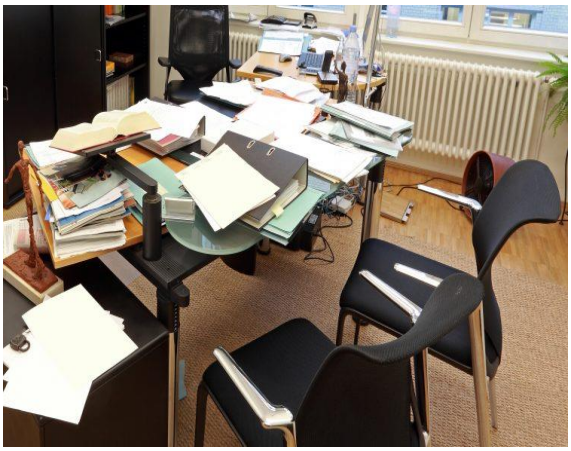
ZASADY BEZPIECZNEGO PRZETWARZANIA DANYCH

Nauczyciel przetwarza dane osobowe uczniów i ich rodziców w celu służbowym nie tylko online, ale również w formie dokumentowej.



Zasada tzw. czystego biurka.
Nauczyciel nie powinien podczas pracy zdalnej z domu pozostawiać w sposób ogólnodostępny dokumentów, które zawierają dane osobowe uczniów i ich rodziców.

Dokumenty zawierające dane osobowe niszczymy w niszczarkach.

ZABRANIA SIĘ !!!!
WYRZUCANIA NIEZNISZCZONYCH DOKUMENTÓW ZAWIERAJĄCYCH DANE OSOBOWE DO ŚMIETNIKA .

URZĄDZENIA DO PROWADZENIA NAUKI ZDALNEJ

(KOMPUTERY PRZENOŚNE, STACJE ROBOCZE)

- prywatny sprzęt jak i służbowy muszą być odpowiednio zabezpieczone, a nauczyciel powinien postępować zgodnie z polityką bezpieczeństwa lub procedurą wprowadzoną w tym zakresie w szkole,
- upewnij się, że wszystkie urządzenia z jakich korzystasz mają niezbędne aktualizacje: systemu operacyjnego, oprogramowania oraz systemu antywirusowego,

- na nauczycielu spoczywa obowiązek sprawdzenia swojego sprzętu czy spełnia podstawowe wymogi bezpieczeństwa, a w razie problemów uzyskaniem odpowiedniego stopnia bezpieczeństwa nauczyciel powinien zgłosić taki problem do dyrektora szkoły,

- pobieraj oprogramowanie wyłącznie ze stron producentów,

- zanim przystąpisz do pracy, wydziel sobie odpowiednią przestrzeń, tak aby ewentualne osoby postronne, nie miały dostępu do dokumentów, nad którymi pracujesz,

- załóż odrębne konto użytkownika, z którego będziesz korzystać tylko ty i będzie ono służyło wyłącznie do twojej pracy zdalnej, obowiązkowo zabezpiecz dostęp do swojego konta silnym hasłem dostępu,

- zabezpieczaj hasłem dostępowym piliki na komputerze, które zawierają dane osobowe,

- **polityka czystego ekranu** przed oddaleniem się od komputera, należy zablokować swoje konto użytkownika używając dwóch klawiszy **Klawisz Windows oraz L,**

- zabezpieczaj swój komputer poprzez używanie silnych haseł dostępu, wielopoziomowe uwierzytelnianie, pozwoli na ograniczenia dostępu do urządzenia, a jednocześnie na ograniczenia ryzyka utraty danych w przypadku kradzieży lub zgubienia urządzenia,

- nie umieszczaj w komputerze przypadkowo znalezionych nośników USB, na których mogą znajdować się na złośliwe oprogramowania,

- zaopatrz się w szyfrowany pendrive, który skutecznie zminimalizuje ryzyko wycieku danych w przypadku utraty i dostania się w niepowołane ręce,

- zabezpieczaj silnym hasłem dostępowym dane, które są przechowywane na urządzeniach przenośnych i nośnikach danych (np. pamięć USB),

- unikaj wchodzenia na nieznane czy przypadkowe strony internetowe,

- nie loguj się do systemów informatycznych w przypadkowych miejscach z niezaufanych urządzeń lub publicznych niezabezpieczonych sieci Wi-Fi,

- wykonuj regularnie kopie zapasowe,

- po zakończeniu pracy wylogowujemy się i wyłączamy komputer.

E- MAIL I BEZPIECZNE KORZYSTANIE Z POCZTY ELEKTRONICZNEJ

- postępuj zgodnie z obowiązującymi zasadami w organizacji dotyczącymi korzystania ze służbowej poczty elektronicznej,

- używaj tylko służbowego konta e-mail,

- nie używaj danych osobowych lub poufnych informacji w temacie wiadomości,

- przed wysłaniem maila upewnij się, że niezbędne jest wysłanie danych osobowych, a jeśli to czynisz, spakuj plik np. 7-zip na hasło, i poinformuj odbiorcę o nim innym kanałem np: telefonicznie,

- przed wysłaniem maila upewnij się, że wysyłasz go do właściwego adresata, zwłaszcza jeśli wiadomość zawiera dane osobowe lub dane wrażliwe,

- dokładnie sprawdź nadawcę maila, czy w nazwie adresu e-mail adresata nie ma np. przestawionych lub pominiętych znaków tak, aby nie wysłać takiej wiadomości do osób nieupoważnionych,

- podczas wysyłania korespondencji zbiorczej trzeba korzystać z opcji „UDW", dzięki której odbiorcy wiadomości nie będą widzieć wzajemnie swoich adresów email.

