Załącznik 2

1. **„Regulamin Ochrony Danych Przy Edukacji Zdalnej w V Liceum Ogólnokształcącym im. Jana III Sobieskiego w Białymstoku” – załącznik do procedur;**

2. **Dobre praktyki, pomagającymi zachować bezpieczeństwo danych podczas lekcji online (źródło www.uodo.gov.pl)**

Regulamin Ochrony Danych Przy Edukacji Zdalnej w V Liceum Ogólnokształcącym im. Jana III Sobieskiego w Białymstoku

I. Postanowienia ogólne.

1. Dokument niniejszy opracowany został na podstawie następujących aktów prawnych:
   1) rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27.04.2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE), dalej w skrócie: „RODO”;
   2) ustawy z dnia 10.05.2018 r. o ochronie danych osobowych, dalej w skrócie: „uodo”;
   3) ustawy z dnia 02.03.2020 r. o szczególnych rozwiązaniach związanych z zapobieganiem, przeciwdziałaniem i zwalczaniem COVID-19, innych chorób zakaźnych oraz wywołanych nimi sytuacji kryzysowych., dalej w skrócie odpowiednio: „ustawa o szczególnych rozwiązaniach związanych z COVID-19”;
   4) ustawy z dnia 26.06.1974 r. Kodeks pracy; dalej w skrócie odpowiednio: „Kodeks pracy”. Praca zdalna nie stanowi telepracy w rozumieniu Kodeksu pracy.
2. Administratorem danych przetwarzanych w ramach edukacji zdalnej jest V Liceum Ogólnokształcące im. Jana III Sobieskiego w Białymstoku.
3. Zakres przetwarzanych danych osobowych w tej sytuacji to: imię, nazwisko, login użytkownika oraz nazwa Szkoły. Dodatkowe informacje dotyczące zasad

przetwarzania i ochrony danych osobowych ujęte zostały w Polityce bezpieczeństwa danych osobowych.

4. Administratorem danych przetwarzanych w narzędziach, systemach, aplikacjach służących do kształcenia na odległość jest dostawca danego rozwiązania. Należy dokładnie zapoznać się z regulaminami i Politykami prywatności dostawców usług i rozwiązań służących do zdalnego nauczania, z których korzystają uczniowie i nauczyciele.
5. Szkoła zapewnia narzędzia umożliwiające nauczycielom prowadzenie zajęć zdalnych oraz bezpieczną komunikację z uczniami i rodzicami, wdrażając je kompleksowo w całej placówce.
6. Szkoła zobowiązuje się do przekazywania pracownikom zadań do wykonania, udzielania informacji merytorycznych oraz organizowania procesu pracy w sposób umożliwiający Pracownikowi pracę zdalną.

II. Zasady korzystania z platform do prowadzenia zajęć w formie zdalnej.

1. W celu przeprowadzenia zajęć w formie zdalnego nauczania, dopuszcza się korzystanie z platformy Microsoft Teams lub Zoom.
2. W przypadku platformy Microsoft Teams warunkiem korzystania z platformy jest posiadanie statusu ucznia bądź nauczyciela V Liceum Ogólnokształcącego w Białystoku.
3. Każdy użytkownik poszczególnych platform do nauczania zdalnego, zobowiązany jest do pracy na własnym koncie.
4. Szkoła wymaga od reprezentującego ucznia rodzica (opiekuna prawnego) podania danych do utworzenia konta w systemie zdalnego nauczania, ale tylko w zakresie niezbędnym do tego, aby to konto założyć.
5. Szkolny administrator/dostawca usługi przydziela konto, hasło i przekazuje dane konfiguracyjne dla rodzica lub nauczyciela w formie elektronicznej. Rodzic / przedstawiciel prawny ucznia, konfigurują usługę zgodnie z instrukcją na stronie logowania. Podczas pierwszego logowania, użytkownik (Uczeń lub przedstawiciel) zobowiązany jest do zmiany hasła na nowe, spełniające zasady tzw. bezpiecznego hasła.
6. Zabronione jest udostępnianie konta innemu użytkownikowi.
7. Użytkownik komputera, programów i platform do nauczania zdalnego rozpoczyna i kończy pracę logowaniem i wylogowaniem się.
8. Po zakończeniu pracy, użytkownik zobowiązany jest wylogować się z systemu informatycznego oraz zabezpieczyć nośniki elektroniczne, na których znajdują się dane osobowe.
9. Nauczyciele i uczniowie ponoszą odpowiedzialność za treści i zawartość swojego konta Microsoft w usłudze Office 365.
10. Zarówno uczniowie jak i nauczyciele przyjmują do wiadomości, że ich działania na platformach mogą być monitorowane przez procesy administracyjne mające wpływ na bezpieczeństwo, wydajność i ogólną konfigurację poszczególnych systemów.

