Podstawowe zasady bezpieczeństwa i higieny pracy w sieci

podczas zdalnego nauczania w LO im. św. Jadwigi Królowej w Kielcach

# PORADNIK DLA NAUCZYCIELI

## I. Komunikacja w sieci

1. Komunikuj się z uczniami i rodzicami za pomocą poczty elektronicznej w dzienniku LIBRUS a nie prywatnego maila. Jeśli do pracy zdalnej wykorzystujesz komunikację mailową – wysyłaj wiadomości wyłącznie na oficjalne adresy uczniów założone na serwerze szkoły.
2. Do przesyłania treści i dokumentów używaj tylko służbowego adresu mailowego,
   założonego przez administratora na serwerze poczty elektronicznej administrowanym przez szkołę.
3. Przed przesłaniem dokumentów drogą elektroniczną lub ich składowaniem do we wspólnym repozytorium zawsze, jeśli to możliwe, zapisuj je w formacie PDF.
4. Sprawdź, czy twój komputer posiada aktywny system antywirusowy oraz odnowione sygnatury antywirusowe.
5. Nie pozostawiaj dostępnych dla innych zalogowanych systemów komunikacji służbowej, w tym otwartej sesji dziennika elektronicznego.
6. Realizuj połączenia służbowe korzystając jedynie z zaufanych miejsc dostępu do sieci internet.
7. Korzystaj z określonych dla nauczycieli placówki miejsc składowania dokumentów w wybranej przestrzeni dysku wirtualnego. (Dysk Google)

## II. Edukacja w sieci

1. Stosuj polecane przez dyrektora szkoły narzędzia pracy zdalnej (Librus, narzędzia GSuit) lub wybieraj sprawdzone narzędzia, wskazywane przez MEN oraz instytucje oświatowe.

2. Wybierając narzędzia pamiętaj, że ich wymagania nie mogą być wygórowane w stosunku do możliwości technicznych (sprzętowych) twoich uczniów.
3. Zanim zastosujesz wybrane rozwiązanie w edukacji swoich uczniów, dokonaj jego sprawdzenia pod kątem jakości i poprawności komunikacji.
4. Używaj połączeń do serwisów i narzędzi zapewniających ich szyfrowanie
5. Udostępniaj i polecaj uczniom tylko takie zasoby edukacyjne, do których dostęp jest bezpłatny i bezpieczny.
6. Przed połączeniem z platformą edukacyjną danego dnia pracy zdalnej sprawdź parametry jakościowe łącza, aby upewnić się, że zapewniają one odpowiednią jakość i stałość połączenia.

## III. Ochrona danych i prywatność

1. W pracy zdalnej przestrzegaj zasady bezpieczeństwa przetwarzania danych osobowych w sposób zapewniający nienaruszalność prywatności uczniów i rodziców
2. Rozważ, czy podejmowane czynności z użyciem narzędzi teleinformatycznych nie naruszają przyjętego dotychczas poziomu bezpieczeństwa danych nam powierzonych do przetwarzania w procesach edukacyjnych i kontaktach bezpośrednich.
3. Wybierając do zastosowania narzędzie teleinformatyczne przetwarzające dokumenty z danymi osobowymi pamiętaj o obowiązku wynikającym z art. 5 RODO w zakresie spełnienia zasady minimalizacji, ograniczonego przechowywania oraz odpowiedniego poziomu bezpieczeństwa dla zapewnienia integralności i poufności.
4. W komunikatorach internetowych lub narzędziach do pracy grupowej, przy zakładaniu kont dla uczniów, nie dołączaj zdjęcia użytkownika, ponieważ wiąże się to z dodatkowymi wymaganiami do spełnienia po stronie administratora takiego rozwiązania.
5. Na dyskach wirtualnych (chmurach) składuj wyłącznie takie materiały edukacyjne, które nie zawierają danych osobowych.

# PORADNIK DLA RODZICÓW

## I. Komunikacja w sieci

1. Komunikację w sprawach kontaktów z wychowawcą i nauczycielami swojego dziecka realizuj jedynie za pomocą poczty elektronicznej dziennika elektronicznego LIBRUS (*https://synergia.librus.pl/wiadomosci*).
2. Przesyłaj dokumenty z wykorzystaniem poczty elektronicznej tylko na służbowe adresy podane przez dyrektora szkoły, wychowawcę klasy lub nauczyciela twojego dziecka, uznane jako dedykowane do komunikacji i zadań służbowych między szkołą a rodzicem.
3. Zapoznawaj się na bieżąco z komunikatami na oficjalnej stronie internetowej szkoły i stosuj publikowane tam zalecenia w kontaktach z placówką.
4. Jeśli masz wątpliwości co do bezpieczeństwa lub poprawności treści, jaką otrzymujesz z wykorzystaniem maila, skorzystaj z telefonu podanego do komunikacji (?) lub sprawdź ją kontaktując się z innymi rodzicami.

