Załącznik nr 3

Zasady bezpiecznego korzystania z internetu i mediów elektronicznych w I Liceum Ogólnokształcącym

im. Józefa Ignacego Kraszewskiego w Białej Podlaskiej

1. Infrastruktura sieciowa placówki umożliwia dostęp do internetu, zarówno personelowi, jak i dzieciom w czasie zajęć i poza nimi.
2. Sieć jest monitorowana, tak aby możliwe było zidentyfikowanie sprawców ewentualnych nadużyć.
3. Rozwiązania organizacyjne na poziomie placówki bazują na aktualnych standardach bezpieczeństwa.
4. Wyznaczona jest osoba odpowiedzialna za bezpieczeństwo sieci w instytucji.

Do obowiązków tej osoby należą:

a) Zabezpieczenie sieci internetowej placówki przed niebezpiecznymi treściami poprzez instalację i aktualizację odpowiedniego, nowoczesnego oprogramowania.
b) Aktualizowanie oprogramowania w miarę potrzeb.
c) Przynajmniej raz w miesiącu sprawdzanie, czy na komputerach ze swobodnym dostępem podłączonych do internetu nie znajdują się niebezpieczne treści. W przypadku znalezienia niebezpiecznych treści wyznaczony pracownik stara się ustalić, kto korzystał z komputera w czasie ich wprowadzenia. Informację o dziecku, które korzystało z komputera w czasie wprowadzenia niebezpiecznych treści, wyznaczony pracownik przekazuje kierownictwu, które aranżuje dla dziecka rozmowę z psychologiem lub pedagogiem na te- mat bezpieczeństwa w internecie. Jeżeli w wyniku przeprowadzonej rozmowy psycholog/pedagog uzyska informację, że dziecko jest krzywdzone, podejmuje działania opisane w procedurze interwencji.

5. Istnieje regulamin korzystania z internetu przez dzieci oraz procedura określająca działania, które należy podjąć w sytuacji znalezienia niebezpiecznych treści na komputerze.
6. W przypadku dostępu realizowanego pod nadzorem pracownika placówki ma on obowiązek informowania dzieci o zasadach bezpiecznego korzystania z internetu. Pracownik placówki czuwa także nad bezpieczeństwem korzystania z sieci przez dzieci podczas zajęć.
7. W miarę możliwości osoba odpowiedzialna za internet przeprowadza z dziećmi rozmowy dotyczące bezpiecznego korzystania z niego.
8. Placówka zapewnia stały dostęp do materiałów edukacyjnych dotyczących bezpiecznego korzystania z internetu, przy komputerach, z których możliwy jest swobodny dostęp do sieci.

Reguły bezpiecznego korzystania z internetu

1. Ogranicz dane osobowe, które udostępniasz w sieci.
2. Używaj silnych i unikalnych haseł.
3. Używaj weryfikacji dwuetapowej.
4. Korzystaj z bezpiecznej skrzynki pocztowej.
5. Skasuj niepotrzebne/nieużywane konta.
6. Uważaj na phishing i ransomware − podejrzane maile i esemesy.

- ✓ wpisuj adres banku lub innej instytucji ręcznie − nie korzystaj z linków otrzymanych mailem lub esemesem;
- ✓ przed zalogowaniem się sprawdź czy jesteś na autentycznej i zabezpieczonej stronie − czy jest chroniona certyfikatem SSL (świadczy o tym ikona zamkniętej kłódki); kliknij na kłódkę przy adresie URL i sprawdź, czy certyfikat został wystawiony dla Twojego banku, biura maklerskiego lub instytucji publicznej;
- ✓ ostrożnie szukaj strony do logowania przy pomocy wyszukiwarki www − przestępcy umieszczają w reklamach linki prowadzące do podstawionych stron, które do złudzenia przypominają prawdziwe, a służą do wyłudzania danych do logowania;
- ✓ pobieraj aplikacje − przede wszystkim służące do korzystania z bankowości mobilnej − tylko z oficjalnych sklepów (Google Play, AppStore) lub ze strony usługodawcy.

7. Zainstaluj mocny program antywirusowy.
8. Unikaj przeglądania stron bez certyfikatu SSL.
9. Zwiększ ustawienia prywatności na swoich kontach w mediach społecznościowych.
10. Aktualizuj system operacyjny i programy.
11. Zabezpiecz router i sieć WiFi.
12. Bezpiecznie używaj sieci.
13. Zdobywaj wiedzę na temat bezpieczeństwa w sieci.

Szkolna procedura postępowania w przypadku ujawnienia treści szkodliwych/ cyberprzemocy

1. Ujawnienie przypadku.
2. Ustalenie okoliczności zdarzenia.
3. Powiadomienie dyrektora oraz szkolnego administratora sieci komputerowej.
4. Zabezpieczenie dowodów
5. Analiza zdarzenia

- ✓ Powiadomienie policji (w zależności od rodzaju ujawnionych treści);
- ✓ zastosowanie się do zaleceń policji/prokuratury alternatywnie
- ✓ wyjaśnienie konsekwencji wynikających przechowywaniem, instalowaniem bądź kopiowaniem treści szkodliwych.

6. Usunięcie treści szkodliwych jeśli jest to w gestii szkolnego administratora sieci Komputerowej. Naprawa systemu.