Załącznik Nr 4 do Zarządzenia Nr 1/2020/2021

Dyrektora Szkoły Podstawowej im. Janusza Korczaka w Brodach

z dnia 31.08.2020 r.

Procedury ochrony danych osobowych

w związku z wykonywaniem pracy zdalnej

(w przypadku realizacją zadań z wykorzystaniem metod i technik kształcenia na odległość lub innego sposobu kształcenia lub wykonywania pracy zdalnej)

Zasady bezpieczeństwa, 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.

DOTYCZY PRACOWNIKÓW

Korzystając z poczty elektronicznej i innych elementów pracy grupowej, takie jak narzędzia konferencyjne lub komunikatory internetowe itd. wykorzystujących w czasie pracy zdalnej należy przestrzegać zasad bezpiecznego przetwarzania danych:

1) Pracownik może przetwarzać dane osobowe tylko w celach związanych z wykonywaniem swoich obowiązków służbowych.

2) Pracownik musi pamiętać o bezpiecznym korzystaniu z komputerów i innych urządzeń zarówno wtedy, gdy zapewnił mu je pracodawca, jak i wtedy, gdy korzysta z własnych.

3) Urządzenia z których korzysta pracownik muszą być odpowiednio zabezpieczone, a pracownik powinien postępować zgodnie z polityką i procedurami wprowadzonymi w tym zakresie w szkole.

4) Jeżeli pracownik używa własnego urządzenia musi samodzielnie spełnić podstawowe wymogi bezpieczeństwa: przede wszystkim należy sprawdzić, czy wykorzystywane urządzenie ma aktualny system operacyjny, czy używane są na nim programy, w szczególności programy antywirusowe, czy dokonane są niezbędne aktualizacje. Na bieżąco aktualizowane powinny być także zainstalowane programy antymalware i antyspyware. Należy rozważnie instalować na swoich urządzeniach oprogramowanie i pobierać je tylko z wiarygodnych źródeł (ze stron producentów).

5) 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. Należy skonfigurować automatyczne blokowanie komputera

po pewnym czasie bezczynności oraz założenie odrębnych kont użytkowników w przypadku korzystania z komputera przez wiele osób.

6) Podczas korzystania z programów lub aplikacji mobilnych należy korzystać z możliwych do zastosowania w nich mechanizmów ochrony prywatności użytkowników. W przypadku programu wymagającego logowania, warto zadbać o silne hasło dostępu, a dodatkowo chronić je przed utratą czy dostępem osób nieuprawnionych.

7) 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.

8) W podstawowym zakresie komunikację prowadzi się poprzez wdrożone w szkole rozwiązania teleinformatyczne.

9) Szczególną uwagę pracownik musi 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 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*.

DOTYCZY NAUCZYCIELI

Korzystając z poczty elektronicznej i innych elementów pracy grupowej, takie jak narzędzia konferencyjne lub komunikatory internetowe itd. wykorzystujących zdalne metody nauczania należy przestrzegać zasad bezpiecznego przetwarzania danych:

1) Nauczyciel może przetwarzać dane osobowe uczniów i ich rodziców tylko w celach związanych z wykonywaniem swoich obowiązków służbowych.

2) Nauczyciel musi pamiętać o bezpiecznym korzystaniu z komputerów i innych urządzeń zarówno wtedy, gdy zapewnił mu je pracodawca, jak i wtedy, gdy korzysta z własnych.

3) RODO nie zabrania wykorzystywania przez nauczyciela prywatnego komputera, tabletu, czy telefonu do przetwarzania danych osobowych w związku ze zdalnym prowadzeniem zajęć. Urządzenia te muszą być jednak odpowiednio zabezpieczone, a nauczyciel powinien postępować zgodnie z polityką i procedurami wprowadzonymi w tym zakresie w szkole.

4) Jeżeli nauczyciel używa własnego urządzenia musi samodzielnie spełnić podstawowe wymogi bezpieczeństwa: przede wszystkim należy sprawdzić, czy wykorzystywane urządzenie ma aktualny system operacyjny, czy używane są na nim programy, w szczególności programy antywirusowe, czy dokonane są niezbędne aktualizacje. Na bieżąco aktualizowane powinny być także zainstalowane programy antymalware i antyspyware. Należy rozważnie instalować na swoich urządzeniach oprogramowanie i pobierać je tylko z wiarygodnych źródeł (ze stron producentów).

5) 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. Należy skonfigurować automatyczne blokowanie komputera po pewnym czasie bezczynności oraz założenie odrębnych kont użytkowników w przypadku korzystania z komputera przez wiele osób.

6) Podczas korzystania z programów lub aplikacji mobilnych należy korzystać z możliwych do zastosowania w nich mechanizmów ochrony prywatności użytkowników. W przypadku programu wymagającego logowania, warto zadbać o silne hasło dostępu, a dodatkowo chronić je przed utratą czy dostępem osób nieuprawnionych.

7) 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.

