ANEKS nr 1

do POLITYKI BEZPIECZEŃSTWA DANYCH OSOBOWYCH

obowiązującej w:

Publicznym Przedszkolu nr 10 w Jastrzębiu-Zdroju

§1

Od dnia 13.12.2021 roku rozdział 11. Szkolenia ust. 2 otrzymuje brzmienie:

"Osoby zatrudnione w obszarze przetwarzania (w szczególności pracownicy administracji, nauczyciele) przed dopuszczeniem do pracy z danymi osobowymi zostają zapoznane z zasadami ochrony danych osobowych zawartych w **załączniku nr 4 do Polityki.** "

§2

Zmianie ulega załącznik nr 1 oraz załącznik nr 4 do Polityki, których treść stanowią załączniki do niniejszego aneksu.

§3

Pozostała treść Polityki pozostaje bez zmian.

Ilość stron	1
Zatwierdził	DYREKTOR Publicznego Przedszkola nr 10 mgr Mikosława Lasecka

Imię i nazwisko pracownika: .....

Upoważnienie do przetwarzania danych osobowych

Na podstawie art.29 RODO (*), w związku z realizacją zadań i obowiązków służbowych wykonywanych na polecenie administratora, tj Dyrektora Publicznego Przedszkola nr 10 w Jastrzębiu-Zdroju zostaje Pani/Pan upoważniona/-y do przetwarzania danych osobowych uczniów/wychowanków oraz ich rodziców/opiekunów prawnych, w tym danych osobowych o których mowa w art. 9 ust.1, RODO (*), w zakresie niezbędnym dla właściwej realizacji powierzonych obowiązków służbowych i zadań na czas wykonywania tych obowiązków służbowych i zadań.

Jednocześnie informuję, że na podstawie art.30a Prawa oświatowego oraz art.13b Ustawy o systemie oświaty jest Pani/Pan obowiązana/-y do zachowania w poufności wszelkich informacji uzyskanych w związku z pełnioną funkcją lub wykonywaną pracą, w tym w szczególności dotyczących zdrowia, potrzeb rozwojowych i edukacyjnych, możliwości psychofizycznych, seksualności, orientacji seksualnej, pochodzenia rasowego lub etnicznego, poglądów politycznych, przekonań religijnych lub światopoglądowych uczniów.
Obowiązku poufności nie stosuje się:
1) w przypadku zagrożenia zdrowia ucznia;
2) jeżeli uczeń, a w przypadku ucznia niepełnoletniego jego rodzic, wyrazi zgodę na ujawnienie określonych informacji;
3) w przypadku gdy przewidują to przepisy szczególne.

Obowiązek poufności nie przestaje obowiązywać po ustaniu zatrudnienia bądź zaprzestaniu pełnienia funkcji.

.....

(Podpis dyrektora placówki / ADO)

Ja niżej podpisana/y oświadczam że :

1) przed przystąpieniem do pracy przy przetwarzaniu danych osobowych zostałam/em zaznajomiona/y z przepisami dotyczącymi ochrony danych osobowych;
2) zapoznałam/em się i rozumiem zasady dotyczące ochrony danych osobowych opisane w załączniku nr 4 do dokumentacji przetwarzania danych osobowych obowiązującej u Administratora Danych Osobowych oraz zobowiązuje się do ich przestrzegania.

.....

(data i podpis osoby składającej oświadczenie)

(*) ROZPORZĄDZENIE PARLAMENTU EUROPEJSKIEGO I RADY (UE) 2016/679 z dnia 27 kwietnia 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 (ogólne rozporządzenie o ochronie danych).

Zasady ochrony danych osobowych w placówkach oświatowych

Osoba, która przetwarza dane osobowe w systemie informatycznym zapoznaje się z zasadami przetwarzania danych osobowych zawartych w części pierwszej i drugiej. Osoby przetwarzające dane w sposób tylko tradycyjny zapoznają się z zasadami przetwarzania w części drugiej.