III. Obowiązki pracownika w zakresie ochrony danych osobowych przy zdalnym nauczaniu

11. Każdy Pracownik dopuszczony do pracy zdalnej jest zobowiązany do jej wykonywania w miejscu zamieszkania lub innym uzgodnionym miejscu z Dyrektorem.
12. W ramach posiadanych możliwości Szkoła zapewni warunki do wykonywania pracy zdalnej poprzez udostępnianie stosownego sprzętu oraz oprogramowania niezbędnego do wykonywania obowiązków służbowych.
13. Pracownik ma obowiązek dbania o powierzony sprzęt, w tym chronienia udostępnionych urządzeń przed zalaniem, zniszczeniem lub kradzieżą.
14. Pracownik jest zobowiązany do wykonywania obowiązków służbowych z zachowaniem szczególnej ostrożności w stosunku do tajemnicy służbowej oraz przetwarzanych informacji, w tym danych osobowych.
15. Pracownik podczas wykonywania pracy zdalnej zobowiązany jest przestrzegać wszystkich zasad związanych z ochroną danych osobowych i bezpieczeństwem informacji. Wykonywanie obowiązków w trybie pracy zdalnej nie zwalnia Pracownika z przestrzegania zasad określonych w obowiązującej u Pracodawcy dokumentacji z zakresu ochrony danych osobowych i bezpieczeństwa informacji, w tym politykach bezpieczeństwa danych osobowych, politykach ochrony danych osobowych, instrukcjach, regulaminach.
16. W przypadku wykrycia lub podejrzenia zaistnienia incydentu związanego z ochroną danych osobowych Pracownik jest zobowiązany zgłosić go niezwłocznie do Pracodawcy w sposób u niego przyjęty.
17. Pracownik jest zobowiązany do zabezpieczenia urządzeń przed dostępem osób trzecich w trakcie pracy jak i po jej zakończeniu.
18. Pracownik jest zobowiązany do wykonywania kopii zapasowych danych wykorzystywanych do świadczenia pracy zdalnej. Częstotliwość, zakres i inne parametry kopii zapasowych powinny być zgodne z procedurami obowiązującymi w Szkole i po uzgodnieniu z pracodawcą.
19. Zabronione jest podłączenie do urządzeń udostępnionych przez Szkołę nośników zewnętrznych z wyjątkiem tych dostarczonych przez Pracodawcę.
20. Jeżeli powierzone zostaną dokumenty papierowe, Pracownik ma obowiązek wydzielenia odrębnego miejsca do ich przechowania, tak aby dokumenty nie uległy uszkodzeniu, zgubieniu bądź zniszczeniu.
21. Pracownik zobowiązany jest do zgłaszania wszelkich niepokojących przypadków mających wpływ na poziom ochrony danych do pracodawcy niezwłocznie w sposób u niego przyjęty.
22. Jeżeli Pracownik nie ma możliwości świadczenia pracy zdalnej z zapewnieniem właściwych zabezpieczeń, w szczególności ze względu na siłę wyższą (np. brak

prądu lub Internetu), niezwłocznie zgłasza to Pracodawcy i postępuje zgodnie z jego instrukcjami.

