Załącznik nr 1 do Zarządzenia nr 6 /2018

Regulamin Ochrony Danych Osobowych
w Zespole Szkolno-Przedszkolnego im, Jana Pawła II w Miłakowie

Spis treści:

Rozdział 1
Postanowienia ogólne

1. Regulamin stanowi wykaz podstawowych obowiązków z zakresu przestrzegania zasad ochrony danych osobowych w Zespole Szkolno-Przedszkolnym im Jana Pawła II w Miłakowie zgodnie z RODO.

2. Regulamin obowiązuje wszystkich pracowników szkoły, podmioty przetwarzające dane osobowe na podstawie zawartych umów między przetwarzającym a powierzającym, użytkowników systemów informatycznych z dostępem do danych osobowych upoważnionych przez administratora na piśmie.

3. Każdy z wymienionych podmiotów jest zobowiązany do zapoznania się z dokumentem i bezwzględnego przestrzegania zawartych w nim zasad.

4. Administratorem danych osobowych w Zespole Szkolno-Przedszkolnym jest dyrektor Zespołu.

Rozdział 2
Zasady bezpiecznego użytkowania sprzętu IT, dysków, programów.

1. W przypadku, gdy użytkownik przetwarzający dane osobowe korzysta ze sprzętu IT zobowiązany jest do jego zabezpieczenia przed zniszczeniem lub uszkodzeniem. Za sprzęt IT rozumie się: komputery stacjonarne, monitory, drukarki, skanery, ksera, laptopy, służbowe tablety, smartfony.

2. Użytkownik jest zobowiązany zgłosić zagubienie, utratę lub zniszczenie powierzonego mu Sprzętu IT.

3. Samowolne instalowanie, otwieranie (demontaż) Sprzętu IT, instalowanie dodatkowych urządzeń (np. twardych dysków, pamięci) do lub podłączanie jakichkolwiek niezatwierdzonych urządzeń do systemu informatycznego jest zabronione.

4. Użytkownik jest zobowiązany do uniemożliwienia osobom niepowołanym wglądu do danych wyświetlanych na monitorach komputerowych – tzw. Polityka czystego ekranu.

5. Przed czasowym opuszczeniem stanowiska pracy, użytkownik zobowiązany jest wywołać blokowany hasłem wygaszacz ekranu (WINDOWS +L) lub wylogować się z systemu bądź z programu.

6. Po zakończeniu pracy, użytkownik zobowiązany jest:
    1) wylogować się z systemu informatycznego, a jeśli to wymagane – następnie wyłączyć sprzęt komputerowy;

2) zabezpieczyć stanowisko pracy, w szczególności wszelkie nośniki magnetyczne i optyczne na których znajdują się dane osobowe.

7. Użytkownik jest zobowiązany do usuwania plików z nośników/dysków do których mają dostęp inni użytkownicy nieupoważnieni do dostępu do takich plików (np. podczas współużytkowania komputerów).

8. Jeśli użytkownik jest uprawniony do niszczenia nośników, powinien TRWALE niszczyć sam nośnik lub trwale usunąć z niego dane (np. zniszczenie płyt DVD w niszczarce, zniszczenie twardego dysku, pendrive młotkiem).

9. Użytkownicy komputerów przenośnych, na których znajdują się dane osobowe lub z dostępem do danych osobowych przez Internet zobowiązani są do stosowania zasad bezpieczeństwa zawartych w Regulaminie użytkowania komputerów przenośnych.

Rozdział 3
Zarządzanie uprawnieniami-procedura rozpoczęcia, zawieszenia i zakończenia pracy.

1. Każdy użytkownik (np. komputera stacjonarnego, laptopa, programów w których użytkownik pracuje, poczty elektronicznej) musi posiadać swój własny indywidualny identyfikator (login) do logowania się.

2. Tworzenie kont użytkowników wraz z uprawnieniami (np. komputera stacjonarnego, laptopa, programów w których użytkownik pracuje, poczty elektronicznej) odbywa się na polecenie Administratora, a wykonywane przez informatyków.

