PROGRAM
POLITYKA BEZPIECZEŃSTWA INTERNETOWEGO
realizowany w ramach
SZKOŁY BEZPIECZNEGO INTERNETU
w Specjalnym Ośrodku Szkolno – Wychowawczym
w Nowym Dworze Gdańskim

POLITYKA BEZPIECZEŃSTWA INTERNETOWEGO Specjalnego Ośrodka Szkolno – Wychowawczego w Nowym Dworze Gdańskim określa zasady działań monitorujących zagrożenia związane z korzystaniem z technologii informacyjnych i komunikacyjnych przez wychowanków placówki, działań profilaktycznych mających na celu zapewnienie im bezpieczeństwa podczas korzystania z sieci Internet i zapobieganie cyberprzemocy oraz procedury reagowania w przypadku jej ujawnienia.

Monitorowanie

Wszystkie komputery, z których korzystają wychowankowie mają zainstalowane oprogramowanie zabezpieczające przed szkodliwymi treściami. Osobą monitorującą ich działanie jest nauczyciel informatyki.

Nauczyciele prowadzący zajęcia z wykorzystaniem TIK zwracają uwagę i natychmiast reagują na symptomy zagrożenia wychowanków szkodliwymi treściami i cyberprzemocą.

Działania profilaktyczne

Mają na celu przeciwdziałanie ewentualnym zagrożeniom poprzez edukację i działania prewencyjne prowadzone w ścisłej współpracy z rodzicami.

Adresaci:

– wychowankowie,

– nauczyciele,

– rodzice.

Działania:

a) skierowane do wychowanków

– pogadanki i wykłady, quizy, konkursy wiedzy i plastyczne związane z tematyką bezpieczeństwa w cyberprzestrzeni,

– zajęcia i pogadanki z zakresu komunikacji interpersonalnej, umiejętności radzenia sobie ze stresem, trening zastępowania agresji,

– uświadamianie znaczenia zachowania prywatności przy korzystaniu z sieci Internet,

– informowanie wychowanków, jak mają reagować i gdzie mogą szukać pomocy w przypadku zetknięcia się z przejawami cyberprzemocy,

- dopuszczanie anonimowych form zgłaszania informacji dotyczących aktów przemocy na terenie placówki.

- konsekwentne reagowanie na zgłaszane problemy oraz zaistniałe incydenty.

b) skierowane do nauczycieli

– zapoznanie nauczycieli z założeniami programu polityki bezpieczeństwa internetowego

– regularne szkolenia nauczycieli nt. cyberprzemocy

– wsparcie merytoryczne i organizacyjne w poruszanie tematyki bezpieczeństwa dzieci w sieci na godzinach wychowawczych,

– wsparcie merytoryczne i organizacyjne we włączaniu problematyki bezpieczeństwa internetowego do programów zajęć dydaktycznych i wychowawczych

– zapoznanie z procedurami reagowania w przypadku ujawnienia cyberprzemocy.

- niezwłoczna i zdecydowana interwencja na wszystkie przejawy przemocy w tym te z udziałem nowych technologii

c) skierowane do rodziców

– aktywne włączanie rodziców w działania podejmowane przez placówkę; poinformowanie rodziców o procedurach postępowania wobec dzieci zachowujących się agresywnie oraz stosujących przemoc z udziałem nowych technologii,

– organizowanie szkoleń i spotkań dla rodziców dotyczących tematyki bezpieczeństwa internetowego.

PROCEDURA
reagowania w sytuacji zagrożenia oraz systemu reagowania na ujawnienie cyberprzemocy

a) **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.

b) **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.

c) **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 smsowych, 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).