    - Pamiętaj, jeśli wysyłasz maile do wielu osób korzystaj z UDW (Ukryte Do Wiadomości).

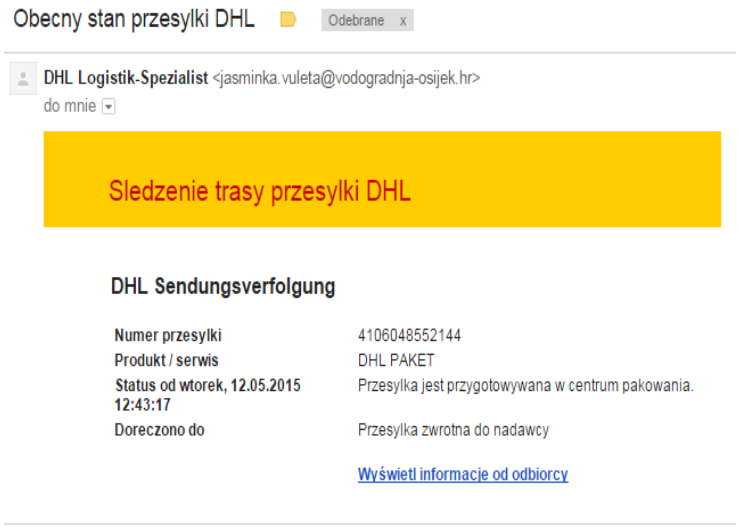
    - Pamiętaj, że adres mailowy w układzie: nazwisko.imię@nazwafirmy.xxx to dane osobowe.

    - Wpisanie adresu w polu UDW powoduje, że odbiorcy nie zobaczą innych adresatów.

Do korespondencji seryjnej używaj opcji

UKRYTE DO WIADOMOŚCI (UDW)!!!

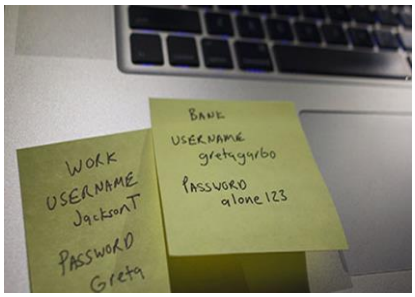
- nie otwieraj wiadomości od nieznanych adresatów, a zwłaszcza nie otwieraj załączników oraz nie klikaj w link zawarty w takiej wiadomości. To może być atak phishingowy.



Skąd wiemy, że nie są to do wiadomości od nadawców, za których się podają ? We wszystkich wiadomościach warto sprawdzić adres e-mail, z którego otrzymaliśmy wiadomość

POLITYKA HASEŁ

- postępuj zgodnie z przyjęta w organizacji procedurą bezpieczeństwa,
- hasło musi składać się z 8 znaków i spełniać warunek złożoności, co oznacza, że musi składać się z wielkich i małych liter, a także cyfr. Duże litery + małe litery + cyfry,
- kolejne hasła muszą być różne,
- zabrania się tworzenia haseł na podstawie imion, dat urodzenia, sekwencji klawiszy klawiatury,
- użytkownik ponosi pełną odpowiedzialność za utworzone hasła i za ich bezpieczne przechowywanie,
- zmieniaj hasła raz na 30 dni,
- jeżeli system nie wymusza zmiany haseł, sam musisz zmieniać hasło,
- wygaszacz ekranu z hasłem,
- nie zapamiętuj haseł w aplikacjach webowych,
- nie zapisuj haseł na kartkach,



- nie podawaj haseł osobom trzecim,
- nie używaj tych samych haseł w różnych systemach informatycznych,
- zabezpieczaj hasłem serwery, pliki, nośniki danych czy inne zasoby sieciowe,
- zabezpieczaj hasłem sieci bezprzewodowe.

DZIENNIK ELEKTRONICZNY

- przy korzystaniu z dziennika elektronicznego postępuj zgodnie z przyjętą w organizacji procedurą bezpieczeństwa i zasadami przedstawionymi powyżej,

- pamiętaj o tym by pod żadnym pozorem nie podawać hasła dostępowego do dziennika elektronicznego,

- nie loguj się do dziennika elektronicznego w przypadkowych miejscach z niezaufanych urządzeń lub publicznych niezabezpieczonych sieci Wi-Fi,

- pamiętaj, że dzienniki elektroniczne, wykorzystywane powszechnie w szkołach , dają możliwość komunikacji z uczniami,

- za ich pośrednictwem można nie tylko wystawiać oceny, ale również zadawać pracę domową, wyznaczać materiały do przeczytania oraz przesyłać linki do różnych materiałów edukacyjnych dostępnych w Internecie.