3. Użytkownik nie może samodzielnie zmieniać swoich uprawnień (np. zostać administratorem Windows na swoim komputerze).

4. Zabronione jest umożliwienie innym osobom pracy na koncie innego użytkownika.

5. Zabrania się pracy wielu użytkowników na wspólnym koncie.

6. Użytkownik (np. komputera stacjonarnego, laptopa, programów w których użytkownik pracuje, poczty elektronicznej) rozpoczyna pracę z użyciem identyfikatora i hasła.

7. Użytkownik jest zobowiązany do powiadomienia Administratora o próbach logowania się do systemu osoby nieupoważnionej, jeśli system to sygnalizuje.

8. W przypadku, gdy użytkownik podczas próby zalogowania się zablokuje system, zobowiązany jest powiadomić o tym Administratora.

9. Użytkownik jest zobowiązany do uniemożliwienia osobom niepowołanym wglądu do danych wyświetlanych na monitorach – tzw. Polityka czystego ekranu.

10. Przed czasowym opuszczeniem stanowiska pracy, użytkownik zobowiązany jest wywołać blokowany hasłem wygaszacz ekranu lub wylogować się z sytemu. Jeżeli tego nie uczyni, po upływie 10 minut system automatycznie aktywuje wygaszacz.

11. Po zakończeniu pracy, użytkownik zobowiązany jest:

1) wylogować się z systemu informatycznego, a następnie wyłączyć sprzęt komputerowy;
2) zabezpieczyć stanowisko pracy, w szczególności wszelką dokumentację oraz nośniki magnetyczne i optyczne, na których znajdują się dane osobowe.

Rozdział 4
Polityka haseł

1. Hasła powinny składać się z co najmniej 8 znaków.

2. Hasła powinny zawierać duże litery + małe litery + cyfry (lub znaki specjalne).

3. Hasła nie mogą być łatwe do odgadnięcia. Nie powinny być powszechnie używanymi słowami. W szczególności nie należy jako haseł wykorzystywać: dat, imion i nazwisk osób bliskich, imion zwierząt, popularnych dat, popularnych słów, typowych zestawów: 123456, qwerty.

4. Hasła nie powinny być ujawniane innym osobom. Nie należy zapisywać haseł na kartkach i w notesach, nie należy naklejać na monitorze komputera, nie trzymać pod klawiaturą lub w szufladzie.

5. W przypadku ujawnienia hasła – należy natychmiast go zmienić.

6. Hasła powinny być zmienianie co 60 dni.

7. Użytkownik systemu w trakcie pracy w aplikacji może zmienić swoje hasło.

8. Użytkownik zobowiązuje się do zachowania hasła w poufałości, nawet po utracie przez nie ważności.

9. Zabrania się używania w serwisach internetowych takich samych lub podobnych haseł jak w systemie komputerowym firmy.

10. Zabrania się stosowania tego samego hasła jako zabezpieczenia w dostępie do różnych systemów.

11. Zabrania się definiowania haseł, w których jeden człon pozostaje niezmienny, a drugi zmienia się według przewidywalnego wzorca (np. Anna001, Anna002, Anna003 itd.). Nie powinno się też stosować haseł, w których któryś z członów stanowi imię, nazwę lub numer miesiąca lub inny możliwy do odgadnięcia klucz.

Rozdział 5
Zasady korzystania z internetu

1. Użytkownik zobowiązany jest do korzystania z internetu wyłącznie w celach służbowych.

2. Zabrania się zgrywania na dysk twardy komputera oraz uruchamia jakichkolwiek programów nielegalnych oraz plików pobranych z niewiadomego źródła. Pliki takie powinny być ściągane tylko za każdorazową zgodą osoby upoważnionej do administrowania infrastrukturą IT i tylko w uzasadnionych przypadkach.

3. Użytkownik ponosi odpowiedzialność za szkody w infrastrukturze IT spowodowane przez oprogramowanie instalowane z Internetu.