8) W podstawowym zakresie komunikację z uczniami i rodzicami prowadzi się poprzez wdrożone w szkole rozwiązania teleinformatyczne, np. dzienniki elektroniczne. W takiej sytuacji nauczyciel musi nadal zachowywać podstawowe zasady bezpieczeństwa przy zdalnym łączeniu się z dziennikiem elektronicznym ze swojego urządzenia w domu.

9) 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. Jeżeli szkoła nie zapewniła nauczycielom

służbowych skrzynek poczty elektronicznej, to jeżeli wykorzystują oni do celów służbowych prywatną skrzynkę pocztową muszą pamiętać, aby korzystać z niej w sposób rozważny i bezpieczny. Ewentualne wnioski o założenie poczty służbowej nauczyciel powinien niezwłocznie powiadomić o tym Dyrektora.

10) Szczególną uwagę nauczyciel musi 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 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*.

11) Nauczyciel powinien wykorzystywać w zdalnym prowadzeniu zajęć te platformy edukacyjne lub narzędzia do e-learningu, które zostały wdrożone w szkole. W takiej sytuacji może oczekiwać, że prowadzenie zajęć zdalnych będzie bezpieczne. Powinien wtedy przestrzegać przyjętych przez szkołę instrukcji i procedur dotyczących ochrony danych osobowych oraz musi zachować podstawowe zasady bezpieczeństwa przy zdalnym łączeniu się z taką platformą ze swojego urządzenia w domu.

12) Nauczyciele nie powinni decydować o korzystaniu z konkretnych rozwiązań (np. prowadzenie lekcji za pomocą komunikatorów czy wideonarzędzi). Biorąc jednak pod uwagę nadzwyczajną sytuację i konieczność natychmiastowego rozpoczęcia zajęć zdalnych, może to być w niektórych sytuacjach uzasadnione. Należy jednak pamiętać, że za przetwarzanie danych uczniów przy wykorzystaniu narzędzi wdrożonych samodzielnie przez nauczyciela zawsze odpowiedzialność ponosi szkoła. Przyjmowanie określonego rozwiązania powinno się odbywać w uzgodnieniu z dyrektorem szkoły, lub wyznaczonym przez niego koordynatorem pracy zdalnej w szkole. Takie rozwiązanie powinno być traktowane jako tymczasowe.

13) Zawsze przy wyborze aplikacji lub innych narzędzi wykorzystywanych do zdalnej edukacji bądź komunikacji z uczniami należy się zastanowić, czy jest niezbędne, aby przetwarzały one dane osobowe, a jeżeli tak, czy można zminimalizować ich zakres, bądź wykorzystywać tylko pseudonimy (np. pierwsza litera imienia itp.). Należy także sprawdzić zasady świadczenia usługi i zasady przetwarzania danych przez usługodawcę (politykę prywatności).

14) Nauczyciel w porozumieniu z dyrektorem szkoły powinien uwzględnić, jakie realne możliwości komunikowania się z nim mają uczniowie lub rodzice, pod warunkiem, że wskazany przez nich konkretny rodzaj komunikatora internetowego zapewnia bezpieczeństwo komunikacji.

15) Na ogólnie dostępnych portalach lub stronach internetowych nauczyciel może jedynie publikować materiały edukacyjne, natomiast nie może przetwarzać danych osobowych uczniów lub rodziców.

16) W celu sprawdzania i monitorowania obecności uczniów w zajęciach prowadzonych zdalnie nauczyciel powinien zachować proporcjonalność i minimalizację danych. Dla przykładu nie może w tym celu korzystać z narzędzi zbierających dane biometryczne, w tym wykorzystujących systemy wykrywania twarzy.

W celu bezpiecznego przetwarzania informacji, w tym danych osobowych na komputerach prywatnych wskazuje się następujące zasady dotyczących bezpieczeństwa danych osobowych podczas pracy poza zakładem pracy:

1) URZĄDZENIA

1. Pracodawca może przekazać urządzenia i oprogramowanie do pracy zdalnej lub pracownik może korzystać ze swojego urządzenia prywatnego do wykonywania obowiązków służbowych.
2. Należy postępować zgodnie z przyjętą w zakładzie pracy procedurą ochrony danych osobowych.
3. Nie instaluj dodatkowych aplikacji i oprogramowania niezgodnych z procedurą ochrony danych osobowych.
4. Upewnij się, że wszystkie urządzenia z jakich korzystasz mają niezbędne aktualizacje systemu operacyjnego (IOS lub Android), oprogramowania oraz systemu antywirusowego.
5. Zanim przystąpisz do pracy, wydziel sobie odpowiednią przestrzeń, tak aby ewentualne osoby postronne, nie miały dostępu do dokumentów, nad którymi pracujesz.
6. Odchodząc od stanowiska pracy każdorazowo blokuj urządzenie, na którym pracujesz.
7. Zabezpieczaj swój komputer poprzez używanie silnych haseł dostępu, wielopoziomowe uwierzytelnianie. Pozwoli to na ograniczenia dostępu do urządzenia, a jednocześnie na ograniczenia ryzyka utraty danych w przypadku kradzieży lub zgubienia urządzenia.

8. Podejmij szczególne środki, aby urządzenia z których korzystasz podczas pracy, szczególnie te wykorzystywane do przenoszenia danych, jak dyski zewnętrzne nie zostały zgubione.

