniów tematyką bezpieczeństwa cyfrowego poprzez przygotowywanie ich do startu w konkursach.

9. Pojawienie się tematyki bezpieczeństwa cyfrowego szkoły na szkolnej stronie internetowej (oraz na profilach szkoły, w portalach społecznościowych) jako oddzielnego zagadnienia. Szczególne znaczenie ma publikacja w nich numerów telefonów, pod którymi można zgłosić przypadki naruszenia bezpieczeństwa cyfrowego w sposób anonimowy lub jako spersonalizowane zgłoszenie. Uczniowie w szkole powinni ponadto wiedzieć, kto pełni rolę szkolnego lidera bezpieczeństwa cyfrowego - do kogo należy zgłaszać indywidualne przypadki niedozwolonych zachowań lub działań. Uzupełnieniem wiadomości na ten temat będą gazetki informacyjne na korytarzu szkolnym oraz w salach informujące o aktualnościach

i o różnych zagadnieniach bezpieczeństwa cyfrowego, czy odsyłające do materiałów informacyjnych i edukacyjnych w sieci.

10. Traktowanie „bezpieczeństwa dzieci w Internecie" również w kontekście propagowania otwartości na odmienność, tolerancji, kształtowania zachowań prospołecznych, wrażliwości na krzywdę i eliminowania obojętności oraz bierności.
11. Poinformowanie uczniów, że mogą się zwracać do nauczycieli z informacją o wszelkich przejawach przemocy również tej z użyciem nowych technologii:
- dopuszczanie anonimowych form zgłaszania informacji dotyczących aktów przemocy na terenie szkoły (skrzynka Rzecznik Praw Ucznia w szkole),
- konsekwentne reagowanie na zgłaszane problemy oraz zaistniałe incydenty.

IV. Działania edukacyjne w szkole adresowane do rodziców uświadamiające ich w zakresie tematyki bezpieczeństwa w sieci

1. Zaangażowanie rodziców do organizacji Szkolnego Dnia Bezpieczeństwa Cyfrowego lub Dnia Bezpiecznego Internetu przez m.in. krótkie szkolenia dla rodziców z wykorzystaniem materiałów multimedialnych, prezentacji, przygotowanych wspólnie z uczniami ulotek informacyjnych.

2. Włączenie w tematykę spotkania - „wywiadówki" z rodzicami każdej z klas w szkole tematyki bezpieczeństwa cyfrowego.

3. Rozesłanie za pomocą systemu e-dziennika informacji na temat potencjalnych zagrożeń wraz z linkami do materiałów edukacyjnych i multimediów oraz apelem do rodziców o zapoznanie się z daną tematyką i rozmowę z dziećmi.

4. Bieżące przesyłanie pojawiających się aktualności, raportów z badań i ciekawostek na w/w temat.

5. W przypadku wystąpienia zagrożenia cyberbezpieczeństwa w klasie należy o tym powiadomić rodziców bezzwłocznie i zorganizować spotkanie specjalnie poświęcone temu incydentowi.

V. Działania skierowane do Rady Pedagogicznej

1. Zapoznanie Rady Pedagogicznej z założeniami „Szkolnych Zasad Bezpiecznego Korzystania z Internetu".

2. Przydział zadań, ustalenie odpowiedzialnych za ich wykonanie.

3. Przeszkolenie Rady Pedagogicznej.

4. Włączenie tematyki bezpieczeństwa dzieci w sieci do programów szkolnych oraz zajęć lekcyjnych.

5. Zachęcanie do korzystania z propozycji edukacyjnych opracowanych zewnętrznie i udostępnianych w formie elektronicznej lub drukowanej.

6. Niezwłoczna i zdecydowana interwencja na wszystkie przejawy przemocy w tym te z udziałem nowych technologii.

7. Indywidualny kontakt nauczyciela z rodzicem, pedagogiem szkolnym i dyrekcją szkoły w przypadku zdarzenia cyberprzemocy (w zależności od potrzeb).

