

Załącznik nr 1 do Zarządzenia nr 1/10/2024

Dyrektora Regionalnej Placówki Opiekuńczo – Terapeutycznej „Tęczowy Domek” w Rzeszowie
w sprawie Standardów Ochrony Małoletnich

Regulamin korzystania z Internetu

1. Podopieczni Regionalnej Placówki Opiekuńczo Terapeutycznej „Tęczowy Domek” (dalej jako: „Placówka”) z Internetu, na terenie Placówki, korzystają za pomocą urządzeń mobilnych i stacjonarnych zapewnionych i skonfigurowanych przez Placówkę – na zasadach określonych w niniejszym Regulaminie.
2. Placówka zapewniając podopiecznym dostęp do Internetu podejmuje działania zabezpieczające podopiecznych przed dostępem do treści nielegalnych, szkodliwych i dla nich nieodpowiednich oraz zabezpieczające podopiecznych przed narażaniem na szkodliwe i nieodpowiednie kontakty online oraz usługi online, a także przed narażeniem na szkodliwe i ryzykowane zachowania w sieci Internet.
3. Do treści nielegalnych zalicza się m.in.: materiały przedstawiające seksualne wykorzystanie dziecka, materiały przedstawiające twardą pornografię, treści propagujące rasizm i inne nielegalne treści – treści nie dotyczące żadnej z powyższych kategorii, ale skierowane przeciwko bezpieczeństwu dzieci, na przykład: propagowanie lub pochwalanie zachowań o charakterze pedofilskim, materiały utrwalające wizerunek nagiej osoby lub osoby w trakcie czynności seksualnej przy użyciu przemocy, groźby bezprawnej lub podstępnej albo rozpowszechniane bez jej zgody, treści pornograficzne udostępniane dziecku, uwodzenie dziecka poniżej 15 r.ż. przez Internet, tzw. child grooming, zjawisko szantażu na tle seksualnym.
4. Do treści szkodliwych i nieodpowiednich zalicza się m.in. treści obrazujące przemoc, obrażenia fizyczne, prezentujące drastyczne sceny, śmierć, okrucieństwo wobec zwierząt, treści nawołujące do podejmowania działań autodestrukcyjnych (samookaleczeń, pro-ana, samobójstw, zażywania szkodliwych substancji, w tym środków psychoaktywnych niezidentyfikowanych jednoznacznie jako narkotyki itp.), treści nawołujące do przemocy, przestępczości, radykalizacji (również sekty) i ekstremizmu, patostreamy, treści dyskryminacyjne oraz pornograficzne.
5. Do zachowań rodzących narażenie na szkodliwe i nieodpowiednie kontakty online oraz usługi online zalicza się m.in. presję rówieśniczą, cyberprzemoc, grooming, szantaż na tle seksualnym, aktywność seksualną jako źródło dochodu osób nieletnich, hazard online, reklamy niedostosowane do wieku, media społecznościowe niedostosowane do wieku oraz podejmowanie wyzwań online, seksting, wywieranie presji, stosowanie przemocy z wykorzystaniem technologii informacyjnych i komunikacyjnych.
6. Na terenie Placówki dostęp podopiecznego do Internetu możliwy jest jedynie:
 - a) pod bezpośrednim nadzorem pracownika na zajęciach oraz podczas rozmów na aplikacji ZOOM na urządzeniach stacjonarnych,
 - b) bez bezpośredniego nadzoru pracownika – na przeznaczonych do tego urządzeniach mobilnych.
7. Na terenie Placówki, z zastrzeżeniem pkt. 5 dostęp podopiecznego do Internetu możliwy jest jedynie za pomocą sieci WIFI Placówki, po podaniu hasła i akceptacji Regulaminu, a urządzenia mobilne zapewniane podopiecznym nie są wyposażone w kartę SIM.
8. W wyjątkowych przypadkach, z uwagi na wiek i potrzeby podopiecznego Dyrektor Placówki, na wniosek wychowawcy może wyrazić pisemną zgodę na zainstalowanie w urządzeniu mobilnym danego podopiecznego karty SIM, umożliwiającej nawiązywanie połączeń telefonicznych oraz wysyłanie wiadomości SMS i MMS oraz dostęp do Internetu poza siecią WIFI Placówki.
9. Podopieczni z urządzeń z dostępem do Internetu na terenie Placówki korzystają w wymiarze czasowym i zgodnie z harmonogramem ustalonym przez wychowawców.
10. W nagłych i uzasadnionych przypadkach (np. sytuacje zdrowotne, rodzinne) możliwe jest korzystanie z urządzeń z dostępem do Internetu poza wyznaczonymi godzinami, po uprzednim uzgodnieniu z opiekunem lub wychowawcą.
11. W przypadku wyjazdów lub wycieczek poza teren Placówki zasady korzystania z urządzeń mobilnych z dostępem do Internetu będą każdorazowo ustalane przez wychowawców lub Dyrektora.
12. Urządzenia mobilne z dostępem do Internetu przechowywane są pod nadzorem wychowawców w miejscu niedostępnym dla podopiecznych.