DZIAŁANIA WOBEC SPRAWCY CYBERPRZEMOCY:
-jeśli sprawca cyberprzemocy jest nieznany (nie jest wychowankiem placówki) 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.
- jeśli sprawca jest znany i jest on wychowankiem placówki należy przeprowadzić rozmowę w celu ustalenia okoliczności oraz przyczyn zajścia oraz poszukania rozwiązania sytuacji konfliktowej.
-wychowanek-sprawca powinien otrzymać jasny komunikat, że Ośrodek nie toleruje żadnych form przemocy.
-należy omówić skutki postępowania oraz konsekwencje, które zostaną wobec niego zastosowane.
-sprawca musi zostać zobligowany do zaprzestania jakichkolwiek form przemocy oraz dosunięcia Internetu krzywdzących materiałów.
-w rozmowie ze sprawca należy zwrócić szczególna uwagę na omówienie sposobów zadośćuczynienia wobec ofiary.
-w przypadku gdy w zdarzeniu brała udział większa grupa wychowanków, należy przeprowadzić rozmowę ze wszystkimi z osobna, zaczynając od lidera grupy.
-nie należy konfrontować sprawcy i ofiary cyberprzemocy.

e) **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 placówka powinna podjąć próbę współpracy z rodzicami i opracować wspólny plan działania, do którego zobowiązany jest wychowanek
f) objęcie sprawcy opieką psychologiczno-pedagogiczną
-praca ze sprawcą powinna opierać się na pomocy wychowankowi w zrozumieniu wyrządzonej krzywdy oraz konsekwencji swojego zachowania. Ma ona za zadanie wpłynąć na zmianę postawy i postępowania, w tym zmienić cele oraz sposób użytkowania nowych technologii.
- w trudnych, uzasadnionych przypadkach można zaproponować rodzicom oraz wychowankowi, poradę specjalisty z poza placówki bądź udział w programie terapeutycznym.

g) **zastosowanie środków dyscyplinarnych wobec wychowanka-sprawcy**
-trzeba pamiętać, że celem sankcji wobec sprawcy jest przede wszystkim zatrzymanie fali przemocy i zapewnienie poczucia bezpieczeństwa poszkodowanemu wychowankowi.
-wzbudzenie refleksji na temat swojego zachowania, zrozumienie krzywdy, skrucha, zadośćuczynienie i powstrzymanie przed podobnym zachowaniem w przyszłości.
-pokazanie innym wychowankom, że cyberprzemoc nie jest tolerowana i że placówka 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.

DZIAŁANIA WOBEC OFIARY CYBERRZEMOCY
-wsparcie psychiczne - ofiara cyberprzemocy musi otrzymać pomoc i wsparcie emocjonalne, musi także zostać zapewniona, iż placówka podejmie odpowiednie kroki w celu rozwiązania problemu.
-porada – wychowanek 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.
-monitoring - po zakończeniu interwencji warto monitorować sytuację wychowanka, 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, placówka powinna powiadomić o takiej ewentualności rodziców ofiary oraz wychowanka.

OCHRONA ŚWIADKÓW CYBERPRZEMOCY
-ważne by w wyniku interwencji świadkowie nie zostali narażeni na działania odwetowe ze strony sprawcy.
-postępowanie interwencyjne wymaga od pedagogów wyjaśniających sprawę, dyskrecji i poufnego postępowania.
-niedopuczczalne 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 wychowanek nie zgłosi informacji o zagrażającym zdarzeniu.

j) **sporządzanie dokumentacji z zajścia:**
-pedagog szkolny 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.
-jeśli rozmowa przebiegała w obecności wychowawcy (będącego w tym przypadku świadkiem) powinien on również podpisać sporządzoną notatkę.
-jeżeli zostały odnalezione i zabezpieczone dowody cyberprzemocy (wydruki, opisy smsów itp.), należy je również włączyć do dokumentacji pedagogicznej.

k) **powiadomienie sądu rodzinnego**

-jeżeli zaistniałego przypadku cyberprzemocy nie można rozwiązać przy użyciu środków wychowawczych jakimi dysponuje placówka, sprawę należy przekierować, zgłaszając ją do sądu rodzinnego z zawiadomieniem o postępowaniu w sprawach nieletnich.

-jeśli rodzice sprawcy cyberprzemocy odmawiają współpracy lub nie stawiają się w placówce, a wychowanek nie zaniechał dotychczasowego postępowania, dyrektor powinien pisemnie powiadomić o zaistniałej sytuacji sąd rodzinny, zwłaszcza jeśli napływają informacje o innych przejawach demoralizacji dziecka.

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

Zatwierdzono na Radzie Pedagogicznej w dniu 26 listopada 2010