Procedury ochrony dzieci przed treściami szkodliwymi w Internecie oraz utrwalonymi w innej formie (Rozdział 8 Standardy Ochrony Małoletnich w Prywatnym Liceum Ogólnokształcącym dla Dorosłych „PRZYSZŁOŚĆ” w Bydgoszczy)

Procedury ochrony dzieci przed treściami szkodliwymi w Internecie oraz utrwalonymi w innej formie (Rozdział 8 Standardy Ochrony Małoletnich w Prywatnym Liceum Ogólnokształcącym dla Dorosłych „PRZYSZŁOŚĆ” w Bydgoszczy

I. Niebezpieczne treści (materiały pornograficzne, promujące nienawiść, rasizm, ksenofobię, przemoc, zachowania autodestrukcyjne)

1. Treści nielegalne lub niezgodne z regulaminem danej strony zgłaszane są administratorom strony.
2. W przypadku zgłoszenia o dostępie do treści nieodpowiednich, administrator sieci ustala okoliczności zdarzenia, podejmując próbę ustalenia sprawcy i świadków incydentu, a także zabezpiecza dowody, konfiguruje zabezpieczenia sieci szkolnej, by na nowo zablokować dostęp do niewłaściwych treści. Z poczynionych ustaleń sporządza *Kartę przebiegu interwencji*.
3. Jeśli treści niebezpieczne dotyczą osób niezwiązanych ze szkołą, dyrektor zgłasza zdarzenie odpowiednim służbom (sądowi rodzinnemu lub Policji), przekazując zabezpieczone materiały.
4. Jeśli uczestnikami zdarzenia są uczniowie szkoły, ze sprawcą i ofiarą przeprowadzona jest rozmowa (oddzielnie) psychologa lub pedagoga szkolnego na temat emocji, jakie może budzić materiał, do jakich zachowań zachęca, omówione zostają także konsekwencje zdarzenia wynikających ze złamania statutu szkoły.
5. Powiadomieni zostają rodzice uczniów, których informuje się o poczynionych ustaleniach i dalszych działaniach szkoły (zastosowane kary statutowe/ środki oddziaływania wychowawczego, powiadomienie organów ścigania, wsparcie psychologiczno - pedagogiczne).
6. Współpraca z organami ścigania lub sądem rodzinnym obligatoryjnie musi zaistnieć w przypadku naruszenia zakazu rozpowszechniania materiałów pornograficznych z udziałem małoletniego (osoby poniżej 18 roku życia – art. 202 § 3 kodeksu karnego) oraz treści propagujących publicznie faszystowski lub inny totalitarny ustrój państwa lub

nawołujących do nienawiści na tle różnic narodowościowych, etnicznych, rasowych, wyznaniowych (art. 256 i art. 257 kodeksu karnego).

II. Ochrona wizerunku

1. W szkole na początku roku szkolnego pozyskiwane są pisemne zgody rodziców i uczniów na publikację wizerunku uczniów na potrzeby dokumentacji fotograficznej działań podejmowanych przez placówkę. W miarę możliwości fotografowane są grupy uczniów, a nie pojedyncze osoby.
2. Zdjęcia i nagrania nie są podpisywane informacjami identyfikującymi ucznia z imienia i nazwiska.
3. Nośniki analogowe zawierające zdjęcia i nagrania uczniów są przechowywane w zamkniętej na klucz szafce, a nośniki elektroniczne zawierające zdjęcia i nagrania są przechowywane w folderze chronionym z dostępem ograniczonym do osób uprawnionych przez instytucję u administratora sieci, przez okres wymagany przepisami prawa o archiwizacji.
4. Nie dopuszczalne jest przechowywanie zdjęć i nagrań z wizerunkiem uczniów na nośnikach nieszyfrowanych lub mobilnych (telefonach komórkowych i pendrive).

III. Naruszenie prywatności

1. Informacja o zagrożeniu naruszeniem prywatności w szkole powinna zostać niezwłocznie przekazana administratorowi systemów informatycznych i dyrektorowi szkoły, którzy podejmują natychmiastowe działania w celu zabezpieczenia danych i ograniczenia dalszego dostępu do informacji niejawnych.
2. Następnie należy ustalić okoliczności zdarzenia, poprzez dokładne udokumentowanie pozyskanych informacji i skontaktować się z ekspertem ds. bezpieczeństwa cyfrowego w organie prowadzącym szkołę.
3. W przypadku poważniejszych zagrożeń i w sytuacji, gdy naruszenie prywatności jest spowodowane przez osoby spoza szkoły, należy nawiązać współpracę z organami ścigania.
4. Osoba wskazana w Rozdziale 1 ust. 6 powiadamia osoby dotknięte zdarzeniem (których dane osobowe wyciekły) o sytuacji, by podjęły indywidualne środki zaradcze.

IV. Cyberprzemoc

1. Uczeń, który stał się ofiarą lub świadkiem cyberprzemocy (wyśmiewania, poniżania uczestników społeczności szkolnej przy użyciu technologii cyfrowych, obraźliwych komentarzy, rozpowszechniania wizerunku, manipulowania zdjęciami itp.) powinien zgłosić sytuację do wychowawcy klasy lub pedagoga/psychologa szkolnego. Zgłoszenia może dokonać także świadek cyberprzemocy.
2. Przedstawiciel personelu, do którego dotarła informacja próbuje ustalić okoliczności zdarzenia, zebrać dowody w postaci zrzutów ekranu, wiadomości, komentarzy, zdjęć, adresów stron internetowych. Zebrane materiały przekazywane są osobie wskazanej w rozdziale 1 ust. 5, która wykonuje Kartę przebiegu interwencji.
3. O zdarzeniu poinformowani zostają rodzice, którzy wspólnie z administratorem sieci i koordynatorem ds. Standardów ustalają, czy sytuacja wymaga powiadomienia organów ścigania i czy odpowiedzialnym za to będzie rodzic czy szkoła.
4. Pedagog/ psycholog szkolny udziela pomocy psychologiczno – pedagogicznej ofierze, wyjaśniając również rolę szkoły w przeciwdziałaniu zjawisku cyberprzemocy i kolejne etapy postępowania szkoły.
5. Jeśli sprawcą jest uczeń szkoły, pedagog lub psycholog szkolny powinien przeprowadzić z nim rozmowę, w wyniku której ustali, czy istnieją przesłanki do zgłoszenia sprawy do sądu rodzinnego lub Policji (przestępstwa ścigane z urzędu), czy wystarczające będzie zastosowanie kar statutowych/ środków oddziaływania wychowawczego.

V. Fake news

2. Włączenie zagadnienia dezinformacji do tematów działalności profilaktycznej, w tym ramach realizacji zajęć z informatyki, celem wspierania umiejętności medialnych.
3. Prowadzenie kontroli mediów społecznościowych pod względem działań mających na celu ograniczenie rozpowszechniania fake newsów oraz sprawdzanie publikowanych w sieci treści.
4. Reagowanie na potencjalne zagrożenie – prostowanie informacji, zgłaszanie administratorowi strony, jeśli treści są nielegalne lub niezgodne z regulaminem.