Załącznik do Zarządzenia nr 6/2023/2024
Dyrektora Niepublicznej Szkoły Podstawowej nr 7
im. Marii Skłodowskiej-Curie w Słupsku
z 8 kwietnia 2024 r.

Zasady bezpiecznego korzystania z Internetu i mediów elektronicznych

§ 1. Przepisy ogólne.

1. Celem przepisów jest zapewnienie bezpiecznego i odpowiedzialnego korzystania z Internetu, ochrona ich prywatności oraz rozwijanie świadomości cyfrowej uczniów Niepublicznej Szkoły Podstawowej im. Marii Skłodowskiej-Curie w Słupsku.
2. Przepisy dotyczą wszystkich form korzystania z Internetu w Szkole.

§ 2. Potencjalne zagrożenia.

1. Do potencjalnych zagrożeń płynących z użytkowania sieci należy zaliczyć:
   1) dostęp do treści niezgodnych z celami wychowania i edukacji (m.in. narkotyki, przemoc, pornografia, hazard);
   2) działalność innych użytkowników zagrażająca dobru uczniów;
   3) oprogramowanie umożliwiające śledzenie i pozyskanie danych osobowych użytkowników szkolnej sieci.

§ 3. Zasady korzystania z urządzeń elektronicznych z dostępem do Internetu.

1. Infrastruktura sieciowa Szkoły umożliwia dostęp do Internetu, zarówno personelowi, jak i uczniom w czasie zajęć.
2. Rozwiązania organizacyjne na poziomie Szkoły bazują na aktualnych standardach bezpieczeństwa.
3. Komputery uczniowskie z dostępem do Internetu na terenie Szkoły korzystają z zabezpieczeń OSE (Ogólnopolska Sieć Edukacyjna) oraz programu antywirusowego z usługą filtrowania szkodliwych treści.
4. Za bezpieczeństwo sieci w Szkole odpowiada Administrator systemów i sprzętu komputerowego.
5. Do obowiązków pracownika, o którym mowa w ust. 4 należą:
   1) zabezpieczenie sieci internetowej przed niebezpiecznymi treściami;
   2) monitorowanie ruchu sieciowego;
   3) zgłaszanie nieetycznych incydentów do Dyrektora Szkoły i CERT.
6. Na terenie Szkoły dostęp ucznia do Internetu możliwy jest pod nadzorem nauczyciela na zajęciach lekcyjnych z dostępem do komputera.
7. Korzystanie z multimediów, Internetu i programów użytkowych podczas zajęć lekcyjnych służy wyłącznie celom informacyjnym i edukacyjnym.
8. Uczeń obsługuje sprzęt komputerowy zgodnie z zaleceniami nauczyciela, z obowiązującym regulaminem pracowni komputerowej.
9. Użytkownikowi komputera zabrania się:
   1) instalowania oprogramowania oraz dokonywania zmian w konfiguracji oprogramowania zainstalowanego w systemie;
   2) usuwania cudzych plików, odinstalowania programów, dekompletowania sprzętu;
   3) dotykania kabli, montażu i demontażu elementów komputera i innych urządzeń znajdujących się w pracowni komputerowej.

§ 4. Zasady korzystania z telefonów komórkowych oraz innych urządzeń elektronicznych

1. Zgodnie z zapisami Statutu Szkoły, a jej terenie obowiązuje uczniów zakaz korzystania z telefonów komórkowych oraz z innych urządzeń elektronicznych.