VI. PROCEDURA UJAWNIANIA CYBERPRZEMOCY

1.Ustalenie okoliczności zdarzenia: rodzaj materiału, sposób jego rozpowszechniania, ustalenie sprawcy oraz świadków zdarzenia:

- ✓ jeśli wiedzę o zajściu posiada nauczyciel nie będący wychowawcą, należy przekazać informacje wychowawcy klasy, który jest zobowiązany poinformować o fakcie pedagoga szkolnego oraz dyrektora,

- ✓ pedagog, wychowawca oraz dyrektor wspólnie dokonują analizy zdarzenia i planują dalsze postępowanie,

- ✓ do zadań szkoły należy także ustalenie okoliczności zdarzenia, sprawców, ofiar oraz odnalezienie ewentualnych świadków,

- ✓ włączenie nauczyciela informatyki, szczególnie na etapie zabezpieczania dowodów i ustalania tożsamości sprawcy.

2. Zabezpieczanie dowodów:

- ✓ wszelkie dowody cyberprzemocy należy odpowiednio zabezpieczyć i zarejestrować (zanotować datę i czas otrzymania materiału, treść wiadomości oraz jeśli to możliwe, dane nadawcy-adres użytkownika, adres e-mail, numer telefonu komórkowego, adres strony WWW, na której ukazały się szkodliwe treści itp.),

- ✓ tak zabezpieczone dowody są materiałem, z którym powinny zapoznać się wszystkie zaangażowane osoby.

3. Identyfikacja sprawcy:

- ✓ świadomość, że znalezienie miejsca pochodzenia materiału nie zawsze jest równoznaczne z odnalezieniem osoby odpowiedzialnej za działania cyberprzemocy. Sprawcy zazwyczaj ukrywają swoją tożsamość: korzystają z internetowych bramek sms-owych, podszywają się pod innych użytkowników sieci, wykorzystują telefony innych uczniów,

- ✓ w identyfikacji sprawcy pomagają rozmowy z innymi uczniami oraz świadkami zdarzenia bądź osobami trzecimi.

JEŚLI USTALENIE SPRAWCY NIE JEST MOŻLIWE należy skontaktować się z dostawcą usługi. Jest on ustawowo zobowiązany do usunięcia z Sieci kompromitujących, obraźliwych bądź krzywdzących materiałów oraz do zablokowania konta. Jednak dane sprawcy nie mogą być udostępnione osobom prywatnym, ani szkole. Aby je pozyskać konieczny jest kontakt z policją.

- ✓ w przypadku gdy numer telefonu sprawcy jest zastrzeżony, operator sieci komórkowej musi podjąć kroki umożliwiające ustalenie danych oraz udostępnienie ich policji. W tym celu należy przekazać informacje o dacie i godzinie rozmowy, bądź nagrania na poczcie głosowej,

- ✓ w przypadku, gdy zostało złamane prawo, a nie udało się ustalić tożsamości sprawcy, należy bezwzględnie skontaktować się z policją. Zgodnie z kodeksem polskiego prawa, które mówi o obowiązku zawiadamiania o przestępstwie (art.304§1 i 2 k.p.k-w przypadku cyberprzemocy przestępstwami ściganymi z urzędu są: włamania, groźby: karalna i bezprawna. Jeśli posiada się wiedzę o tych przestępstwach należy zawiadomić policje lub prokuraturę).

VII. DZIAŁANIA WOBEC SPRAWCY CYBERPRZEMOCY

1. Jeśli sprawca cyberprzemocy jest nieznany (nie jest uczniem szkoły):

- ✓ należy podjąć wszelkie czynności w celu przerwania aktu cyberprzemocy-zaczynając od zawiadomienia administratora serwisu (w celu usunięcia krzywdzących materiałów), kończąc na powiadomieniu policji lub prokuratury.

