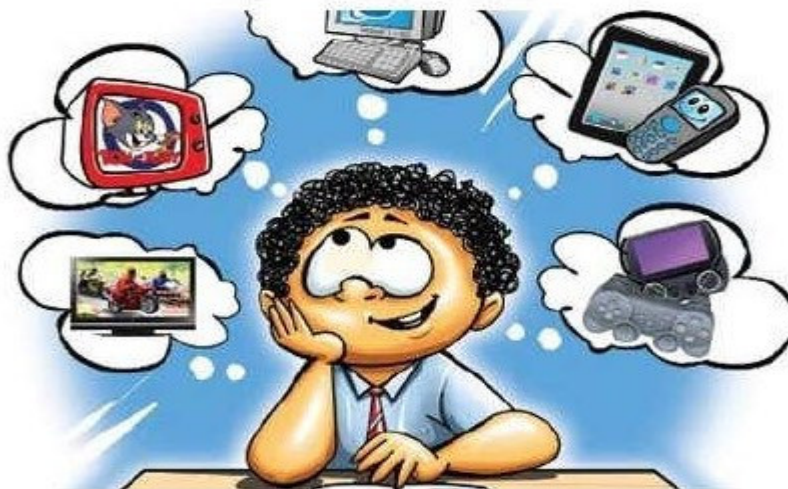


## **Informacja dla nauczycieli, uczniów i ich rodziców o kształceniu na odległość w szkole z uwzględnieniem higieny pracy uczniów i nauczycieli oraz zasad bezpieczeństwa w sieci**

Podstawa prawna: Rozporządzenie Ministra Pracy i Polityki Socjalnej z dnia 1 grudnia 1998 r. w sprawie bezpieczeństwa i higieny pracy na stanowiskach wyposażonych w monitory ekranowe. (Dz.U. 1998 nr 148 poz. 973)



### **Bezpieczeństwo i higiena pracy:**

1. Stanowisko powinno być tak zaprojektowane, aby zapewnić dostateczną przestrzeń pozwalającą na umieszczenie wszystkich elementów obsługiwanych ręcznie w zasięgu rąk;
2. Ekran monitora nie może być ustawiony naprzeciwko okna, wtedy odbija się w nim światło!;
3. Klawiatura powinna być oddalona o co najmniej 10 cm od krawędzi biurka;
4. Odległość oczu od monitora powinna wynosić od 40 cm do 75 cm;
5. W trakcie pisania nadgarstki powinny być podparte;
6. Między ramieniem a przedramieniem powinien być co najmniej kąt prosty;
7. Siedź wyprostowany, oparty, rozluźnij barki;
8. Krzesło powinno być obrotowe i posiadać podłokietniki;
9. Jeżeli masz podnózek, używaj go, zapewnia on naturalną pozycję stóp;
10. Odległość pomiędzy sąsiadującym monitorem powinna wynosić co najmniej 60 cm;
11. Wilgotność powietrza nie powinna być mniejsza niż 40%;
12. Zrób przerwę po każdej 45 minutach pracy, do 15 minut, w tym czasie najlepiej spojrzeć za okno lub najdalej położony punkt, zrób kilka przysiadów, wymachów itp.;

13. Mrugaj oczami! W czasie pracy przy komputerze nasze oczy rzadziej mrugają, więc nie są nawilżane;
14. Nasze oczy powinny znajdować się na wysokości górnej krawędzi monitora, tak aby kierować je ku dołowi, nie ku górze, dostosuj wysokość krzesła lub monitora;
15. Zainstaluj program, który dostosowuje jasność oraz barwy Twojego monitora w zależności od pory dnia i eliminuje szkodliwe światło niebieskie np. program f.lux.

