Załącznik Nr 7 do Zarządzenia Nr 07/2024
Dyrektora II Liceum Ogólnokształcącego im. Ziemi Olkuskiej w Olkuszu
z dnia 18 czerwca 2024r.

STANDARDY OCHORNY MAŁOLETNICH
w II Liceum Ogólnokształcącym
im. Ziemi Olkuskiej
w Olkuszu

- wymogi dotyczące bezpiecznych relacji między małoletnimi oraz zasady korzystania z urządzeń z dostępem do sieci Internet i ochrony przed treściami szkodliwymi i zagrożeniami z tym związanymi

I. Ogólne zasady komunikacji i zachowania

§ 1

1. Zasady komunikacji między małoletnimi, jak również uczniami Szkoły nie będącym małoletnimi:

1) Każdy zasługuje na uważne słuchanie, empatię oraz postawę wyrażającą szacunek;

2) Nie wolno zawstydzać, upokarzać, lekceważyć i obrażać małoletniego;

3) Każdy uczeń, w tym małoletni wyraża własne poglądy, oceny i spojrzenie na świat w sposób wolny od agresji i przemocy oraz nikomu nie wyrządza krzywdy.

2. Małoletni jeżeli jest świadkiem stosowania przez inną osobę wobec ucznia Szkoły, w szczególności małoletniego jakiejkolwiek formy agresji lub przemocy, powinien reagować na nią, np: jeśli jest to możliwe pomagają ofierze, szukając pomocy u osoby dorosłej, zgłaszając zdarzenie personelowi Szkoły;

3. Małoletni jest zobowiązany do respektowania praw i wolności osobistych swoich kolegów i koleżanek, ich prawa do własnego zdania, popełniania błędów, do własnych poglądów, wyglądu i zachowania – w ramach społecznie przyjętych norm i wartości.

4. Uczeń, w tym małoletni uznaje prawo innych do odmienności i zachowania tożsamości ze względu na cechy rodzinne, wiek, płeć, orientację seksualną, cechy fizyczne, niepełnosprawność, pochodzenie etniczne, geograficzne, narodowe, religię, status ekonomiczny.

5. We wzajemnym kontakcie uczniowie w tym małoletni zachowują wysoką kulturę.

Używają zwrotów grzecznościowych typu proszę, dziękuję, przepraszam.

6. Uczniowie budują wzajemnie relacje poprzez wzajemne zrozumienie oraz konstruktywne, bez krzywdzenia, w tym użycia siły rozwiązywanie problemów i konfliktów między sobą.

II. Inne zachowania niedozwolone

§ 2

1) Nie jest dopuszczalne ujawnianie danych wrażliwych dotyczących małoletniego, wyszczególnionych w art. 9 ust. 1 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (Dz.U. UE.L. z 2016 r. Nr 119, poz. 1), obejmujących w szczególności pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe oraz przetwarzania danych genetycznych, danych biometrycznych w celu jednoznacznego zidentyfikowania osoby fizycznej lub danych dotyczących zdrowia, seksualności lub orientacji seksualnej tej osoby;

2) Zachowania niedozwolone obejmują używanie agresji i przemocy, wulgarnych słów, gestów oraz żartów, czynienie uwag, które stanowią, lub mogą być odebrane jako nawiązywanie w wypowiedziach do aktywności bądź atrakcyjności seksualnej;

4) Niedozwolone jest wykorzystywanie relacji wynikającej z zależności lub przewagi fizycznej (zastraszanie, przymuszanie, groźby).

5) Nie jest dozwolone utrwalanie wizerunku innych osób dla celów prywatnych poprzez filmowanie, nagrywanie głosu, fotografowanie.

6) Nie jest dozwolone przynoszenie do Szkoły i/lub proponowanie alkoholu, wyrobów tytoniowych ani substancji psychoaktywnych/odurzających jak również ich używanie.

7) Niedozwolone jest również:

a) pisanie obraźliwych, poniżających, wulgarnych, niecenzuralnych lub zawierających groźby treści na ścianach, meblach, drzwiach itp., a także w mediach społecznościowych, w wiadomościach tekstowych, a także stosowanie cyberprzemocy;

b) niszczyć, nie szanować własności innych osób;

c) kradzież, przywłaszczać sobie przedmiotów;

d) grożenie, wyłudzanie pieniędzy lub innych korzyści;

e) rozwiązywanie konfliktów w sposób siłowy i wykorzystywać przewagi fizycznej;

f) szykanowanie innych osób z jakiegokolwiek powodu, a także wykluczanie, izolowanie, manipulowanie, obniżanie statusu innej osoby w grupie;

g) śledzenie, szpiegowanie, zmuszanie do określonego zachowania się

h) upublicznianie materiałów i fotografii bez zgody widocznych na nich osób;
i) przynoszenie do Szkoły niebezpiecznych przedmiotów i substancji;