4. Zabrania się wchodzenia na strony, na których prezentowane są informacje o charakterze przestępczym, hackerskim, pornograficznym, lub innym zakazanym przez prawo ze względu na zainstalowane na nich szkodliwe oprogramowanie infekujące w sposób automatyczny system operacyjny komputera szkodliwym oprogramowaniem.

5. Zabrania się w opcjach przeglądarki internetowej włączać opcji autouzupełniania formularzy i zapamiętywania haseł.

6. W przypadku korzystania z szyfrowanego połączenia przez przeglądarkę, należy zwracać uwagę na pojawienie się odpowiedniej ikonki (kłódka) oraz adresu www rozpoczynającego się frazą „https:" Dla pewności należy „kliknąć" na ikonę kłódki i sprawdzić, czy właścicielem certyfikatu jest wiarygodny właściciel.

7. Należy zachować szczególną ostrożność w przypadku podejrzanego żądania lub prośby zalogowania się na stronę (np. na stronę banku, portalu społecznościowego, e-sklepu, poczty mailowej) lub podania naszych loginów i haseł, PIN-ów, numerów kart płatniczych przez Internet.

Rozdział 6
Zasady korzystania z poczty elektronicznej

1. Osoby upoważnione do przetwarzania danych osobowych zobowiązane są do korzystania z poczty elektronicznej tylko w celach służbowych.

2. Przesyłanie danych osobowych z użyciem maila może odbywać się tylko przez osoby do tego upoważnione.

3. W przypadku przesyłania danych osobowych poza szkołę należy wysłać pliki zaszyfrowane/spakowane (np. programem 7 zip, winizipem, winrarem) i zahasłowane, gdzie hasło powinno być przesłane do odbiorcy telefonicznie lub SMS-em.

4. W przypadku zabezpieczenia plików hasłem, obowiązuje minimum 8 znaków: duże i małe litery i cyfry lub znaki specjalne a hasło należy przesłać odrębnym mailem lub inną metodą, np. telefonicznie lub SMS-em.

5. Każdy użytkownik przed wysłaniem poczty jest zobowiązany sprawdzić poprawność adresu odbiorcy dokumentu.

6. Zaleca się, aby użytkownik podczas przesyłania danych osobowych mailem zawarł w treści prośbę o potwierdzenie otrzymania i zapoznania się z informacją przez adresata.

7. W celu ochrony przed zainfekowaniem komputera użytkownika i komputerów pracujących w sieci (kryptowirusy) zabrania się otwierania załączników (plików) w mailach nawet od prawdopodobnie znanych użytkownikowi nadawców bez weryfikacji nadawcy.

8. Zabrania się, bez weryfikacji wiarygodności nadawcy „klikać" na hiperlinki w mailach. Nieprzestrzeganie tej zasady może doprowadzić do zainfekowania komputera użytkownika i innych pracujących w sieci.

9. Wszystkie przypadki e-maili budzących podejrzenie należy zgłaszać Administratorowi.

10. Przy wysyłania maili do wielu adresatów jednocześnie, należy użyć metody „Ukryte do wiadomości – UDW". Zabronione jest rozsyłanie maili do wielu adresatów z użyciem opcji „Do wiadomości".

11. Zabrania się rozsyłania maili z tzw. „ łańcuszkami szczęścia". Adres mailowy prywatny służy wyłącznie do korespondencji służbowej.

12. Nakazuje się okresowe czyszczenie poczty z nieaktualnych -e- mali i opróżnianie kosza.

13. Zakazuje się wysyłania korespondencji służbowej na prywatne skrzynki pocztowe pracowników lub innych osób.

14. Użytkownicy mają prawo korzystać z poczty mailowej dla celów prywatnych wyłącznie okazjonalnie i powinno być to ograniczone do niezbędnego minimum.

15. Korzystanie z poczty elektronicznej dla celów prywatnych nie może wpływać na jakość i ilość świadczonej przez Użytkownika pracy oraz na prawidłowe i rzetelne wykonywanie przez niego obowiązków służbowych.