### **Jak zadbać o bezpieczeństwo w sieci – dla dzieci**

1. Telefon zaufania dla dzieci to 116 111;
2. Nie ufaj osobie poznanej przez Internet. Nigdy nie możesz być pewien, kim ona naprawdę jest. Mówi, że ma 8 lat, ale może mieć 40!
3. Nie spotykaj się z osobami poznanymi przez Internet! Zawsze skonsultuj to z rodzicami;
4. Gdy coś Cię przestraszy lub zaniepokoi, wyłącz monitor i powiedz o tym dorosłemu. Powiedz też, jeśli szukając informacji, trafiłeś na stronę, która namawia do nienawiści lub do czegoś, co wyda ci się podejrzanym;
5. Nie zdradzaj nikomu swojego imienia ani adresu! Nie mów też, ile masz lat i do jakiej szkoły chodzisz. Nie podawaj numeru telefonu;
6. Wymyśl sobie jakiś fajny nick, czyli internetowy pseudonim. Nie podawaj w nim daty urodzenia ani wieku. Wykorzystaj imię bohatera ulubionego filmu lub słowo z piosenki. Użyj swojej fantazji. Na pewno wymyślisz coś ciekawego!;
7. Pomyśl kilka razy, zanim wyślesz wiadomość, e-mail czy smsa. Kiedy klikniesz „wyślij”, nie można już tego cofnąć;
8. Nie dokuczaj innym. Pamiętaj, że w Internecie obowiązuje zasada nieużywania brzydkich słów. Traktuj innych tak, jak byś chciał, żeby Ciebie traktowano;
9. Dbaj o swoje hasło jak o największą tajemnicę. Wymyśl takie, które będzie trudne do odgadnięcia. Niech to nie będzie Twoje imię ani imię najlepszej przyjaciółki;
10. Dbaj o bezpieczeństwo swoich przyjaciół. Nie podawaj nikomu ich danych, nie publikuj zdjęć bez ich zgody. Nie wiesz, jaki ktoś zrobi z nich użytek, a kiedy je wysyłasz lub umieszczasz w Internecie, nie masz już nad nimi kontroli;
11. Zabezpiecz komputer. Używaj dobrego programu antywirusowego, dbaj, by baza wirusów była aktualna. Nie otwieraj e-maili od nieznanym, nie klikaj na linki podesłane przez obcą osobę – mogą Ci zawirusować komputer!;
12. Szanuj prawo własności w Sieci. Zawsze podawaj źródło pochodzenia materiałów znalezionych w Internecie;
13. Zainstaluj program antywirusowy.

## **Jak zadbać o bezpieczeństwo w sieci – dla rodziców i nauczycieli**

1. Telefon dla rodziców i nauczycieli w sprawach bezpieczeństwa dzieci 800 100 100;
  2. Korzystaj z oprogramowania antywirusowego;
  3. Aktualizuj oprogramowanie komputerowe i mobilne;
  4. Nie instaluj w telefonie niepotrzebnych aplikacji;
  5. Otwieraj wiadomości tylko od znanych osób;
  6. Ostrożnie pobieraj pliki z sieci;
  7. Unikaj klikania w nieznane linki i załączniki w wiadomościach e-mail;
  8. Nie podawaj w sieci danych osobowych ani haseł, nie wysyłaj swoich zdjęć;
  9. Chronić swoje konta na serwisach społecznościowych;
  10. Stosuj trudne do odgadnięcia hasła, które są kombinacją liter i cyfr;
  11. Stosuj inne hasło na każdym portalu;
  12. Czytaj regulaminy;
  13. Sprawdzaj, czy strona, do której się logujesz, ma zabezpieczenie SSL, czy zaczyna się od https:/ i czy jest zamknięta kłódka obok paska adresu;
  14. Pamiętaj, że osoba po drugiej stronie nie musi być tym, za kogo się podaje;
  15. Zawsze sprawdzaj 2 razy numer konta odbiorcy, jeżeli robisz przelew przez Internet;
  16. Uważaj na “phishing” - próba wyłudzenia informacji ma miejsce wtedy, gdy ktoś próbuje nakłonić Cię do podania danych osobowych przez Internet. Wyłudzenie informacji zwykle odbywa się za pośrednictwem e-maili, reklam lub stron, które wyglądają podobnie do stron, z których już korzystasz. Ktoś, kto próbuje wyłudzić informacje, może na przykład wysłać Ci e-maila, który wygląda, jakby został wysłany przez Twój bank, i zawiera prośbę o podanie danych Twojego konta bankowego;
  17. Korzystaj z dwuetapowej weryfikacji - konfiguracja weryfikacji dwuetapowej znacznie zmniejszy szansę na uzyskanie nieautoryzowanego dostępu do konta;
  18. Jeżeli zostawiasz dziecku komputer na dłużej, możesz używać programów do kontroli rodzicielskiej;
- Ochrona danych osobowych podczas pracy zdalnej: <https://uodo.gov.pl/pl/138/1459>.

## **EWOLUCJA CZŁOWIEKA I KOMPUTERA**