23. Niedozwolone jest podejmowanie pracy zdalnej w miejscach publicznych, takich jak kawiarnie, restauracje, galerie handlowe, dworce, świetlice szkolne, gdzie osoby postronne mogłyby usłyszeć fragmenty służbowych rozmów lub zapoznać się z fragmentami wykonywanej pracy.
24. Pracując w miejscu zamieszkania lub innym uzgodnionym miejscu, Pracownik powinien zapewnić, aby osoby nieupoważnione, w tym domownicy lub współlokatorzy, nie miały wglądu w wykonywaną pracę, w szczególności poprzez właściwe ustawienie ekranu komputera, a także zapewnienie pracy z dokumentami w sposób uniemożliwiający wgląd.
25. Odchodząc od komputera lub kończąc korzystanie z innego sprzętu elektronicznego należy upewnić się, że urządzenie zostało zablokowane.
26. Odchodząc od stanowiska pracy Pracownik jest zobowiązany schować i zabezpieczyć dokumenty przed dostępem osób trzecich.
27. Zabrania się wyrzucania niezniszczonych dokumentów na śmietnik.
28. Należy zapewnić bezpieczne przewożenie dokumentacji papierowej np. w teczkach, aktówkach, plecakach w celu zabezpieczenia ich przed zagubieniem i kradzieżą.

IV. Środki bezpieczeństwa dla miejsc i narzędzi wykorzystywanych do zdalnego nauczania

1. Przechowując dane na sprzęcie, do którego mogą mieć dostęp inne osoby, należy używać mocnych haseł dostępowych, a przed odejściem od stanowiska pracy urządzenie powinno zostać zablokowane. Zalecane jest także skonfigurowanie automatycznego blokowania komputera po pewnym czasie bezczynności, oraz założenie odrębnych kont użytkowników w przypadku korzystania z komputera przez wiele osób.
2. Gdy dane są przechowywane na urządzeniach przenośnych (np. pamięć USB), muszą być bezwzględnie szyfrowane i chronione hasłem, by zapewnić odpowiednie bezpieczeństwo danych osobowych, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem.
3. Prowadzenie zajęć zdalnych może wymagać korzystania przez nauczyciela z poczty elektronicznej do kontaktu z uczniami lub rodzicami. Nauczyciel powinien prowadzić taką korespondencję ze służbowej skrzynki pocztowej, bądź korzystając z komunikatora dziennika elektronicznego, które to narzędzia zapewnia mu Szkoła.
4. W wyjątkowych, uzasadnionych przypadkach i za zgodą Dyrektora Szkoły, dopuszcza się możliwość wykorzystania do celów służbowych prywatnej skrzynki pocztowej bądź innego prywatnego komunikatora, jednak przy zachowaniu rozwagi i bezpieczeństwa.
5. Szczególną uwagę należy zwrócić na zabezpieczenie danych osobowych udostępnianych w przesyłanych wiadomościach. Zawsze przed wysłaniem

wiadomości, należy upewnić się , czy niezbędne jest wysłanie danych osobowych, oraz że zamierza się wysyłać ją do właściwego adresata. Ponadto trzeba sprawdzić, 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 powinno się korzystać z opcji „UDW", dzięki której odbiorcy wiadomości nie będą widzieć wzajemnie swoich adresów e-mail.

6. Zabronionym jest prowadzenie zajęć zdalnych korzystając z niezabezpieczonych i otwartych sieci WiFi.
7. Urządzenia wykorzystywane do pracy zdalnej muszą spełniać minimalne wymagania dla urządzenia w zakresie bezpieczeństwa:
   1) Na urządzeniu powinno być legalne i aktualne oprogramowanie,
   2) Zostały włączone automatyczne aktualizacje,
   3) Została włączona zapora systemowa,
   4) Został zainstalowany i działa w tle program antywirusowy,
   5) Zalogowanie do systemu wymaga uwierzytelnienia z wykorzystaniem indywidualnego loginu i hasła użytkownika,
   6) Wyłączono autouzupełnianie i zapamiętywanie hasła w przeglądarce internetowej.