III. Zasady korzystana z urządzeń elektronicznych z dostępem do sieci Internet

§ 3

1. Zasady używania urządzeń elektronicznych z dostępem do siedzi Internet, w tym telefonów komórkowych na terenie Szkoły określa Statut Szkoły. Zasady te służą m.in. ochronie małoletnich przed treściami szkodliwymi i zagrożeniami w sieci Internet oraz przetwarzanymi w innej formie.
2. Uczniowie przynoszą do szkoły telefony komórkowe oraz inny sprzęt elektroniczny na własną odpowiedzialność i za zgodą opiekunów.
3. 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.
4. Na terenie szkoły dostęp małoletniego ucznia do Internetu możliwy jest pod nadzorem nauczyciela na zajęciach lekcyjnych z dostępem do komputera. Korzystanie z multimediów, Internetu i programów użytkowych podczas zajęć lekcyjnych służy wyłącznie celom informacyjnym i edukacyjnym.
5. Rozwiązania organizacyjne dotyczące dostępu do sieci Internet na poziomie Szkoły bazują na aktualnych standardach bezpieczeństwa.
6. Na wszystkich komputerach z dostępem do Internetu na terenie szkoły monitorowany jest ruch sieciowy.
7. W szkole wyznaczony jest pracownik odpowiedzialny za bezpieczeństwo sieci.
8. Do obowiązków pracownika, o którym mowa w ust. 8 należą:
a) zabezpieczenie szkolnej sieci internetowej przed niebezpiecznymi treściami;
b) monitorowanie szkolnego ruchu sieciowego;
c) zgłaszanie ujawnionych nieetycznych incydentów.
9. Małoletni uczeń obsługuje sprzęt komputerowy zgodnie z zaleceniami personelu Szkoły, przy czym każdemu użytkownikowi zabrania się:
a) instalowania oprogramowania oraz dokonywania zmian w konfiguracji oprogramowania zainstalowanego w systemie,
b) usuwania cudzych plików, odinstalowania programów, dekompletowania sprzętu,
c) dotykania kabli, montażu i demontażu elementów komputera, drukarek, i innych urządzeń znajdujących się w Szkole.

IV. Zagrożenia w sieci Internet

§ 4

1. Bezpieczne korzystanie z urządzeń elektronicznych z dostępem do sieci Internet obejmuje następujące zasady, które Szkoła upowszechniana:

1) nie podawania przez małoletnich swoich danych osobowych, takich jak: imię, nazwisko, numer telefonu czy adres bez wiedzy ich opiekunów;

2) rozważnego rozpowszechnianie swojego wizerunku – informowanie małoletnich, iż w przypadku publikacji zdjęć w sieci należy mieć na uwadze, aby dostęp do nich miały wyłącznie osoby znajome oraz o ryzyku związanym z udostępnianiem zdjęć nieznajomym, w szczególności zdjęć intymnych, czy w niepełnym ubraniu;

3) nie atakowania nikogo w sieci, niezależnie od tego, jakie zdanie wyraża. Zaniechanie agresji, w tym słownej;

4) nie korzystania z sieci przez zbyt długi czas, bo zbyt długie korzystanie z urządzeń elektronicznych, w szczególności komputera, tabletu czy smartfona może zaszkodzić zdrowiu.

5) dłuższe korzystanie z sieci Internet, oznacza rzadszy kontakt bezpośredni, a takie kontakty są najbardziej wartościowe.

2. Małoletni są informowani o możliwości zgłoszenia opiekunom lub personelowi Szkoły o napotkaniu przez nich w sieci Internet treści, które wydają się szkodliwe, czy w jakikolwiek sposób wywołują niepokój małoletniego;

3. Małoletni są informowani o możliwości zgłoszenia opiekunom lub personelowi Szkoły otrzymanych przez małoletniego propozycji spotkania, od osób z którymi kontakt małoletni nawiązał i utrzymuje wyłącznie przy pomocy sieci Internet.

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

§ 5

1. Pod pojęciem „treści szkodliwe i zagrożenia z sieci” rozumiane są:

a) 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 i samobójstw, korzystania z narkotyków;

b) treści stwarzające niebezpieczeństwo werbunku uczniów do organizacji nielegalnych i terrorystycznych;

c) 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 małoletnich przed dostępem do treści szkodliwych i zagrożeń z sieci:

a) monitorowanie ruchu sieciowego w szkolnej sieci Internet;

b) prowadzenie systematycznych działań wychowawczych i edukacji medialnej – 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 oraz cyberprzemocy i działań niepożądanych, w tym informowania o skutkach działań m.in. środków dyscyplinujących wynikających ze Statutu Szkoły i przepisów prawa oraz określonych rodzajów przewinień;

c) stosowanie środków dyscyplinujących wynikających ze Statutu Szkoły;

d) powiadomienie organów ścigania w przypadku podejrzenia iż zostało złamane prawo lub sprawca nie jest uczniem szkoły i jego tożsamość nie jest nikomu znana oraz jeśli mimo zastosowanych działań, niepożądane zachowania nadal mają miejsce, przekazanie informacji do sądu rodzinnego z podejrzeniem demoralizacji małoletniego.