OCHRONA DANYCH OSOBOWYCH W NAUCZANIU ZDALNYM - NAUCZYCIELE

I. Przed rozpoczęciem pracy

- ✓ Zidentyfikuj użytkowników (uczniowie powinni logować się przy użyciu utworzonych kont, podobnie nauczyciele – zasadą jest, iż wyłącznie uprawnione osoby mogą być uczestnikami lekcji);
- ✓ Ustaw kamerę tak, by pokazywała wyłącznie to, co jest niezbędne do prowadzenia lekcji;
- ✓ Wykorzystuj sprzęt w sposób bezpieczny, niezależnie od tego czy jest to sprzęt służbowy, czy też prywatny. Przestrzegaj zasad bezpieczeństwa opisanych w obowiązujących w placówce procedurach i instrukcjach, a w szczególności Instrukcji ochrony danych osobowych. Przetwarzaj dane uczniów, rodziców, pracowników wyłącznie w ramach i na potrzeby realizacji obowiązków służbowych. <u>W przypadku wykorzystywania sprzętu prywatnego, podejmij dodatkowe czynności:</u>
    - przeskanowanie urządzenia aktualnym programem antywirusowym;
    - założenie osobnego profilu służbowego na swoim urządzeniu w celu separowania danych służbowych od danych prywatnych;
    - utworzenie hasła chroniącego dostęp do profilu służbowego;
    - urządzenie powinno mieć zainstalowany aktualny program antywirusowy oraz firewall;
    - sprawdź czy urządzenie posiada legalne i aktualne oprogramowanie;
    - jeśli jest taka możliwość - informatyk Palcówki, w miarę potrzeby, dokonuje innych niezbędnych czynności w oparciu o wiedzę fachową i doświadczenie zawodowe.

II. W trakcie zajęć

- ✓ Unikaj podawania danych osobowych w trakcie zajęć – uczniów, nauczycieli, rodziców;
- ✓ Jeśli pojawi się potrzeba omówienia sytuacji danego ucznia, połącz się z nim osobno – nigdy nie prowadź rozmów w sprawach indywidualnych na forum;
- ✓ Wykorzystuj rekomendowane platformy, narzędzia – polecane przez pracodawcę;
- ✓ Nie prowadź zajęć w miejscach publicznych, gdzie osoby postronne mogłyby usłyszeć fragmenty prowadzonych rozmów lub zapoznać się z fragmentami zajęć;
- ✓ Zamknij wszystkie niepotrzebne strony, aplikacje, zakładki – by uczestnicy ich nie widzieli podczas udostępniania ekranu;

III. Po zakończeniu zajęć

- ✓ <u>Upewnij się, że:</u>
- kamera i mikrofon są wyłączone;
- narzędzie służące do prowadzenia edukacji zdalnej, zostało zamknięte (nastąpiło wylogowanie się z systemu) i nie działa w tle;

IV. Dodatkowe zasady bezpieczeństwa, o których należy pamiętać

- ✓ Hasła do konta nie mogą być przekazywane osobom trzecim, w tym niedozwolone jest zapisywanie ich na kartce. Hasła powinny być bezpieczne, składające się z minimum 10 znaków, dużych i małych liter, znaków specjalnych. Nie należy używać tych samych haseł w różnych systemach informatycznych.
- ✓ <u>Gdy dzielisz komputer z domownikami, pamiętaj:</u>

- dane służbowe należy przetwarzać jedynie na wydzielonym profilu służbowym;
- po zakończeniu pracy należy każdorazowo wylogować się z profilu służbowego;
- nie należy dopuszczać domowników, w tym osób trzecich do pracy na profilu służbowym;
- nie należy przekazywać hasła do profilu służbowego domownikom, ani innym osobom trzecim;
- jeśli praca wymaga zalogowania się do baz danych – po zakończeniu pracy należy każdorazowo wylogować się z systemu;
- domowa sieć wi-fi powinna zostać zabezpieczona hasłem;
- zaleca się niekorzystanie z publicznych, otwartych sieci wi-fi w trakcie trwania pracy zdalnej.

✓ W przypadku konieczności przeniesienia danych służbowych z komputera służbowego na prywatny należy przestrzegać następujących zasad:

- jeśli dane maja zostać przeniesione na nośniku zewnętrznym – nośnik należy zaszyfrować lub zabezpieczyć znajdujące się na nim pliki i foldery hasłem;
- jeśli dane mają zostać przeniesione poprzez wiadomość e-mail – należy korzystać jedynie ze skrzynki służbowej;

✓ Jeśli w pracy zdalnej wykorzystuje się nośniki zewnętrzne:

- powinny być one przechowywane poza zasięgiem domowników i innych osób trzecich;
- w czasie przechowywania na nośnikach danych służbowych nie powinny znajdować się na nich dane prywatne;
- nośniki powinny być zaszyfrowane lub zawarte na nich pliki i foldery z danymi powinny być chronione hasłem.

PAMIĘTAJ! Praca na prywatnych urządzeniach nie upoważnia do korzystania z prywatnych skrzynek e-mail w celach służbowych. Jednocześnie zabezpieczaj dane osobowe, zwarte w przesyłanych wiadomościach e-mail poprzez: zabezpieczenie hasłem przekazywanych plików, wykorzystywanie opcji „UDW" (w przypadku wysyłki korespondencji zbiorczej), jak również upewnij się, że wpisany adres e-mail jest poprawny. Hasło do plików należy przekazywać inną drogą komunikacji (np. sms, rozmowa telefoniczna).