

## BEZPIECZNA PRACA Z KOMPUTEREM I W INTERNECIE

Upowszechnianie wśród dzieci i młodzieży wiedzy o bezpieczeństwie oraz kształtowanie właściwych postaw wobec zagrożeń, w tym związanych z korzystaniem z technologii informacyjno-komunikacyjnych, jest jednym z podstawowych zadań systemu oświaty. Placówka zapewniając uczniom dostęp do Internetu, podejmuje działania zabezpieczające uczniów przed dostępem do treści, które mogą stanowić zagrożenie dla ich prawidłowego rozwoju.

**Jednak w przypadku konieczności nauki zdalnej, zapewnienie bezpieczeństwa uczniów pozostających w domu spoczywa na pełnoletnich uczniach lub rodzicach/opiekunach prawnych. Są oni także odpowiedzialni za potencjalne szkody, jakie mogą spowodować za pośrednictwem Internetu innym osobom.**

### **PONIŻEJ ZNAJDĄ PAŃSTWO WYBRANE, MOŻLIWE ZAGROŻENIA, NA KTÓRE NALEŻY ZWRÓCIĆ UWAGĘ.**

#### **Treści zagrażające rozwojowi psychicznemu i moralnemu uczniów.**

Podczas przeglądania treści potrzebnych do nauki w wynikach wyszukiwania może pojawić się strona, która nie jest przeznaczona dla uczniów niepełnoletnich. Również niektóre aplikacje sugerowane użytkownikowi strony są nieodpowiednie dla uczniów. Warto ustawić w używanych systemach operacyjnych opcje kontroli rodzicielskiej. W miarę możliwości rodzice powinni jednak towarzyszyć uczniowi podczas nauki. Jest to szczególnie ważne w przypadku młodszych uczniów.

#### **Niezweryfikowane informacje. Co jest prawdą, a co fałszem**

Podczas nauki on-line uczeń może natrafić w Internecie na informacje, które wzbudzą w nim niepokój. Ważne jest, aby omówić taką sytuację i wyjaśnić, że wiele treści zamieszczanych w sieci nie służy informowaniu, a często tylko przykuwaniu uwagi czy zwiększaniu częstotliwości odwiedzin danej strony.

#### **Reklamy**

W sieci pojawia się mnóstwo reklam, które są często profilowane dla konkretnego użytkownika. Rodzice powinni pamiętać o wynikających z tego zagrożeniach.

#### **Uzależnienie od Internetu**

Uczeń, korzystając z Internetu do nauki i zabawy, nie powinien przekraczać czasu zalecanego na pracę przy komputerze dla danej grupy wiekowej. Może to skutkować zarówno problemami z koncentracją i nauką, ale również ze zdrowiem fizycznym.

#### **Bezpieczeństwo sprzętów i dostępu do sieci**

Sprawdzajmy aktualność zabezpieczeń na komputerach i smartfonach, z których korzystają młodzi uczniowie. Istnieją darmowe programy kontroli rodzicielskiej. Każdy system operacyjny daje również możliwość ustawienia pewnych ograniczeń.

#### **Niebezpieczne kontakty**

Dzieci i młodzież, które korzystają z Internetu, szczególnie z portali społecznościowych, są narażone na kontakt z osobami mającymi złe intencje, zamierzającymi popełnić przestępstwo. Dlatego też rodzice i nauczyciele powinni szczególnie interesować się, z kim uczeń utrzymuje kontakt oraz informować o wszelkich próbach kontaktu ze strony obcych osób.

#### **Cyberprzemoc**

O wszelkich formach cyberprzemocy (słownej, nękania, podszywania się pod inne osoby) należy informować odpowiednie organy, zarówno w sytuacji, kiedy ofiarą jest uczeń, jak i wówczas, kiedy jest on świadkiem takich działań.

#### **Gry komputerowe i wideo**

Uczniowie korzystający z Internetu są również narażeni na nieodpowiednie treści zawarte w grach. Aby tego uniknąć, warto sprawdzać kategorię wiekową danej gry oraz to, czy nie zawiera np. scen przemocy, hazardu,

pornografii. Europejski system klasyfikacji gier PEGI nadaje oznaczenia wieku i treści zawartych w grze. Są one obecne praktycznie na każdej grze dostępnej on-line bądź w sklepie.