Część I

1. Zasady bezpiecznego użytkowania komputerów.

1) Należy mieć świadomość, że dane osobowe mogą znajdować się na twardych dyskach komputerów stacjonarnych i komputerów przenośnych.
2) Każdy pracownik zobowiązany jest do zabezpieczenia komputerów przed dostępem osób nieupoważnionych.
3) Osoba upoważniona ma obowiązek natychmiast zgłosić zagubienie, utratę lub zniszczenie powierzonego mu komputera.
4) Samowolne zmiany (montaż, demontaż) w wyposażeniu komputera bez zgody Dyrekcji są zabronione.
5) Zabrania się przechowywania danych osobowych na komputerach prywatnych i domowych pracowników a w szczególności plików z danymi uczniów.

2. Zasady korzystania z oprogramowania:

1) Osoba upoważniona zobowiązuje się do korzystania wyłącznie z oprogramowania objętego prawami autorskimi.
2) Instalowanie jakiegokolwiek oprogramowania na komputerach może być dokonane wyłącznie przez osobę upoważnioną lub za jej zgodą.
3) Zabroniona jest samowolna zmiana parametrów systemu operacyjnego komputera.
4) Pliki z danymi osobowymi nie powinny być trwale zapisywane na twardych dyskach komputerów, jeżeli komputery nie zapewniają indywidualnego logowania się wszystkich użytkowników. Pliki te powinny być usunięte (skasowane) po ich wykorzystaniu np. do wydruku.

3. Zasady korzystania z internetu:

1) Korzystać z internetu można wyłącznie w celach służbowych, chyba że Administrator wyrazi zgodę na inne cele.
2) Zabrania się zapisywania na dysk twardy komputera oraz uruchamiania nielegalnych/nielicencjonowanych programów oraz plików pobranych z niewiadomego źródła. Pliki takie powinny być pobierane tylko za każdorazową zgodą Administratora i tylko w uzasadnionych przypadkach.
3) Osoba upoważniona ponosi odpowiedzialność za szkody spowodowane przez oprogramowanie instalowane z internetu.
4) Zabrania się wchodzenia na strony, na których prezentowane są informacje o charakterze przestępczym, hakerskim, pornograficznym lub innym zakazanym przez prawo (na większości stron tego typu jest zainstalowane szkodliwe oprogramowanie, infekujące w sposób automatyczny system operacyjny komputera szkodliwym oprogramowaniem).
5) Nie należy 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:".
7) Należy zachować szczególną ostrożność w przypadku żądania lub prośby podania kodów, PIN-ów, numerów kart płatniczych przez internet.

4. Zasady korzystania z poczty elektronicznej:

1) Przesyłanie danych osobowych z użyciem maila poza Placówkę może odbywać się tylko przez osoby upoważnione.

2) W przypadku wysyłania danych osobowych mailem, pliki należy zabezpieczyć hasłem. Hasło należy przesłać odrębnym mailem lub innym kanałem. Rekomendowane jest hasło co najmniej 12 znakowe.
3) Użytkownicy powinni zwracać szczególną uwagę na poprawność adresu odbiorcy dokumentu.
4) Nie należy otwierać załączników (np. plików z rozszerzeniem .exe) w mailach nadesłanych przez nieznanego lub znanego nadawcę.
5) Nie wolno rozsyłać za pośrednictwem maila informacji, które mogą zagrażać systemowi informatycznemu tzw. "łańcuszków szczęścia" itp.
6) Należy okresowo usuwać niepotrzebne maile ze swoich skrzynek pocztowych.
7) Podczas wysyłania maili do wielu adresatów jednocześnie, należy użyć metody " ukryte do wiadomości - UDW".
8) Mail jest przeznaczony wyłącznie do wykonywania obowiązków służbowych, chyba że Dyrekcja placówki zdecyduje o innych celach użycia.

5. **Ochrona antywirusowa:**
1) Zaleca się, aby pracownicy skanowali pliki wprowadzane z zewnętrznych nośników programem antywirusowym.
2) Zakazane jest wyłączanie systemu antywirusowego podczas pracy systemu informatycznego przetwarzającego dane osobowe.
3) W przypadku stwierdzenia zainfekowania systemu, Pracownik zobowiązany jest poinformować niezwłocznie o tym fakcie Administratora.

