ZASADY BEZPIECZEŃSTWA W INTERNECIE

W ZESPOLE SZKÓŁ W POŁCZYNIE-ZDROJU

I. Zasady ogólne

1. Uczniowie mogą korzystać z Internetu na komputerach przeznaczonych dla uczniów w pracowniach komputerowych, pracowni architektury krajobrazu, pracowni podstaw gastronomii i bibliotece szkolnej.
2. Internet może być wykorzystywany wyłącznie do celów edukacyjnych, informacyjnych oraz do poszukiwań bibliograficznych.
3. Korzystanie z dostępu do Internetu ogranicza się do przeglądania zasobów sieci przy pomocy przeglądarki zainstalowanej na dysku lokalnym komputera.
4. Zabrania się korzystania z programów peer to peer, peer to mail, torrent, rapidshare, emule, kaza itp. umożliwiających wymianę materiałów z innym członkami sieci chronionych prawem autorskim.
5. Korzystanie z Internetu jest bezpłatne.

II. Zasady użytkowania sprzętu komputerowego i dostępu do Internetu

1. Użytkownik korzystający ze stanowiska komputerowego jest odpowiedzialny za powierzony sprzęt i zainstalowane oprogramowanie.
2. Niedozwolone są wszelkie działania powodujące uszkodzenie komputera, wprowadzanie jakichkolwiek zmian w konfiguracji, łamanie zabezpieczeń systemu oraz świadome wprowadzanie wirusów komputerowych do systemu.
3. Ściągnięte z Internetu pliki lub programy oraz teksty własne można zapisywać na pendrive lub dysku za zgodą nauczyciela.
4. Zabrania się:
    a. instalowania gier,
    b. otwierania stron zawierających treści niezgodne z obowiązującymi normami etyczno- moralnymi, propagujące przemoc i rasizm,
    c. korzystania z serwerów CHAT i innych komunikatorów internetowych,
    d. używania bramek sms,

e. wchodzenia na strony zawierające pirackie oprogramowanie.

5. **Nauczyciele mają prawo kontrolować czynności wykonywane przez użytkownika przy komputerze.**

III. Zasady bezpieczeństwa.

1. Nie otwieraj plików nieznanego pochodzenia.

2. Nie wysyłaj w e-mailach żadnych poufnych danych, nieznanych linków i załączników e-mail.

3. Staraj się nie odwiedzać zbyt często stron, które oferują niesamowite atrakcje (pieniądze, darmowe filmiki, muzykę, albo łatwy zarobek przy rozsyłaniu spamu) - często na takich stronach znajdują się ukryte wirusy, trojany i inne zagrożenia.

4. Używaj oprogramowania przeciw wirusom i spyware. Najlepiej stosuj ochronę w czasie rzeczywistym.

5. Aktualizuj - oprogramowanie oraz bazy danych wirusów (dowiedz się czy twój program do ochrony przed wirusami posiada taką funkcję i robi to automatycznie, często nie mają jej programy darmowe).

6. Nie korzystaj ze stron banków, poczty elektronicznej czy portali społecznościowych, które nie mają ważnego certyfikatu, chyba, że masz stuprocentową pewność z innego źródła, że strona taka jest bezpieczna.

7. Nie używaj niesprawdzonych programów zabezpieczających czy też do publikowania własnych plików w Internecie (mogą one np. podłączać niechciane linijki kodu do źródła strony).

8. Co jakiś czas skanuj komputer i sprawdzaj procesy sieciowe - jeśli się na tym nie znasz poproś o sprawdzenie kogoś, kto się zna. Czasami złośliwe oprogramowanie nawiązujące własne połączenia z Internetem, wysyłające twoje hasła i inne prywatne dane do sieci może się zainstalować na komputerze mimo dobrej ochrony - należy je wykryć i zlikwidować.

9. Sprawdzaj pliki pobrane z Internetu za pomocą skanera, nawet jeśli wydają się niezarażone (ostrożności nigdy za wiele).

10. Pamiętaj o uruchomieniu firewalla. Najlepiej na poziomie średniej ochrony
    z możliwością ustalania reguł. Jeżeli nie jesteś pewien czy sobie poradzisz
    z ręczną obsługą reguł, możesz ustawić średni lub nawet wysoki poziom ochrony.

11. Ważna zasada dotycząca bezpieczeństwa osobistego: nie zostawiaj danych osobowych w niesprawdzonych serwisach i na stronach, jeżeli nie masz absolutnej pewności, że nie są one widoczne dla osób trzecich. Nie przekazuj numerów telefonów, adresów domowych. Używaj pseudonimów.

12. Pamiętaj, że żaden bank nie wysyła e-maili do swoich klientów z prośbą
    o podanie hasła lub loginu w celu ich weryfikacji.

13. Kiedy korzystasz z chmur, załóż, że wysłane tam treści nie są już prywatne.
14. Nie korzystaj z uniwersalnych haseł, szczególnie w przypadku usług w chmurach.
15. Wykorzystując materiały z Internetu wykorzystywane do przygotowania min. prezentacji na lekcji, referatów itp. podawaj źródło pochodzenia.
16. Szyfruj dane przed wysłaniem (zadbaj również o kopie bezpieczeństwa).
17. Netykieta – szanuj innych użytkowników Internetu, traktuj ich tak jak chcesz żeby oni traktowali ciebie.
18. Nauczyciel może odmówić użytkownikowi dostępu lub zażądać odejścia od komputera, jeśli uzna, że jego zachowanie zagraża bezpieczeństwu systemu, lub sprzętu.

IV. Odpowiedzialność użytkowników

1. Użytkownik ponosi pełną odpowiedzialność za wszelkie szkody przez niego spowodowane w lokalnych systemach komputerowych oraz wszelkie inne straty lub nadużycia popełnione przy użyciu udostępnionych mu zasobów Internetu i programów użytkowych.
2. Nauczyciel może odmówić użytkownikowi dostępu do komputera i Internetu, jeśli uzna, iż wykonuje on czynności niepożądane nawet, jeśli nie zostały one określone w niniejszych zasadach.
3. Osoby naruszające niniejsze zasady mogą być czasowo pozbawione prawa do korzystania z zasobów internetowych.