



***Załącznik nr 5 do do Polityki ochrony małoletnich przed krzywdzeniem
w Fundacji Edukacji Społecznej EKOS i Szkołach Fundacji EKOS w Swarzędzu***

I. Zasady korzystania z Internetu i mediów elektronicznych

1. Infrastruktura sieciowa Fundacji i Szkół umożliwia dostęp do Internetu, zarówno personelowi, jak i małoletnim, w tym uczniom, w czasie zajęć w ramach szkolnej sieci WIFI oraz sieci komputerów stacjonarnych.
2. Na wszystkich komputerach z dostępem do Internetu na terenie Szkoły jest zainstalowane oraz systematycznie aktualizowane oprogramowanie antywirusowe.
3. Dostęp ucznia do szkolnego Internetu możliwy jest pod nadzorem nauczyciela na lekcjach z informatyki i innych zajęciach edukacyjnych w ramach sieci WIFI.
4. Uczeń może korzystać z Internetu na komputerach z zainstalowanym programem filtrującym treści lub na swoim komputerze w ramach sieci WIFI, po uprzednim zapoznaniu się i podpisaniu zasad bezpiecznego korzystania ze szkolnej sieci WIFI i podaniu adresu IP.
5. Korzystanie z multimediów, Internetu i programów użytkowych służy wyłącznie celom informacyjnym i edukacyjnym.
6. Uczeń obsługuje sprzęt komputerowy zgodnie z zaleceniami nauczyciela, zgodnie z obowiązującym regulaminem i instrukcją korzystania z komputerów.
7. Uczeń samowolnie bez nadzoru nauczyciela prowadzącego zajęcia nie może podłączać żadnych urządzeń do komputerów szkolnych w tym pendrive'ów, telefonów, kart SD Micro, dysków itp. urządzeń pod USB i innych portów.
8. Pracownicy mają obowiązek informowania małoletnich o zasadach bezpiecznego korzystania z Internetu. Nauczyciele czuwają także nad bezpieczeństwem korzystania z Internetu przez małoletnich podczas lekcji.
9. Szkoła zapewnia stały dostęp do materiałów edukacyjnych, dotyczących bezpiecznego korzystania z Internetu.
10. Pracownicy, a także pracownicy zewnętrznego serwisu komputerowego, kontrolują czy na komputerach podłączonych do Internetu, nie znalazły się niebezpieczne treści. W przypadku ich znalezienia, jeżeli jest to możliwe, ustalają kto korzystał z komputera w czasie ich wprowadzenia. Informacje o dokonanych ustaleniach przekazują Prezesowi Fundacji lub Dyrektorowi Szkół. Prezes Fundacji lub Dyrektor Szkół niezwłocznie aranżują dla ucznia rozmowę z psychologiem lub pedagogiem. Jeżeli w jej wyniku pedagog/psycholog uzyska informację, że małoletni ma związek z cyberprzemocą, podejmuje działania zgodnie z procedurą interwencji.



II. Zasady korzystania z urządzeń elektronicznych

11. Korzystanie z telefonów komórkowych i innych urządzeń elektronicznych przez uczniów w Szkole i na terenie szkolnym odbywa się na zasadach określonych w Statucie Szkoły.
12. Szkoła nie ponosi odpowiedzialności za zaginięcie lub zniszczenie czy kradzież sprzętu przynieszonego przez uczniów.
13. Uczeń ma obowiązek wyłączyć lub wyciszyć telefon (bez wibracji) i schować go w torbie/plecaku przed rozpoczęciem zajęć edukacyjnych.
14. Telefony i inne urządzenia elektroniczne (np. tablety, komputery) można wykorzystywać podczas zajęć lekcyjnych w celach dydaktycznych pod opieką oraz za zgodą nauczyciela prowadzącego zajęcia. Uczeń może korzystać z telefonu, a także innych urządzeń elektronicznych w celu wyszukania informacji niezbędnych do realizacji zadań podczas zajęć, po uzyskaniu zgody nauczyciela prowadzącego dane zajęcia lub na jego polecenie.
15. Na terenie Szkoły zakazuje się uczniom filmowania, fotografowania oraz utrwalania dźwięku na jakichkolwiek nośnikach cyfrowych, chyba że za zgodą Prezesa Fundacji, nauczyciela lub Dyrektora Szkół.
16. Niedopuszczalne jest przysyłanie treści obrażających inne osoby.
17. Jeśli istnieje możliwość zabrania telefonu i/lub innego urządzenia elektronicznego na wycieczkę, wyjście edukacyjne uczeń ma prawo korzystania z tych urządzeń wyłącznie w zakresie nie wpływającym na organizację i przebieg tego przedsięwzięcia.
18. Podczas wyjść zorganizowanych przez Szkołę (teatr, kino, muzeum, filharmonia, zwiedzanie z przewodnikiem, lekcja w terenie, konkursy, zawody sportowe itp.) uczeń jest zobowiązany do wyłączenia/wyciszenia telefonu (bez wibracji) i schowania go.
20. W przypadkach przewidzianych w Statucie Szkoły telefon zostaje przekazany do Sekretariatu, z którego może zostać odebrany przez rodzica/ opiekuna prawnego ucznia.
21. W szczególnych przypadkach uzasadnionych trudnościami w samokontroli lub funkcjonowaniu ucznia, dopuszcza się zawarcie indywidualnego kontraktu wychowawczego pomiędzy uczniem, jego rodzicami a wychowawcą klasy.
22. Postanowienia kontraktu, o którym mowa w pkt 21, w porozumieniu i za zgodą rodziców, mogą zobowiązywać ucznia do każdorazowego pozostawiania telefonu komórkowego (lub innego urządzenia cyfrowego) w Sekretariacie Szkoły w depozycie na cały czas trwania jego

zajęć edukacyjnych w danym dniu, jeżeli działanie to ma mieć pozytywny, terapeutyczno-wychowawczy wpływ na jego funkcjonowanie i koncentrację w Szkole.