2. Jeśli sprawca jest znany i jest on uczniem szkoły:

- ✓ należy przeprowadzić rozmowę w celu ustalenia okoliczności oraz przyczyn zajścia oraz poszukania rozwiązania sytuacji konfliktowej,

- ✓ uczeń-sprawca powinien otrzymać jasny komunikat, że szkoła nie toleruje żadnych form przemocy,

- ✓ należy omówić skutki postępowania oraz konsekwencje, które zostaną wobec niego zastosowane zgodnie ze Statutem Szkoły,

- ✓ sprawca musi zostać zobligowany do zaprzestania jakichkolwiek form przemocy oraz do usunięcia z Internetu krzywdzących materiałów,

- ✓ w rozmowie ze sprawcą należy zwrócić szczególną uwagę na omówienie sposobów zadość uczynienia wobec ofiary,

- ✓ w przypadku gdy w zdarzeniu brała udział większa grupa uczniów, należy przeprowadzić rozmowę ze wszystkimi z osobna, zaczynając od lidera grupy,

- ✓ nie należy konfrontować sprawcy i ofiary cyberprzemocy.

3. Powiadomienie rodziców sprawcy:

- ✓ rodzice sprawcy powinni zostać poinformowani o zaistniałym zdarzeniu, jego przebiegu oraz powinni zapoznać się z materiałem dowodowym, oraz decyzją dotyczącą dalszego postępowania z dzieckiem, a także o środkach dyscyplinarnych podjętych wobec ich dziecka,

- ✓ w miarę możliwości szkoła powinna podjąć próbę współpracy z rodzicami i opracować wspólny plan działania, do którego zobowiązany jest uczeń.

4. Objęcie sprawcy opieką psychologiczno-pedagogiczną:

- ✓ praca ze sprawcą powinna opierać się na pomocy uczniowi w zrozumieniu wyrządzonej krzywdy oraz konsekwencji swojego zachowania. Ma ona za zadanie wpłynąć na zmianę postawy i postępowania ucznia, w tym zmienić cele oraz sposób użytkowania nowych technologii.

- ✓ w trudnych, uzasadnionych przypadkach można zaproponować rodzicom oraz uczniowi, poradę specjalisty z poza szkoły bądź udział w programie terapeutycznym.

5. Zastosowanie środków dyscyplinarnych wobec ucznia-sprawcy:

- ✓ trzeba pamiętać, że celem sankcji wobec sprawcy jest przede wszystkim zatrzymanie fali przemocy i zapewnienie poczucia bezpieczeństwa poszkodowanemu uczniowi,
- ✓ wzbudzenie refleksji na temat swojego zachowania, zrozumienie krzywdy, skrucha, zadość uczynienie i powstrzymanie przed podobnym zachowaniem w przyszłości,
- ✓ pokazanie innym uczniom, że cyberprzemoc nie jest tolerowana i że szkoła efektywnie reaguje na jej przejawy,
- ✓ podejmując decyzję o rodzaju kary trzeba wziąć pod uwagę: rozmiar i rangę szkody, czas trwania prześladowania, determinacje oraz świadomość popełnianego czynu.

VIII. DZIAŁANIA WOBEC OFIARY CYBERRZEMOCY

1. Wsparcie psychiczne

- ✓ ofiara cyberprzemocy musi otrzymać pomoc i wsparcie emocjonalne, musi także zostać zapewniona, iż szkoła podejmie odpowiednie kroki w celu rozwiązania problemu,

2. Porada

- ✓ uczeń będący ofiarą cyberprzemocy powinien otrzymać poradę, jak ma się zachować, aby mógł czuć się bezpiecznie i co musi zrobić by nie doprowadzić do eskalacji prześladowania,