13. Korzystanie z mediów społecznościowych przez podopiecznego, o ile jest zgodne z Regulaminem danej aplikacji, jest możliwe jedynie po uzyskaniu zgody wychowawcy pedagoga oraz pod ich nadzorem.
14. W ramach mediów społecznościowych podopieczni nie mogą:
 - a) kontaktować się z nieznajomymi,
 - b) akceptować zaproszeń od osób nieznanych osobiście,
 - c) udostępniać prywatnych informacji lub zdjęć, materiałów video lub audio,
 - d) udostępniać adresu zamieszkania i danych kontaktowych,
 - e) udostępniać informacji o Placówce,
 - f) danych dotyczących innych podopiecznych i personelu Placówki.
15. Wychowawcy mają obowiązek informowania podopiecznych o zasadach bezpiecznego korzystania z Internetu i mediów społecznościowych.
16. Placówka zapewnia stały dostęp do materiałów edukacyjnych, dotyczących bezpiecznego korzystania z Internetu, a Informatyk przeprowadza w tym zakresie cykliczne szkolenia z personelem i podopiecznymi.
17. Informatyk podejmuje działania, aby sieć internetowa była zabezpieczona przed zagrożeniami cyfrowymi i uniemożliwiała dostęp do treści nielegalnych, szkodliwych i nieodpowiednich dla podopiecznych, w szczególności poprzez instalowanie i aktualizację odpowiedniego oprogramowania oraz zapewnia na wszystkich urządzeniach z dostępem do Internetu na terenie Placówki:
 - a) oprogramowanie filtrujące treści internetowe – aplikacja mOchrona,
 - b) oprogramowanie monitorujące korzystanie przez podopiecznych z Internetu – aplikacja mOchrona,
 - c) oprogramowanie antywirusowe,
 - d) oprogramowanie antyspamowe,
 - e) firewall,
18. Aplikacja mOchrona standardowo blokuje dostęp do następujących kategorii nieodpowiednich treści:
 - a) Pornografia i treści dla dorosłych
 - a) Przemoc i drastyczne treści
 - b) Hazard i zakłady online
 - c) Narkotyki i inne substancje odurzające
 - d) Broń i materiały wybuchowe
 - e) Ekstremizm i radykalne ideologie
 - f) Strony promujące anoreksję i bulimię
 - g) Nielegalne oprogramowanie i piractwo
 - h) Strony phishingowe i oszustwa internetowe
 - i) Treści zawierające mowę nienawiści
 - j) Fora i czaty bez moderacji
 - k) Strony promujące samookaleczenie lub samobójstwo
 - l) Nieodpowiednie gry online (z przemocą, hazardem itp.)
 - m) Strony z alkoholem i tytoniem
 - n) Treści związane z okrucieństwem wobec zwierząt
19. Aplikacja mOchrona umożliwia wychowawcom:
 - a) włączanie lub wyłączanie blokady dla poszczególnych kategorii treści,
 - b) dodawanie własne strony do czarnej listy,
 - c) tworzenie białej listy dozwolonych stron, dostosowywanie poziomu ochrony w zależności od wieku i potrzeb dziecka, z których to uprawnień wychowawcy powinni korzystać w porozumieniu z pedagogiem stosownie do potrzeb i sytuacji danego podopiecznego.
20. Dodatkowo, aplikacja mOchrona wykorzystuje zaawansowane algorytmy do analizy treści w czasie rzeczywistym, co pozwala na blokowanie nowych, nieznanych wcześniej stron z nieodpowiednimi treściami.
21. Urządzenia z dostępem do Internetu są cyklicznie sprawdzane przez Informatyka, nie rzadziej niż raz w miesiącu, czy nie znajdują się na nich niebezpieczne oprogramowanie i nieodpowiednie treści, oraz czy ich oprogramowanie jest aktualne.
22. Urządzenia mobilne z dostępem do Internetu są raz w tygodniu fizycznie sprawdzane przez wychowawcę danego podopiecznego, czy nie znajdują się na nich niebezpieczne oprogramowanie i nieodpowiednie treści – zgodnie z Instrukcją przygotowaną przez Informatyka – Załącznik nr 1 do niniejszego Regulaminu.
23. Urządzenia mobilne z dostępem do Internetu, które mają zainstalowane kartę SIM są codziennie sprawdzane przez wychowawcę danego podopiecznego, czy nie znajdują się na nich niebezpieczne oprogramowanie

i nieodpowiednie treści – zgodnie z Instrukcją przygotowaną przez Informatyka – Załącznik nr 1 do niniejszego Regulaminu.