6. **Polityka haseł:**
1) Hasło dostępu do programu lub do systemu operacyjnego komputera zawierającego dane osobowe składa się co najmniej z 8 znaków (dużych i małych liter oraz cyfr lub znaków specjalnych). Zalecane jest użycie min. 12 znaków.
2) Zmiana hasła następuje nie rzadziej, niż co 30 dni oraz niezwłocznie w przypadku podejrzenia, że hasło mogło zostać ujawnione.
3) Jeżeli zmiany hasła nie wymusza system, wówczas do zmiany hasła zobowiązany jest użytkownik.
4) Hasła nie mogą być powszechnie używanymi słowami. W szczególności nie należy jako haseł wykorzystywać: dat, imion, nazwisk, inicjałów, numerów telefonów.
5) Użytkownik zobowiązuje się do zachowania hasła w poufności, nawet po utracie przez nie ważności.

7. **Procedura rozpoczęcia, zawieszenia i zakończenia pracy.**
1) Użytkownik rozpoczyna pracę z systemem informatycznym przetwarzającym dane osobowe z użyciem identyfikatora i hasła.
2) Użytkownik jest zobowiązany do uniemożliwienia osobom niepowołanym odczytanie danych wyświetlanych na monitorach- tzw. Polityka czystego ekranu.
3) Przed czasowym opuszczeniem stanowiska pracy, użytkownik zobowiązany jest wywołać blokowany hasłem wygaszacz ekranu lub wylogować się z systemu.
4) Po zakończeniu pracy, użytkownik zobowiązany jest:
   a) wylogować się z systemu informatycznego, a następnie wyłączyć sprzęt komputerowy,
   b) zabezpieczyć stanowisko pracy, w szczególności wszelka dokumentację oraz nośniki, na których znajdują sie dane osobowe.

8. **Zasady użytkowania laptopów oraz dysków przenośnych (w tym tablety i smartfony)**
1) Wyłącznie za zgodą Administratora można wynosić laptopy oraz dyski przenośne poza organizację.
2) Wynoszone poza organizację dane osobowe lub inne dane poufne znajdujące się w laptopie lub dysku przenośnym muszą zostać zaszyfrowane hasłem.

3) Laptopy oraz dyski przenośne powinny być wykorzystywane tylko do prac służbowych. W przypadku korzystania z komputera przenośnego w innym celu wszystkie dane osobowe przetwarzane na polecenie ADO muszą być zabezpieczone hasłem.
4) W przypadku kradzieży/zgubienia laptopa lub dysku przenośnego, a także naruszenia ochrony danych osobowych osoba upoważniona zobowiązana jest zgłosić niezwłocznie to zdarzenie ADO.
5) Osoba upoważniona zobowiązana jest do zabezpieczenia laptopa oraz dysku przenośnego w czasie transportu, a przede wszystkim:

a) zaleca się przenoszenie laptopa oraz dysku przenośnego w teczce lub aktówce,
b) zabrania się pozostawiania laptopa oraz dysku przenośnego w samochodzie podczas nieobecności osoby upoważnionej.

6) Użytkownik laptopa oraz dysku przenośnego jest zobowiązany do regularnego tworzenia kopii bezpieczeństwa danych. Nośniki z takimi kopiami powinny być przechowywane w miejscu zabezpieczonym przed dostępem osób nieupoważnionych.
7) Pracując na laptopie oraz dysku przenośnym w miejscach publicznych i środkach transportu, osoba upoważniona zobowiązana jest do chronienia wyświetlanych danych osobowych na monitorze przed wglądem osób nieupoważnionych.
8) Zabrania się logowania do nie zabezpieczonej sieci.
9) W przypadku uszkodzenia lub zużycia nośnika zawierającego dane osobowe, należy dokonać jego fizycznego zniszczenia lub trwałego usunięcia znajdujących się na nim danych.
10) Komputery przenośne należy zabezpieczyć przed dostępem osób nieupoważnionych (np. schować w szafach zamykanych na klucz).

Część II

9. Postępowanie z danymi osobowymi w wersji papierowej:

1) Za bezpieczeństwo dokumentów i wydruków zawierających dane osobowe odpowiedzialne są osoby upoważnione oraz kierownicy właściwych jednostek organizacyjnych.
2) Dokumenty i wydruki zawierające dane osobowe przechowuje się w pomieszczeniach zabezpieczonych fizycznie przed dostępem osób nieupoważnionych.
3) Należy stosować " politykę czystego biurka". Polega ona na zabezpieczeniu dokumentów np. w szafach, biurkach, pomieszczeniach przed kradzieżą lub wglądem osób nieupoważnionych.
4) Niepotrzebne dokumenty oraz tymczasowe wydruki należy niszczyć w niszczarkach niezwłocznie po ustaniu celu ich przetwarzania.
5) Po zakończeniu pracy należy zabezpieczyć (zamykać na klucz w szafach) dokumenty zawierające dane osobowe oraz zabezpieczyć system informatyczny (wyłączyć komputery).