9. Jeśli zgubiłeś urządzenie, na którym pracujesz lub zostało skradzione natychmiast podejmij odpowiednie kroki, aby o ile to możliwie, zdalnie wyczyścić jego pamięć.

2) EMAIL

1. Postępuj zgodnie z obowiązującymi zasadami dotyczącymi korzystania ze służbowej poczty elektronicznej (e-mail),
2. Używaj przede wszystkim służbowych kont email. Jeśli pracujesz przetwarzając dane osobowe i musisz używać prywatnego e-maila, upewnij się, że treść i załączniki są właściwie szyfrowane.
3. Unikaj używania danych osobowych lub poufnych informacji w temacie wiadomości.
4. Przed wysłaniem maila upewnij się, że wysyłasz go do właściwego adresata, zwłaszcza jeśli wiadomość zawiera dane osobowe lub dane wrażliwe.
5. Dokładnie sprawdź nadawcę maila.
6. Wysyłając e-maila kilku adresatom stosuj ukrywanie adresatów (poprzez UDW).
7. 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.

8. Nie przesyłaj mailem informacji zaszyfrowanej razem z hasłem. Nawet w osobnej wiadomości. Ten kto ma dostęp do Twojej poczty bez problemu odszyfruje wiadomość.

3) DOSTĘP DO SIECI I CHMURY

1. Używaj tylko z zaufanego dostępu do sieci lub chmury oraz przestrzegaj wszelkich zasad i procedur organizacyjnych dotyczących logowania i udostępniania danych.
2. Jeśli natomiast nie pracujesz w chmurze lub nie masz dostępu do sieci, zadbaj, aby przechowywane dane były w bezpieczny sposób zarchiwizowane.

W celu bezpiecznego przetwarzania informacji, w tym danych osobowych na komputerach prywatnych wskazuje się następujące zasady postępowania:

1. Komputer prywatny z dostępem do Internetu musi być zabezpieczony za pomocą aktualnego oprogramowania antywirusowego.

2. Elektroniczne nośniki informacji takie jak płyty CD, dyski przenośne należy każdorazowo sprawdzać programem antywirusowym przed użyciem, po zainstalowaniu ich w systemie.

3. Komputer powinien posiadać wydzielone konto użytkownika wraz z ustawionym hasłem, znanym tylko uprawnionemu pracownikowi do pracy zdalnej w celu odizolowania danych osobowych od danych prywatnych w przypadku ich przetwarzania. Konto to nie powinno być udostępniane członkom rodziny.

4. Dostęp zdalny do systemów wewnętrznych pracodawcy w tym dziennika elektronicznego powinna być realizowana tylko podczas wykonywania służbowych czynności, po wykonaniu których Pracownik powinien zadbać o rozłączenie się z dostępu zdalnego.

5. Przy przesyłaniu jakichkolwiek danych służbowych pocztą elektroniczną powinna być użytkowana służbowa skrzynka poczty elektronicznej dostępna przez Internet (stronę www) lub dziennik elektroniczny. Jeśli do przenoszenia danych elektronicznych użytkowane będą zewnętrzne nośniki danych (pendrive, dysk zewnętrzny itp.) nośnik musi być zabezpieczony programem kryptograficznym (np. Bitlocker).

6. Pracownikom korzystającym z systemu informatycznego, w którym przetwarzane są dane osobowe zabrania się:

1) ujawniania loginu i hasła współpracownikom i osobom z zewnątrz,

2) pozostawiania haseł w miejscach widocznych dla innych osób,

3) udostępniania stanowisk pracy wraz z danymi osobowymi osobom nieuprawnionym,

4) przy korzystaniu z poczty elektronicznej należy zwrócić szczególną uwagę na otrzymywane załączniki dołączane do treści wiadomości. Zabrania się otwierania załączników i wiadomości poczty elektronicznej od „niezaufanych” nadawców,

5) zabrania się użytkownikom komputerów, wyłączania, blokowania odinstalowywania programów zabezpieczających komputer (skaner antywirusowy, firewall) przed oprogramowaniem złośliwym oraz nieautoryzowanym dostępem.

Dodatkowo wskazuje się na zasady dotyczące wynoszenia służbowej dokumentacji w formie tradycyjnej:

1. Pracownik wynosząc dokumentacje za zgodą dyrektora musi sporządzić listę wynoszonych w danym dniu dokumentów odnosząc się do sygnatury sprawy lub innego numeru/opisu identyfikacyjnego dokumentacje.

2. Dokumenty muszą być przenoszone w zamykanej torbie, w celu ich ochrony przed warunkami atmosferycznymi (np. zamoknięciem, rozwianiem itp.).

3. Za bezpieczeństwo (poufność, integralność, dostępność) wyniesionej dokumentacji odpowiada Pracownik;

4. Zabrania się wyciągania dokumentacji z torby w środkach komunikacji publicznej i w samochodach;

5. Korzystając z samochodu do przewożenia dokumentacji, torba z dokumentami powinna zostać schowana w bagażniku samochodu.