16. Użytkownicy nie mają prawa korzystać z poczty elektronicznej w celu rozpowszechniania treści o charakterze obraźliwym, niemoralnym lub nietycznym i naruszającym cudzą godność i prywatność

17. Zabrania się dokonywanie w sieci zakupów, rezerwacji usług lub świadczeń na rzecz użytkownika oraz dokonywania bankowych z prywatnego konta.

18. Użytkownik bez zgody Administratora nie ma prawa wysyłać wiadomości zawierających dane osobowe dotyczące Pracodawcy / Zleceniodawcy, jego pracowników, klientów, dostawców lub kontrahentów za pośrednictwem Internetu, w tym przy użyciu prywatnej elektronicznej skrzynki pocztowej.

19. Wszelkie przesyłane dokumentów, opracowania, jak i innych treści przesyłane przez użytkownika podlegają zasadom ochrony prawa autorskiego i prawa własności przemysłowej, które użytkownik jest obowiązany przestrzegać.

Rozdział 7
Zasady użytkowania komputerów przenośnych

1. Każdy Użytkownik komputera przenośnego winien zapoznać się z Zasadami użytkowania komputerów przenośnych oraz pisemnie zobowiązać się do jego przestrzegania.

2. W przypadku przechowywania na komputerze przenośnym danych osobowych lub stanowiących tajemnicę Administratora, Użytkownik zobowiązany jest do ich przechowywania na dysku szyfrowanym, zabezpieczonym co najmniej 8- znakowym hasłem (duże, małe litery, znaki specjalne lub cyfry).

3. Na komputerach przenośnych przeznaczonych do zewnętrznych prezentacji multimedialnych nie powinny, o ile jest to możliwe, znajdować się dane osobowe lub stanowiące tajemnicę Administratora.

4. W przypadku kradzieży lub zgubienia komputera przenośnego, Użytkownik powinien natychmiast powiadomić o tym osobę odpowiedzialną za ochronę danych tj. Administratora Danych, zaznaczając jednocześnie, jakiego rodzaju dane były na tym urządzeniu przechowywane.

5. Użytkownik zobowiązany jest do zabezpieczenia komputera przenośnego w czasie transportu, a w szczególności:

1) zaleca się przenoszenie go w specjalnym futerale;

2) zabrania się pozostawiania komputera przenośnego w samochodzie podczas postoju w miejscu publicznym bez nadzoru;

3) podczas jazdy samochodem zaleca się przechowywanie komputera przenośnego pod tylnym siedzeniem kierowcy.

6. W przypadku, gdy komputer przenośny pozostawiony jest w miejscu dostępnym dla osób nieupoważnionych, Użytkownik jest zobowiązany do stosowania kabla zabezpieczającego. W szczególności dotyczy to zabezpieczenia komputera na stanowisku pracy, podczas konferencji, prezentacji, szkoleń, targów itp.

7. W przypadku pozostawiania komputerów przenośnych w szkole zaleca się umieszczanie ich po zakończeniu pracy w zamykanych szafkach.

8. Użytkownik komputera przenośnego jest zobowiązany do regularnego tworzenia kopii bezpieczeństwa danych na serwerze lub na określonych nośnikach (pendrive, CD,

DVD). Nośniki z takimi kopiami powinny być przechowywane w bezpiecznym miejscu, z uwzględnieniem ochrony przed dostępem osób niepowołanych.

9. Pracując na komputerze przenośnym w miejscach publicznych i środkach transportu, Użytkownik zobowiązany jest chronić wyświetlane na monitorze informacje przed wglądem osób nieupoważnionych.

Rozdział 8
Zasady wynoszenia nośników z danymi osobowymi poza szkołę

1. Użytkownicy nie mogą wynosić poza szkołę bez zgody Administratora danych żadnych wymiennych elektronicznych nośników informacji, tj. wymienne twarde dyski, pen-drive, płyty CD, DVD, pamięci typu Flash.

2. W sytuacjach koniecznych, za zgodą Administratora danych, wynoszone nośniki wymienne muszą być zaszyfrowane, a pliki opatrzone hasłem.