V. Zasady na lekcjach online

1. Przed każdymi zajęciami wyłączamy wszystko, co mamy na komputerze lub komórce. To, co dzieje się w tle może rozpraszać i przeszkadzać w uczestnictwie w zajęciach.
2. Logujemy się zawsze swoim imieniem i nazwiskiem, nie podszywamy się pod nikogo innego, nie zmieniamy nicków w czasie lekcji.
3. Link i hasło do lekcji online jest indywidualne dla każdej klasy. Dla bezpieczeństwa wszystkich uczestników lekcji nie podajemy nikomu spoza klasy hasła dostępu do naszych zajęć.
4. Lekcji nie wolno nagrywać, fotografować, robić printscreenów i upubliczniać. Złamanie tej ważnej zasady może wiązać się z konsekwencjami prawnymi.
5. Głos na zajęciach zabieramy po kolei. Jest to ustalone przez osobę, która prowadzi zajęcia lub przez ucznia - poprzez zgłoszenia się do odpowiedzi.
6. Zajęcia online wymagają od nas wszystkich skupienia. Szanujmy swój czas i koncentrujmy się na tym, co dzieje się na zajęciach. Jeśli zajęcia będą zakłócane, nauczyciel może wyciszać klasę i dać dostęp do mikrofonu tylko wskazanym uczniom.

VI. Postanowienia końcowe

1. Regulamin o aktualnej treści obowiązuje do czasu jego zmiany. W szczególności regulamin obowiązuje w okresie zagrożenia rozprzestrzeniania się SARS-CoV-2 z

uwzględnieniem stosowania przepisów ustawy o szczególnych rozwiązaniach związanych z COVID-19.

2. W sprawach nieuregulowanych niniejszym regulaminem, stosuje się przepisy prawa powszechnie obowiązującego, w tym z zakresu prawa pracy i ochrony danych osobowych, a także wewnętrzne polityki, instrukcje, procedury oraz regulaminy obowiązujące u Pracodawcy z uwzględnieniem dokumentacji z zakresu ochrony danych osobowych i bezpieczeństwa informacji.

Dobre praktyki

DOBRE PRAKTYKI POMAGAJĄCE ZACHOWAĆ BEZPIECZEŃSTWO DANYCH PODCZAS LEKCJI ONLINE

20 zasad bezpieczeństwa, o których powinni pamiętać zarówno szkolni administratorzy, jak i nauczyciele oraz uczniowie, przygotowując się do lekcji online, aby chronić swoje dane

1. Na bieżąco aktualizuj systemy operacyjne.
2. Systematycznie aktualizuj programy antywirusowe, antymalware i antyspyware.
3. Regularnie skanuj stacje robocze programami antywirusowymi, antymalware i antyspyware.
4. Pobieraj oprogramowanie wyłącznie ze stron producentów.
5. Nie otwieraj załączników z nieznanych źródeł dostarczanych poprzez korespondencję elektroniczną.
6. Nie zapamiętuj haseł w aplikacjach webowych.
7. Nie zapisuj haseł na kartkach.
8. Nie używaj tych samych haseł w różnych systemach informatycznych.
9. Zabezpieczaj serwery plików czy inne zasoby sieciowe.
10. Zabezpieczaj sieci bezprzewodowe – Access Point.
11. Dostosuj złożoność haseł odpowiednio do zagrożeń.
12. Unikaj wchodzenia na nieznane czy przypadkowe strony internetowe.
13. Nie loguj się do systemów informatycznych w przypadkowych miejscach z niezaufanych urządzeń lub publicznych niezabezpieczonych sieci Wi-Fi.
14. Wykonuj regularne kopie zapasowe.
15. Korzystaj ze sprawdzonego oprogramowania do szyfrowania e-maili lub nośników danych.
16. Szyfruj dane przesyłane pocztą elektroniczną.
17. Szyfruj dyski twarde w komputerach przenośnych.
18. Przy pracy zdalnej korzystaj z szyfrowanego połączenia VPN.
19. Odchodząc od komputera, blokuj stację komputerową.
20. Nie umieszczaj w komputerze przypadkowo znalezionych nośników USB. Może znajdować się na nich złośliwe oprogramowanie.

źródło: www.uodo.gov.pl

MINISTER EDUKACJI NARODOWEJ

UODO