2. Przez pojęcie „telefon komórkowy” rozumie się także smartfon, urządzenie typu smartwatch, itp.
3. Przez pojęcie „inne urządzenia elektroniczne” rozumie się także tablet, odtwarzacz muzyki, dyktafon, kamerę, aparat cyfrowy, słuchawki, itp.
4. Uczniowie przynoszą do Szkoły telefony komórkowe oraz inny sprzęt elektroniczny na własną odpowiedzialność i za zgodą rodziców.
5. Szkoła nie ponosi odpowiedzialności za zaginięcie lub zniszczenie, czy kradzież sprzętu przynoszonego przez uczniów.
6. Uczniowie nie mogą korzystać bez zgody nauczyciela z telefonu komórkowego oraz innych urządzeń elektronicznych z dostępem do Internetu podczas zajęć edukacyjnych, opiekuńczych, treningów, uroczystości, a także zajęć pozalekcyjnych organizowanych na terenie Szkoły.
7. Telefony i inne urządzenia elektroniczne (np. tablety, laptopy, itp) można wykorzystywać podczas zajęć lekcyjnych w celach dydaktycznych pod opieką oraz za zgodą i w formie określonej przez prowadzącego zajęcia.
8. Na terenie Szkoły zakazuje się uczniom filmowania, fotografowania oraz utrwalania dźwięku na jakichkolwiek nośnikach cyfrowych.
9. W szczególnych przypadkach nagrywanie zajęć edukacyjnych oraz utrwalanie ich w jakikolwiek sposób możliwe jest wyłącznie po uzyskaniu zgody Dyrektora Szkoły lub nauczyciela prowadzącego zajęcia edukacyjne.
10. Nagrywanie dźwięku i obrazu za pomocą telefonu lub innych urządzeń jest możliwe jedynie za wyraźną zgodą osoby nagrywanej lub fotografowanej. Niedopuszczalne jest nagrywanie lub fotografowanie sytuacji niezgodnych z powszechnie przyjętymi normami etycznymi i społecznymi oraz przesyłanie treści obrażających inne osoby.

§ 5. Zasady ochrony uczniów przed treściami szkodliwymi i zagrożeniami z sieci.

1. Pod pojęciem „treści szkodliwe i zagrożenia z sieci” rozumiane są:
   1) treści szkodliwe, niedozwolone, nielegalne i niebezpieczne dla zdrowia (pornografia, treści obrazujące przemoc, promujące działania szkodliwe dla zdrowia i życia, popularyzujące ideologię faszystowską i działalność niezgodną z prawem, nawołujące do samookaleczeń lub samobójstw, korzystania z narkotyków;
   2) treści stwarzające niebezpieczeństwo werbunku uczniów do organizacji nielegalnych lub terrorystycznych;
   3) 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.
2. Podstawowe działania zabezpieczające uczniów przed dostępem do treści szkodliwych i zagrożeń z sieci:
   1) monitorowanie działania sieci;
   2) edukacja medialna – dostarczanie uczniom wiedzy i umiejętności dotyczących posługiwania się technologią komunikacyjną, prowadzenie działań profilaktycznych propagujących zasady bezpiecznego korzystania z sieci oraz uświadamiających zagrożenia płynące z użytkowania różnych technologii komunikacyjnych;
   3) prowadzenie systematycznych działań wychowawczych (integracja zespołu klasowego, budowanie dobrych relacji pomiędzy uczniami, wprowadzanie norm grupowych; uczenie uczniów odróżniania dobra od zła);
   4) włączenie rodziców uczniów w działania Szkoły na rzecz zapobiegania cyberprzemocy – poinformowanie ich o polityce szkoły 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;
   5) podejmowanie interwencji w każdym przypadku ujawnienia lub podejrzenia cyberprzemocy lub ujawnienie niebezpiecznych treści, która obejmuje:

a) ustalenie okoliczności zdarzenia,
b) zabezpieczenie dowodów,
c) poinformowanie o sytuacji opiekunów uczniów będących uczestnikami zdarzenia,
d) objęcie pomocą poszkodowanego ucznia,
e) podjęcie działań wobec agresorów, w tym zastosowanie środków dyscyplinujących zgodnie ze Statutem Szkoły i rodzajem przewinienia;
f) powiadomienie policji, gdy sprawa jest poważna, zostało złamane prawo lub sprawca nie jest uczniem Szkoły i jego tożsamość nie jest nikomu znana;
g) jeśli mimo zastosowanych działań, niepożądane zachowania nadal mają miejsce, przekazanie informacji do sądu rodzinnego z podejrzeniem demoralizacji małoletniego.

Niniejsze **Zasady bezpiecznego korzystania z Internetu i mediów elektronicznych w**chodzą w życie 15 kwietnia 2024 r.