3. Zabrania się wynoszenia poza szkołę dokumentacji papierowej, zwierającej dane osobowe (dzienniki, arkusze ocen). W przypadku innej dokumentacji (prace klasowe, listy uczestników wycieczek, dokumentacja wycieczek) należy ją przenosić w zamykanych teczkach lub w innej bezpiecznej formie.

4. W przypadku przesyłania dokumentacji j/w należy korzystać z zaufanych firm kurierskich, za pokwitowaniem i w opakowaniach gwarantujących niedostępność osób trzecich.

Rozdział 9
Zasady zabezpieczania dokumentacji papierowej z danymi osobowymi

1. Upoważnieni pracownicy są zobowiązani do stosowania tzw. „**Polityki czystego biurka**”. Polega ona na zabezpieczaniu (zamykaniu) dokumentów np. w szafach, biurkach, pomieszczeniach przed kradzieżą lub wglądem osób nieupoważnionych po godzinach pracy lub podczas ich nieobecności w trakcie godzin pracy.

2. Upoważnieni pracownicy zobowiązani są do niszczenia dokumentów i wydruków w niszczarkach lub utylizacji ich w specjalnych bezpiecznych pojemnikach z przeznaczeniem do bezpiecznej utylizacji.

3. Zabrania się pozostawiania dokumentów z danymi osobowymi poza zabezpieczonymi pomieszczeniami, np. w korytarzach, na kserokopiarkach, drukarkach, w pomieszczeniach ogólnodostępnych.

4. Zabrania się wyrzucania niezniszczonych dokumentów na śmietnik lub porzucania ich na zewnątrz, np., na terenach publicznych miejskich lub w lesie.

Rozdział 10
Zasady niszczenia danych na nośnikach elektronicznych

1. W odniesieniu do nośników przenośnych (pen-drive'y) oraz nośników danych zainstalowanych w komponentach informatycznych – złomowanych stosowane są mechanizmy bezpiecznego kasowania informacji:
   1) za pomocą specjalistycznego oprogramowania;
   2) przy użyciu demagnetyzacji;
   3) poprzez fizyczne niszczenie (pocięcie, spalenie) nośników.
2. Wyznaczony administrator dokonuje kontroli prawidłowości usunięcia informacji.
3. Nośniki usuwalne, które nie mogą być ponownie wykorzystane, są niszczone.
4. Za właściwe skasowanie informacji zawartej na nośniku przenośnym lub w pamięci masowej stacji roboczej odpowiada użytkownik.
5. Za kasowanie informacji z pamięci masowych serwerów oraz nośników kopii archiwalnych i zapasowych odpowiada administrator danych.
6. Niszczenie nośnika zostaje odnotowane w protokole zniszczenia.

Rozdział 11
Zasady niszczenia danych na nośnikach papierowych

1. Dokumentacja papierowa niszczona jest w niszczarkach paskowych oraz w niszczarkach o podwyższonym standardzie/ Dokumentacja papierowa niszczona jest za pośrednictwem firmy niszczącej dokumenty. Firma zobowiązana jest do wykazania się bezpieczną procedurą utylizacji.

Rozdział 12
Procedura napraw w serwisach zewnętrznych

1. Komputery przeznaczone do naprawy należy wysyłać bez dysków, a urządzenia mobilne bez kart pamięci.
2. W przypadku naprawy sprzętu z danymi osobowymi na nośniku należy je wpierw trwale usunąć z użyciem specjalistycznego oprogramowania.
3. W przypadku naprawy sprzętu z danymi osobowymi na nośniku - rekomendowane jest zawarcie specjalnego zapisu w umowie serwisowej, gwarantującego bezpieczną naprawę (należy na to zwrócić uwagę przy zakupach sprzętu).

4. W przypadku naprawy sprzętu z danymi osobowymi na nośniku - rekomendowane jest przekazywanie do naprawy uszkodzonego sprzętu z danymi zaszyfrowanymi na dysku / karcie pamięci. Sprzęt przekazywany jest do serwisu bez podawania hasła.
5. Rekomendowane jest korzystanie z serwisu, który dokonuje napraw u klienta (umowy gwarancyjne on-site).