10. Zapewnienie poufności danych osobowych:

1) Osoba upoważniona zobowiązana jest do zachowania w tajemnicy danych osobowych, do których ma lub będzie miał dostęp wskazanych w nadanym upoważnieniu.
2) Osoba upoważniona zobowiązana jest do nie wykorzystywania danych osobowych w celach pozasłużbowych bądź niezgodnych ze zleceniem, o ile nie są one jawne.
3) Osoba upoważniona zobowiązana jest do zachowania w tajemnicy sposobów zabezpieczania danych osobowych o ile nie są one jawne.
4) Zabrania się przekazywania bezpośrednio lub przez telefon danych osobowych osobom nieupoważnionym.
5) Zakazuje się przekazywania informacji o danych osobowych osobom nieupoważnionym, np. sytuacjach towarzyskich, pozazawodowych.
6) Zakazuje się wynoszenia dokumentów zawierających dane osobowe poza placówkę w formie papierowej oraz na nośnikach bez zgody Dyrekcji placówki lub braku podstawy

prawnej. W szczególności dotyczy to wynoszenia list egzaminacyjnych, dokumentacji pedagoga, psychologa, danych medycznych.

11. Postępowanie w przypadku naruszenia ochrony danych osobowych:

1) W przypadku stwierdzenia lub podejrzenia naruszenia ochrony danych osobowych należy niezwłocznie powiadomić Administratora.
2) Typowe sytuacje stwierdzenia lub podejrzenia naruszenia ochrony danych:
   a) ślady na drzwiach, oknach i szafach wskazują na próbę włamania,
   b) dokumentacja jest niszczona bez użycia niszczarki,
   c) fizyczna obecność w budynku lub pomieszczeniach osób zachowujących sie podejrzanie,
   d) otwarte drzwi do pomieszczeń, szaf, gdzie przechowywane są dane osobowe,
   e) wynoszenie danych osobowych w wersji papierowej i elektronicznej na zewnątrz organizacji bez pozwolenia Administratora,
   f) udostępnienie danych osobowych osobom nieupoważnionym w formie papierowej, elektronicznej lub ustnej,
   g) telefoniczne próby wyłudzenia danych,
   h) kradzież komputerów lub CD/DVD, twardych dysków, pendrive-ów z danymi osobowymi,
   i) maile zachęcające do ujawnienia identyfikatora i/lub hasła,
   j) pojawienie się wirusa komputerowego lub niestandardowe zachowanie komputerów,
   k) hasła do systemów przyklejone są w pobliżu komputera.

12. Postępowanie dyscyplinarne.

1) Przypadki nieuzasadnionego zaniechania obowiązków wynikających z niniejszego dokumentu potraktowane będą jako ciężkie naruszenie obowiązków pracowniczych. Wobec osoby, która w przypadku naruszenia danych osobowych lub uzasadnionego domniemania takiego naruszenia nie podjęła działania określonego w niniejszym dokumencie, a w szczególności nie powiadomiła odpowiedniej osoby zgodnie z określonymi zasadami, a także gdy nie zrealizowała stosownego działania dokumentującego ten przypadek, można wszcząć postępowanie dyscyplinarne.
2) Kara dyscyplinarna, orzeczona wobec osoby uchylającej się od powiadomienia nie wyklucza odpowiedzialności karnej tej osoby zgodnie z Rozporządzeniem Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 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 (ogólne rozporządzenie o ochronie danych) oraz możliwości wniesienia wobec niej sprawy z powództwa cywilnego przez administratora o zrekompensowanie poniesionych strat.

13. Postanowienia końcowe:

Z powyższymi zasadami pracownicy zostają zapoznani przed dopuszczeniem do przetwarzania danych osobowych, co zostaje potwierdzone oświadczeniem w treści upoważnienia do przetwarzania danych osobowych.