3. Monitoring

- ✓ po zakończeniu interwencji warto monitorować sytuację ucznia, by dociec czy przypadkiem sytuacja po ukaraniu sprawców się nie zaogniła. W tym miejscu konieczna jest również współpraca z rodzicami, którzy powinni zostać przygotowani przez pedagoga szkolnego, jak zapewnić bezpieczeństwo i komfort psychiczny poszkodowanemu. W szczególnie agresywnych przypadkach cyberprzemocy, powinno się zaproponować rodzicom i dziecku pomoc

specjalisty,

- ✓ w sytuacji gdy przypadek cyberprzemocy wymaga założenia sprawy sądowej, szkoła powinna powiadomić o takiej ewentualności rodziców ofiary oraz ucznia. Jednocześnie pomóc jej w przygotowaniu odpowiednich dokumentów sądowych uzasadniających i przedstawiających dowody winy oskarżonego.

IX. OCHRONA ŚWIADKÓW CYBERPRZEMOCY

1. Ważne by w wyniku interwencji świadkowie nie zostali narażeni na działania odwetowe ze strony sprawcy.

2. Postępowanie interwencyjne wymaga od pedagogów wyjaśniających sprawę dyskrecji i poufnego postępowania.

3. Niedopuszczalne jest konfrontowanie świadka ze sprawcą, ani upublicznianie jego udziału w sprawie. Jest to nieprofesjonalna metoda wyjaśniania sprawy, może ona sprawić, że świadek stanie się kolejną ofiarą, może również sprawić, iż następnym razem uczeń nie zgłosi informacji o zagrażającym zdarzeniu.

X. SPORZĄDZANIE DOKUMENTACJI Z INCYDENTU

1. Pedagog szkolny lub nauczyciel zobowiązany jest do sporządzenia notatki służbowej z rozmów ze sprawcą, poszkodowanym i jego opiekunami, a także ze świadkami zdarzenia (dokument powinien zawierać datę i miejsce rozmowy, dane personalne osób biorących w niej udział i opis ustalonego przebiegu wydarzeń).

2. Notatkę z rozmowy powinny podpisać osoby wskazane przez osobę prowadzącą interwencję.

3. Jeżeli zostały odnalezione i zabezpieczone dowody cyberprzemocy (wydruki, opisy smsów itp.), należy je również włączyć do dokumentacji pedagogicznej.

XI. POWIADOMIENIE SĄDU RODZINNEGO

1. Jeżeli zaistniałego przypadku cyberprzemocy nie można rozwiązać przy użyciu środków wychowawczych jakimi dysponuje szkoła, sprawę należy przekierować, zgłaszając ją na policję lub do sądu rodzinnego z zawiadomieniem o postępowaniu w sprawach nieletnich.

2. Jeśli rodzice sprawcy cyberprzemocy odmawiają współpracy lub nie stawiają się w szkole, a uczeń nie zaniechał dotychczasowego postępowania, dyrektor szkoły powinien pisemnie powiadomić o zaistniałej sytuacji sąd rodzinny, zwłaszcza jeśli do szkoły napływają informacje o innych przejawach demoralizacji dziecka.

3. W przypadkach szczególnie drastycznych aktów agresji z naruszeniem prawa, dyrektor szkoły zobowiązany jest zgłosić te fakty policji i do sądu rodzinnego.

Problem niestosowania zasad netykiety istnieje nie od dziś i ważne jest, by systematycznie przypominać młodym użytkownikom o zagrożeniach jakie niesie ze sobą praca i zabawa w sieci.

Pamiętajmy jednak, że mimo tych wszystkich zagrożeń Internet to wspaniałe źródło informacji i rozrywki. Trzeba jednak mieć "oczy szeroko otwarte" i nie dać się wciągnąć w niebezpieczne kontakty, nie ulegać pokusom, zachować kulturę słowa i nie przekraczać dozwolonych granic.

Pamiętajmy, że tylko wtedy będziemy bezpieczni w Sieci.

Dyrekcja:

Opracowały:

Iwona Szyszkowska

Ilona Słupczyńska