Rozdział 13
Skrócona instrukcja postępowania w przypadku naruszenia ochrony danych osobowych.

1. Każda osoba upoważniona do przetwarzania danych osobowych zobowiązana jest do powiadomienia Administratora w przypadku stwierdzenia lub podejrzenia naruszenia ochrony danych osobowych.

2. Do sytuacji wymagających powiadomienia, należą:

1) niewłaściwe zabezpieczenie fizyczne pomieszczeń, urządzeń i dokumentów;
2) niewłaściwe zabezpieczenie sprzętu IT, oprogramowania przed wyciekiem, kradzieżą i utratą danych osobowych;
3) nieprzestrzeganie zasad ochrony danych osobowych przez pracowników(np. niestosowanie zasady „czystego biurka”/ekranu, ochrony haseł, niezamykanie pomieszczeń, szaf, biurek).

3. Do incydentów wymagających powiadomienia należą:

1) zdarzenia losowe zewnętrzne(pożar obiektu/pomieszczenia, zalanie wodą, utrata zasilania, utrata łączności;
2) zdarzenia losowe wewnętrzne (awarie serwera, komputerów, twardych dysków, oprogramowania, pomyłki informatyków, użytkowników, utrata/zagubienie danych;)
3) umyślne incydenty (włamanie do systemu informatycznego lub pomieszczeń, kradzież danych/sprzętu, wyciek informacji, ujawnienie danych osobom nieupoważnionym, świadome zniszczenie dokumentów/danych, działanie wirusów i innego szkodliwego oprogramowania).

Rozdział 14
Obowiązek zachowania poufności danych i ochrony danych osobowych.

1. Każda z osób dopuszczona do przetwarzania danych osobowych jest zobowiązana do:
   1) przetwarzania danych osobowych wyłącznie w zakresie i celu przewidzianym w powierzonych przez dyrektora zadaniach;
   2) zachowania w tajemnicy danych osobowych, do których ma dostęp w związku z wykonywaniem zadań powierzonych przez dyrektora;
   3) niewykorzystywania danych osobowych w celach niezgodnych z zakresem i celem zadań powierzonych przez dyrektora;

4) zachowania w tajemnicy sposobów zabezpieczenia danych osobowych;
5) ochrony danych osobowych przed przypadkowym lub niezgodnym z prawem zniszczeniem, utratą, modyfikacją danych osobowych, nieuprawnionym ujawnieniem danych osobowych, nieuprawnionym dostępem do danych osobowych oraz ich przetwarzaniem.

2. Jeśli jest to przewidziane, osoba dopuszczona do przetwarzania danych odbywa szkolenie z zasad ochrony danych osobowych.

3. Osoby zapoznane z treści niniejszego Regulaminu ochrony danych osobowych lub przeszkolone zobowiązane są podpisać Oświadczenie o poufności.

4. Zabrania się przekazywania bezpośrednio lub przez telefon danych osobowych osobom nieupoważnionym lub osobom, których tożsamości nie można zweryfikować lub osobom podszywającym się pod kogoś innego.

5. Zabrania się przekazywania lub ujawniania danych osobom lub instytucjom, które nie mogą wykazać jasną podstawą prawną do dostępu do takich danych.

6. Zabrania się ujawniania na grupach dyskusyjnych, forach internetowych, blogach, itp. Jakichkolwiek szczegółowych dotyczących funkcjonowania Zespołu, w tym informacji na temat sprzętu i oprogramowania, z jakiego korzysta Zespół oraz informacji kontaktowych innych niż ogólnodostępne w materiałach zewnętrznych.

Rozdział 15
Postępowanie dyscyplinarne

1. Przypadki nieuzasadnionego zaniechania obowiązków wynikających z niniejszego dokumentu potraktowane będą jako ciężkie naruszenie obowiązków pracowniczych lub naruszenie zasad współpracy.

2. Postępowanie sprzeczne z powyższymi zasadami może też być uznane przez Pracodawcę za naruszenie przepisów karnych zawartych w ogólnym Rozporządzeniu o ochronie danych UE z dnia 27 kwietnia 2016 r.