23. W przypadku naruszenia przez ucznia zasad korzystania z telefonu komórkowego fakt ten zostaje odnotowany w dzienniku elektronicznym w formie upomnienia lub nagany. Gdy naruszenia się powtarzają, Dyrektor na wniosek wychowawcy klasy może określić dla ucznia indywidualnie zasady korzystania z telefonu i innych urządzeń.

III. Zasady zabezpieczania materiału dowodowego w sprawach o cyberprzemoc i hejt

21. W przypadku ujawnienia hejtu, nękania rówieśniczego w sieci, upublicznienia wizerunku bez zgody lub innych cyberprzestępstw wobec uczniów, osoba odpowiedzialna za Internet lub inny wyznaczony pracownik Szkoły dokonuje niezwłocznego zabezpieczenia materiału dowodowego. Jeśli dowody znajdują się na urządzeniu prywatnym ucznia, ich okazanie i zabezpieczenie odbywa się w jego obecności.

22. Zabezpieczenie dowodów cyfrowych polega na:

- a. utrwaleniu widoku ekranu (screenshot): wykonaniu zrzutów ekranu w taki sposób, aby widoczna była pełna treść (np. wpis, komentarz, wiadomość), data i godzina zdarzenia, pełna nazwa profilu lub pseudonim sprawcy oraz, jeśli to możliwe, adres URL strony internetowej,
- b. zapisie technicznym: zgraniu materiałów wideo, plików audio lub wiadomości e-mail (wraz z nagłówkami wiadomości) na zabezpieczony, służbowy nośnik pamięci (np. pendrive) przechowywany wraz z dokumentacją interwencji w osobnej, dedykowanej i poufnej teczce interwencyjnej, która jest przechowywana i zabezpieczona przed dostępem osób nieuprawnionych przez osobę odpowiedzialną za *Politykę ochrony małoletnich* w placówce (Koordynatora ds. standardów),
- c. sporządzeniu protokołu: osoba zabezpieczająca sporządza krótką notatkę służbową, wskazując: datę, godzinę, źródło (np. nazwa aplikacji: Messenger, Instagram, TikTok), metodę zabezpieczenia i nazwiska osób obecnych przy tej czynności.

23. Zabezpieczone materiały stanowią informację poufną. Mogą być udostępnione wyłącznie Dyrektorowi Szkoły, zespołowi interwencyjnemu, organom ścigania/sądowi lub rodzicom poszkodowanego małoletniego. Pracownikom zabrania się przesyłania tych materiałów za pośrednictwem prywatnych urządzeń i kont osobistych.

IV. Zasady ochrony małoletnich przed treściami szkodliwymi i zagrożeniami z sieci

24. Fundacja i Szkoły mają obowiązek podejmować działania zabezpieczające małoletnich przed łatwym dostępem do tych treści z sieci, które mogą zagrażać ich prawidłowemu rozwojowi.

25. Pod pojęciem „treści szkodliwe i zagrożenia z sieci” rozumiane są: treści szkodliwe, niedozwolone, nielegalne i niebezpieczne dla zdrowia (pornografia, treści obrazujące przemoc, promujące działania szkodliwe dla zdrowia i życia małoletnich, popularyzujące ideologię faszystowską i działalność niezgodną z prawem, nawołujące do samookaleczeń i samobójstw, korzystania z narkotyków, treści stwarzające niebezpieczeństwo werbunku małoletnich do organizacji nielegalnych i terrorystycznych, różne formy cyberprzemocy, np. 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).

26. Podstawowe działania podejmowane przez Fundację i Szkoły zabezpieczające małoletnich przed dostępem do treści szkodliwych i zagrożeń z sieci:

- a. monitorowanie działania i aktualizowanie programu antywirusowego, zapory sieciowej, stosowanie filtrów antyspamowych,
- b. instalowanie aplikacji filtrujących na każdym komputerze, z którego korzystają pracownicy i uczniowie,
- c. edukacja medialna – dostarczanie małoletnim wiedzy i umiejętności dotyczących posługiwania się technologią komunikacyjną,
- d. prowadzenie systematycznych działań wychowawczych (integracja zespołu klasowego, budowanie dobrych relacji pomiędzy uczniami, wprowadzanie norm grupowych, odróżnianie dobra od zła),
- e. prowadzenie działań profilaktycznych propagujących zasady bezpiecznego korzystania z sieci oraz uświadamiających zagrożenia płynące z użytkowania różnych technologii komunikacyjnych,
- f. włączenie rodziców uczniów w działania Szkół na rzecz zapobiegania cyberprzemocy- poinformowanie ich o polityce Szkół w zakresie reagowania na cyberprzemoc, edukacja na temat cyberprzemocy i zagrożeń z sieci: warsztaty, szkolenia dla rodziców, udostępnianie materiałów i publikacji, w tym polecanie i wskazywanie sposobów instalowania ochrony rodzicielskiej,
- g. podejmowanie interwencji w każdym przypadku ujawnienia lub podejrzenia cyberprzemocy lub ujawnienie niebezpiecznych treści.