Załącznik nr 5 do ***Polityki ochrony dzieci przed krzywdzeniem w szkołach Fundacji EKOS w Swarzędz***

Zasady korzystania z Internetu i mediów elektronicznych

1. Infrastruktura sieciowa Szkół umożliwia dostęp do Internetu, zarówno personelowi, jak i 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. Na terenie Szkół 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 Szkół mają obowiązek informowania dzieci o zasadach bezpiecznego korzystania z Internetu. Nauczyciele czuwają także nad bezpieczeństwem korzystania z Internetu przez dzieci podczas lekcji.

9. Szkoła zapewnia stały dostęp do materiałów edukacyjnych, dotyczących bezpiecznego korzystania z Internetu.

10. Pracownicy Szkół, 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 dyrektorowi Szkół. Dyrektor Szkół niezwłocznie aranżuje

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.

Zasady korzystania z urządzeń elektronicznych

1. Uczniowie przynoszą do szkoły telefony komórkowe oraz inny sprzęt elektroniczny na własną odpowiedzialność, za zgodą rodziców.

2. Szkoła nie ponosi odpowiedzialności za zaginięcie lub zniszczenie czy kradzież sprzętu przynoszonego przez uczniów.

3. Uczeń ma obowiązek wyłączyć lub wyciszyć telefon (bez wibracji) i schować go w torbie/plecaku przed rozpoczęciem zajęć edukacyjnych.

4. 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.

5. Na terenie szkoły zakazuje się uczniom filmowania, fotografowania oraz utrwalania dźwięku na jakichkolwiek nośnikach cyfrowych, chyba, że jest uzasadnione merytorycznie i za zgodą nauczyciela lub Dyrektora Szkół.

6. Niedopuszczalne jest przesyłanie treści obrażających inne osoby.

7. 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.

8. 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.

9. W przypadku naruszenia przez ucznia zasad korzystania z telefonu komórkowego fakt ten zostaje odnotowany w dzienniku elektronicznym w formie upomnienia lub nagany,

10. W szczególnych przypadkach telefon zostaje przekazany do Sekretariatu, z którego może zostać odebrany przez rodzica/ opiekuna prawnego ucznia.

Zasady ochrony małoletnich przed treściami szkodliwymi i zagrożeniami z sieci

1. Szkoła ma obowiązek podejmować działania zabezpieczające dzieci przed łatwym dostępem do tych treści z sieci, które mogą zagrażać ich prawidłowemu rozwojowi.

2. 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 dzieci, popularyzujące ideologię faszystowską i działalność niezgodną z prawem, nawołujące do samookaleczeń i samobójstw, korzystania z narkotyków, treści stwarzające niebezpieczeństwo werbunku dzieci 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).

3. Podstawowe działania podejmowane przez szkołę zabezpieczające dzieci 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 dzieciom 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.