24. Bieżąca kontrola nad treściami internetowymi, do których dostęp mają poszczególni podopieczni, dokonywana za pomocą oprogramowania filtrującego treści internetowe i monitorującego korzystanie przez podopiecznych z Internetu sprawowana jest przez wychowawcę danego podopiecznego.
25. Nadzór nad sprawowaniem kontroli, o której mowa powyżej należy do obowiązków Pedagoga, któremu zapewniony jest dostęp do aplikacji mOchrona wszystkich podopiecznych Placówki.
26. Pedagog za pomocą aplikacji mOchrona dokonuje cyklicznych sprawdzeń – nie rzadziej niż raz na miesiąc, czy podopieczni nie uzyskują dostępu do treści internetowych dla nich nie przeznaczonych.

Załączniki:

- Instrukcja sprawdzania urządzeń mobilnych.

Załącznik nr 1 do Regulaminu Korzystania z Internetu
Sprawdzanie zabezpieczeń na telefonie podopiecznego

Lista 1: Sprawdzanie w panelu mOchrona na komputerze

Logujemy się na komputerze lub innym urządzeniu z dostępem do panelu rodzica mOchrony klikamy na ikonę dziecka i po kolei sprawdzamy poniższe kategorie. Po skończonej kontroli – zaznaczamy w zeszycie kontroli.

1. Aktywność w Internecie:
 - a. Przejrzyj historię przeglądanych stron
 - b. Sprawdź, czy nie ma odwiedzin na nieodpowiednich stronach
2. Używane aplikacje:
 - a. Sprawdź listę zainstalowanych aplikacji
 - b. Zwróć uwagę na nowe lub nieznane aplikacje
3. Czas korzystania z urządzenia:
 - a. Sprawdź, ile czasu dziecko spędza na telefonie
 - b. Przeanalizuj, jakie aplikacje są najczęściej używane
4. Lokalizacja:
 - a. Sprawdź historię lokalizacji urządzenia
 - b. Upewnij się, że miejsca przebywania są znane i bezpieczne
5. Filtry treści:
 - a. Sprawdź, czy filtry blokujące nieodpowiednie treści są włączone
 - b. W razie potrzeby dostosuj ustawienia filtrów

Lista 2: Sprawdzanie bezpośrednio na telefonie

- 1) Media społecznościowe:
 - (a) Otwórz aplikacje społecznościowe i sprawdź ustawienia prywatności
 - (b) Przejrzyj listy znajomych, zwracając uwagę na nieznane osoby
- 2) Wiadomości i komunikatory:
 - a) Sprawdź, czy nie ma podejrzanych rozmów z nieznanymi
 - b) Zwróć uwagę na treść wiadomości pod kątem potencjalnych zagrożeń
- 3) Zdjęcia i filmy:
 - a) Przejrzyj galerię zdjęć i filmów
 - b) Upewnij się, że nie ma nieodpowiednich lub ryzykownych materiałów
- 4) Zabezpieczenia telefonu:
 - a) Sprawdź, czy telefon ma ustawione hasło, kod PIN lub blokadę biometryczną
 - b) Upewnij się, że antywirus jest zainstalowany i aktywny (w przypadku Androida)
- 5) Ustawienia prywatności systemu:
 - a) Sprawdź uprawnienia aplikacji (dostęp do kamery, mikrofonu, lokalizacji)
 - b) Upewnij się, że funkcje udostępniania lokalizacji są odpowiednio skonfigurowane
- 6) Stan fizyczny telefonu:
 - a) Sprawdź czy telefon jest kompletny i nie nosi śladów fizycznej ingerencji.
 - b) Sprawdź czy w telefonie zainstalowana jest karta SIM lub karta pamięci.

Pamiętaj, aby podczas sprawdzania telefonu szanować prywatność dziecka i przeprowadzać kontrolę w atmosferze zaufania i otwartej komunikacji. Celem jest zapewnienie bezpieczeństwa, a nie inwigilacja.

W wypadku stwierdzenia nieprawidłowości należy niezwłocznie zawiadomić pedagoga oraz Informatyka oraz sporządzić na tę okoliczność notatkę służbową (notatka służbowa – załącznik nr 1 do Polityki Ochrony Małoletnich).