Załącznik nr 5
do Standardów ochrony dzieci
w SOSW Nr 1 im. Marii Konopnickiej
w Otwocku

Zasady bezpiecznego korzystania z internetu i mediów elektronicznych w Specjalnym Ośrodku Szkolno-Wychowawczym Nr 1 im. Marii Konopnickiej w Otwocku

Zasady korzystania z urządzeń elektronicznych z dostępem do sieci Internet.

1. Infrastruktura sieciowa Ośrodka umożliwia dostęp do internetu, zarówno personelowi jak i dzieciom, w czasie zajęć i poza nimi.
1. Na terenie Ośrodka dostęp dziecka do Internetu możliwy jest:
   a) pod nadzorem nauczyciela szkoły na zajęciach lekcyjnych i rewalidacyjnych,
   b) pod nadzorem nauczyciela przedszkola na zajęciach wychowania przedszkolnego,
   c) pod nadzorem wychowawcy na zajęciach opiekuńczo-wychowawczych w świetlicy i grupie wychowawczej,
   d) pod nadzorem nauczyciela w bibliotece szkolnej.
2. Przy zapewnieniu dzieciom dostępu do Internetu, w Ośrodku wykorzystywane są systemy zabezpieczeń posiadające certyfikat Ogólnopolskiej Sieci Edukacyjnej (OSE).
2. Sieć jest monitorowana, tak, aby możliwe było zidentyfikowanie sprawców ewentualnych nadużyć.
3. Wyznaczona jest osoba odpowiedzialna za bezpieczeństwo sieci w Ośrodku. Do obowiązków tej osoby należą:
   a) zabezpieczenie sieci internetowej placówki przed niebezpiecznymi treściami poprzez instalację i aktualizację odpowiedniego, nowoczesnego oprogramowania,
   b) aktualizowanie oprogramowania w miarę potrzeb,
   c) sprawdzanie przynajmniej raz w miesiącu, czy na komputerach podłączonych do internetu, z których korzystają uczniowie nie znajdują się niebezpieczne treści.
4. W przypadku znalezienia niebezpiecznych treści lub niedozwolonego oprogramowania, opiekun szkolnej sieci komputerowej ustala, kto korzystał z komputera w czasie ich wprowadzania.
5. Informację o dziecku, które korzystało z komputera w czasie wprowadzania niebezpiecznych treści, opiekun szkolnej sieci komputerowej przekazuje dyrektorowi Ośrodka.
6. Na terenie Ośrodka zabrania się dzieciom:
   a) korzystania z telefonów komórkowych i innych urządzeń elektronicznych służących do przekazu informacji podczas zajęć edukacyjnych i uroczystości szkolnych;
   b) nagrywania dźwięku, obrazu oraz fotografowania za pomocą telefonu lub innych urządzeń elektronicznych.
7. Użycie urządzeń multimedialnych na zajęciach edukacyjnych i pozalekcyjnych jest możliwe za zgodą prowadzącego, jeżeli wymaga tego tok zajęć lub program nauczania.
8. Dozwolone jest użycie telefonu komórkowego na zajęciach edukacyjnych w celu ratowania życia lub zdrowia.

9. W razie niedozwolonego używania telefonu komórkowego lub innych urządzeń elektronicznych przez uczniów, mogą być zastosowane kary, o których mowa w statutach przedszkola i poszczególnych szkół.
10. Regulamin korzystania z internetu przez dzieci znajduje się w pracowni informatycznej, w świetlicowych kącikach informatycznych, bibliotece szkolnej.
11. W przypadku dostępu realizowanego pod nadzorem pracownika placówki, ma on obowiązek informowania dzieci o zasadach bezpiecznego korzystania z internetu.
12. Pracownik Ośrodka czuwa także nad bezpieczeństwem korzystania z internetu przez dzieci podczas zajęć.
13. Ośrodek zapewnia stały dostęp do materiałów edukacyjnych, dotyczących bezpiecznego korzystania z internetu.
14. W miarę możliwości na zajęciach z wychowawcą klasy/grupy przeprowadzane są z dziećmi cykliczne warsztaty dotyczące bezpiecznego korzystania z internetu.

Procedury ochrony dzieci przed cyberprzemocą

1. Podstawowe formy zjawiska cyberprzemocy 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.
2. W przypadku uzyskania od dziecka informacji o cyberprzemocy pracownik powinien poinformować o zdarzeniu wychowawcę klasy/grupy lub pedagoga/psychologa.
3. Procedura reagowania wobec sprawcy przemocy, gdy jest nim uczeń/wychowanek Ośrodka:
   a) powiadomienie przez wychowawcę klasy/grupy pedagoga lub psychologa,
   b) powiadomienie przez pedagoga/psychologa rodziców/opiekunów sprawcy,
   c) podjęcie działań zmierzających do rozwiązania sytuacji konfliktowej, w tym przeprowadzenie rozmowy w celu ustalenia okoliczności zdarzenia i przyczyn takiego zachowania, zobowiązanie sprawcy do zaprzestania stosowania cyberprzemocy,
   d) zastosowanie konsekwencji regulaminowych wynikających ze Statutu (w tym powiadomienie policji w przypadku, gdy doszło do przemocy na terenie Ośrodka),
   e) zapewnienie sprawcy pomocy psychologicznej,
   f) monitorowanie zachowania ofiary, sprawcy (rozmowy wychowawczo-wspierające z częstotliwością wynikającą z indywidualnej postawy dziecka, zgodnie z ustaleniami).
4. Procedura reagowania wobec ofiary cyberprzemocy, jeśli zdarzenie zostało zgłoszone do wychowawcy lub pedagoga/psychologa:
   a) rozmowa pedagoga lub psychologa z ofiarą cyberprzemocy, udzielenie wsparcia zrozumienie dla jego uczuć, w tym trudności z ujawnieniem okoliczności wydarzenia, strachu, wstydu poinformowanie o podjętych procedurach interwencyjnych i środkach zapewniających mu bezpieczeństwo, (podczas rozmowy z uczniem zgłaszającym, że jest on ofiarą cyberprzemocy, należy zapewnić go, że 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),
   b) ustalenie okoliczności i zabezpieczenie dowodów (wydruk, zrzut ekranu, zapis strony)