## II. Edukacja w sieci

1. Głównym narzędziem wymiany informacji między uczniem a nauczycielem jest dziennik elektroniczny LIBRUS.
2. Na czas pracy zdalnej w środowisku edukacyjnym obowiązującym w LO im. św. Jadwigi
3. Królowej w Kielcach (logowanie do platform edukacyjnych, kontakty z nauczycielami itp.) uczeń posługuje się wyłącznie adresem mailowym nadanym przez szkołę, wpisanym do dziennika LIBRUS.

## III. Ochrona danych i prywatność

1. Dbaj o zachowanie w tajemnicy twojego loginu i hasła umożliwiającego dostęp do dziennika elektronicznego.
2. Nie zostawiaj sesji e-dziennika otwartej, jeśli już z niego nie korzystasz.
3. Pamiętaj, że szkoła nie prowadzi przez internet zbiórek pieniędzy, więc niczego nie opłacaj.
4. Nie klikaj w maile pochodzące od nieznanych nadawców, zawierające w swojej treści aktywne linki do stron z oprogramowaniem edukacyjnym dla twojego dziecka lub z informacją o konieczności pobrania takiego oprogramowania.
5. Nie przesyłaj żadnych danych osobowych wypełniając „otwarte” formularze dołączone do maili. Niezbędne dane osobowe twojego dziecka zostały zgromadzone przez szkołę w procesie rekrutacji.

# PORADNIK DLA UCZNIÓW

## I. Komunikacja w sieci

1. Podczas pracy zdalnej w środowisku edukacyjnym obowiązującym w LO im. św. Jadwigi Królowej w Kielcach (logowanie do platform edukacyjnych, kontakty z nauczycielami itp.) posługuj się wyłącznie adresem mailowym nadanym przez szkołę, wpisanym do dziennika LIBRUS.
2. Zaopatrz swój komputer w aktualny system antywirusowy (np. Avast, Panda Dome, Avira, Bitdefender).
3. Do pracy w obszarze edukacyjnym korzystaj z zaufanych połączeń internetowych.
4. Zwracaj uwagę, czy strony z treściami, do których odwiedzania jesteś zapraszany, mają szyfrowane połączenia z weryfikacją tożsamości dostawcy – protokół https (kłódeczka w narożniku przeglądarki).
5. Nie wyłączaj zabezpieczeń domyślnych swojego komputera.
6. Korzystaj z oprogramowania realizującego funkcję sandbox, czyli tzw. piaskownicy – zapewniając sobie bezpieczne próbowanie nowych programów, których źródła pochodzenia nie znasz, a najlepiej takich nie instaluj.
7. Nie opłacaj żadnych dostępów do zasobów edukacyjnych – taka prośba przekazana mailem lub komunikatem na stronie powinna wzbudzić u Ciebie podejrzenie i konieczność zakończenia połączenia.
8. Nie udostępniaj innym osobom swojego hasła do dedykowanych identyfikatorów na platformie edukacyjnej lub do połączeń z zasobami szkoły.
9. Udostępniając zasoby własnego komputera dla potrzeb innych, zwracaj szczególna uwagę na to, co faktycznie udostępniasz oraz jakie uprawnienia nadajesz ewentualnym ich użytkownikom.

## II. Edukacja w sieci

1. Korzystaj z bezpośrednio podawanych adresów pobrania oprogramowania udostępnianych na dedykowanych platformach edukacyjnych zalecanych na stronach MEN lub swojej szkoły.

2. Przed połączeniem z platformą edukacyjną danego dnia pracy zdalnej sprawdź parametry jakościowe łącza, aby upewnić się, że zapewniają one odpowiednią jakość i stałość połączenia.
3. Jeśli proces edukacji zdalnej przewiduje przesyłanie wyników opracowań realizowanych narzędziami zainstalowanymi na Twoim komputerze –staraj się dokonać konwersji do formatu PDF.
4. Zawsze przechowuj dokumenty źródłowe, których wysłanie było obligatoryjne w procesie oceny twojej pracy zdalnej.
5. Nie otwieraj plików podsyłanych mailami w formie zawartych w treści linków odsyłających do zasobów w sieci, pochodzących od niezweryfikowanych nadawców lub odsyłających do stron www wzbudzających podejrzenie.

## III. Ochrona danych i prywatność

1. Dbaj o prywatność w sieci, czytaj klauzule informacyjne RODO zamieszczane przez dostawców usług.
2. Zapoznaj się z opisem działania mechanizmu powszechnie używanych cookies. Pamiętaj, że od ciebie zależy wyrażenie zgody na ich używanie.
3. Zweryfikuj ustawienia prywatności Twojej przeglądarki. Upewnij się, czy nie są nadmiarowe i domyślnie zgadzasz się na fakt pobierania pewnych danych podczas połączeń, np. twojej lokalizacji.
4. Ogranicz do minimum wymianę danych osobowych, kontując się z innymi przy pomocy internetu.
5. Nie przechowuj ważnych dokumentów na dysku komputera służącego do komunikacji z wykorzystaniem internetu. Zgraj je na dysk zewnętrzny i załóż hasło dostępu.