### OCHRONA DANYCH OSOBOWYCH I WIZERUNKU

Placówki pracujące na platformie epodreczniki.pl mogą być pewne, że dane osobowe uczniów są bezpieczne. Jednak zarówno uczniowie, jak i nauczyciele powinni mieć świadomość, że neodpowiedzialne logowanie się do stron komercyjnych, bez przeczytania regulaminu portali, automatyczne wyrażanie zgód na dostęp do zdjęć, filmów, kontaktów, które są w telefonie, może okazać się niebezpieczne.

Ważne jest również, aby podczas zdalnej nauki nie narazić się na nieumyślne złamanie prawa, gdy nieświadomie udostępnimy dane osobowe lub wizerunek kolegów i koleżanek ucznia. Dlatego bezwzględnie należy zapoznawać się z Regulaminami oraz Politykami bezpieczeństwa portali edukacyjnych oraz społecznościowych.

Placówka ze swej strony oferuje wsparcie i pomoc w korzystaniu z rekomendowanych przez MEN platform i aplikacji, a dane osobowe ucznia, którymi administruje podlegają ochronie zgodnie z przyjętymi politykami przetwarzania danych. Placówka stosuje środki techniczne zapewniające poufność przetwarzanych danych osobowych, jednak ze względu na publiczny charakter sieci Internet i korzystanie z usług świadczonych drogą elektroniczną, użytkownicy powinni liczyć się z zagrożeniem pozyskania i modyfikowania danych przez osoby nieuprawnione. Dlatego użytkownicy powinni również w celu podwyższenia bezpieczeństwa swojego sprzętu oraz danych stosować właściwe środki techniczne, które zminimalizują wskazane wyżej zagrożenia poprzez stosowanie programów antywirusowych i chroniących tożsamość korzystających z sieci Internet.

Dane osobowe ucznia (w szczególności jego imię i nazwisko, klasa, nazwa szkoły do której uczeń uczęszcza, oraz nazwa domeny) udostępnione usługodawcy internetowemu w celu realizacji zdalnego nauczania przez placówkę podlegają odrębnemu administrowaniu przez tego usługodawcę i do tych danych ma zastosowanie polityka prywatności usługodawcy.

Szkoła przetwarza, w tym także może udostępnić dane osobowe ucznia usługodawcy internetowemu na podstawie art.6 ust.1 lit. c) i e) RODO, w celu realizacji swoich celów ustawowych oraz wypełniając zadania realizowane w interesie publicznym.

Placówka może udostępnić dane osobowe ucznia również instytucjom uprawnionym na podstawie przepisów prawa, a także podmiotom, z którymi zawrze umowy powierzenia danych osobowych (np. realizującym wsparcie informatyczne systemu). Brak możliwości udostępnienia danych ucznia usługodawcy internetowemu uniemożliwi lub znacznie utrudni szkole realizację zdalnego nauczania.

Uczniom pełnoletnim oraz rodzicom/opiekunom prawnym uczniów niepełnoletnich przysługuje:

na podstawie art. 15 RODO prawo dostępu do danych osobowych,

na podstawie art. 16 RODO prawo do sprostowania danych osobowych,

na podstawie art. 18 RODO prawo żądania ograniczenia przetwarzania danych osobowych z zastrzeżeniem przypadków, o których mowa w art. 18 ust. 2 RODO,

prawo do wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych z siedzibą w Warszawie, ul. Stawki 2, gdy uzna, że przetwarzanie danych osobowych jej dotyczących narusza przepisy RODO.

Żądanie skorzystania z przysługujących praw w zakresie ochrony danych osobowych powinno zostać skierowane do usługodawcy internetowego administrującego platformą lub aplikacją przetwarzającą dane osobowe lub do placówki, w zależności od procesu przetwarzania, którego żądanie dotyczy.

Jednocześnie informujemy, że nie przekazujemy danych osobowych poza teren Europejskiego Obszaru Gospodarczego, z zastrzeżeniem ponadnarodowego charakteru przepływu danych w ramach usługodawców internetowych, którzy mogą przekazywać Państwa dane poza teren Europejskiego Obszaru Gospodarczego.

Jednocześnie wskazujemy, iż Facebook posiada certyfikat EU-US-Privacy Shield. W ramach umowy pomiędzy USA a Komisją Europejską ta ostatnia stwierdziła odpowiedni poziom ochrony danych w przypadku przedsiębiorstw posiadających certyfikat Privacy Shield.

W opracowaniu wykorzystano źródło:

[https://dokumenty.men.gov.pl/Kształcenie\\_na\\_odleglosc\\_%e2%80%93\\_poradnik\\_dla\\_szkol.pdf](https://dokumenty.men.gov.pl/Kształcenie_na_odleglosc_%e2%80%93_poradnik_dla_szkol.pdf)