c) poinformowanie przez psychologa lub pedagoga rodziców poszkodowanego o zdarzeniu, podjętych działaniach oraz wskazanie możliwości uzyskania pomocy, w tym złożenie zawiadomienia na policji),
d) w przypadku, gdy cyberprzemoc miała miejsce na terenie Ośrodka , dyrektor ma obowiązek powiadomić o zdarzeniu odpowiedni wydział policji,
e) zapewnienie opieki psychologiczno-pedagogicznej poszkodowanemu dziecku na terenie Ośrodka,
f) monitorowanie sytuacji dziecka (rozmowy z psychologiem z częstotliwością zależną od indywidualnych potrzeb dziecka),
g) w przypadku, gdy sprawca jest nieznany dyrektor Ośrodka podejmuje starania o niezwłoczne przerwanie cyberprzemocy, np. poprzez zawiadomienie administratora serwera) oraz powiadamia policję.

5. Podejmowane działania interwencyjne powinny być w miarę możliwości prowadzone jednocześnie w odniesieniu do sprawcy i ofiary
6. Realizując procedurę należy unikać działań, które mogłyby wtórnie stygmatyzować ofiarę lub sprawcę, np.: wywoływania ucznia z lekcji, konfrontowania ofiary i sprawcy.
7. Należy zadbać o bezpieczeństwo świadków zdarzenia, zwłaszcza, jeśli byli oni osobami ujawniającymi cyberprzemoc.
8. W każdej sytuacji, w trakcie ustalania okoliczności, należy ustalić charakter zdarzenia (rozmiar i rangę szkody, jednorazowość/powtarzalność) i dokonać oceny, czy zdarzenie to wyczerpuje znamiona cyberprzemocy, czy jest np. niezbyt udanym żartem (wówczas należy podjąć działania profilaktyczne mające na celu niedopuszczenie do eskalacji tego typu zachowań).
9. Samo wystąpienie zjawiska cyberprzemocy nie jest jednoznaczne z koniecznością zaangażowania policji i sądu rodzinnego – działania pracowników Ośrodka powinny umożliwiać rozwiązanie sytuacji problemowej na poziomie pracy wychowawczej.
10. Ośrodek powiadomi odpowiednie służby (np. policję, sąd rodzinny), gdy wykorzysta wszystkie dostępne środki wychowawcze a ich zastosowanie nie przyniesie pożądanych rezultatów (np. nie ma zmian postawy ucznia).
11. W przypadku stwierdzenia, że zostało naruszone prawo (groźba karalna – art. 190 kk, uporczywe nękanie, podszywanie się – art. 190a kk, zmuszanie do określonego działania – art. 191 kk, naruszenie intymności seksualnej, utrwalenie wizerunku nagiej osoby bez jej zgody – art. 191a kk, zniesławienie – art. 212 kk, zniewaga – art. 216 kk) powiadamiana jest policja.
12. Zgłoszenia naruszenia prawa dokonuje dyrektor Ośrodka.

Postępowanie w przypadku podejrzenia,
że dziecko jest uczestnikiem niebezpiecznej gry

1. W przypadku podejrzenia, że dziecko jest uczestnikiem niebezpiecznej gry w sieci należy niezwłocznie powiadomić dyrektora Ośrodka oraz rodziców/opiekunów dziecka.
2. Rozmowę z dzieckiem przeprowadza psycholog dzieckiem w celu ustalenia okoliczności przystąpienia do gry oraz w miarę możliwości kontaktów z innymi uczestnikami.

3. W miarę możliwości należy rozeznać czy dziecko nie posiada śladów mogących świadczyć o uczestnictwie w niebezpiecznych grach, np. samookaleczeń, w razie konieczności zapewnić opiekę lekarską.
4. Nie należy usuwać pod żadnym pozorem ujawnionych danych w postaci wiadomości (sms, e-mail, chat itp.), w miarę możliwości należy zabezpieczyć treści poprzez ich zapisanie, wydrukowanie, itp.
5. Podejrzenie uczestnictwa dziecka w niebezpiecznej grze dyrektor Ośrodka przekazuje policji w celu wyjaśnienia.

Eliza Trzcińska -Przybysz

Elektronicznie podpisany przez Eliza Trzcińska-Przybysz
Data: 2024.02.27 11:28:20 +01'00'