SZKOŁA PODSTAWOWA NR 4
im. Jana Pawła II
ul. Kochanowskiego 6, 37-100 Łańcut
tel./fax 17 225 00 80
NIP 8151769903, REGON 000803041
www.sp4lancut.pl, e-mail: lancutsp4@op.pl

Zarządzenie nr 22/2020/2021

Dyrektora Szkoły Podstawowej nr 4 w Łańcucie z dnia 1 marca 2021r.

w sprawie wprowadzenia Polityki bezpieczeństwa danych osobowych oraz Instrukcji zarządzania systemami informatycznymi w Szkole Podstawowej nr 4 im. Jana Pawła II w Łańcucie

Na podstawie motywu 74 i 78 oraz art. 24 ust. 1 i 2 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 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 (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L. 2016. 119. 1) zarządzam co następuje:

§1

Wprowadzam do stosowania *Politykę bezpieczeństwa danych osobowych oraz Instrukcję zarządzania systemami informatycznymi w Szkole Podstawowej nr 4 im. Jana Pawła II w Łańcucie* stanowiącą załącznik nr 1 do niniejszego Zarządzenia.

§2

Zobowiązuję wszystkich pracowników Szkoły Podstawowej nr 4 im. Jana Pawła II w Łańcucie do bezwzględnego stosowania i przestrzegania ustaleń zawartych w *Polityce bezpieczeństwa danych osobowych oraz Instrukcji zarządzania systemami informatycznymi w Szkole Podstawowej nr 4 im. Jana Pawła II w Łańcucie.*

§3

Traci moc Zarządzenie nr 7/2018/2019 Dyrektora Szkoły Podstawowej nr 4 im. Jana Pawła II w Łańcucie z dnia 14 grudnia 2018r. w sprawie wprowadzenia Polityki ochrony danych osobowych w Szkole Podstawowej nr 4 im. Jana Pawła II w Łańcucie.

§5

Zarządzenie wchodzi w życie z dniem podpisania.

p.o. DYREKTOR SZKOŁY
mgr Agnieszka Słysz

SZKOŁA PODSTAWOWA NR 4
im. Jana Pawła II
ul. Kochanowskiego 6, 37-100 Łańcut
tel./fax 17 225 00 80
NIP 8151769903, REGON 000803041
www.sp4lancut.pl, e-mail: lancutsp4@op.pl

Załącznik nr 1

do Zarządzenia nr 22/2020/2021

Dyrektora Szkoły Podstawowej nr 4 w Łańcucie

z dnia 1.03.2021r.

POLITYKA BEZPIECZEŃSTWA DANYCH OSOBOWYCH ORAZ INSTRUKCJA ZARZĄDZANIA SYSTEMAMI INFORMATYCZNYMI W SZKOLE PODSTAWOWEJ NR 4 W ŁAŃCUCIE

CZĘŚĆ I – WSTĘP

§ 1. 1. Polityka bezpieczeństwa danych osobowych oraz Instrukcja zarządzania systemami informatycznymi w Szkole Podstawowej nr 4 im. Jana Pawła II w Łańcucie (*dalej jako Polityka*) jest zbiorem zasad i procedur obowiązujących przy przetwarzaniu i wykorzystywaniu danych osobowych we wszystkich czynnościach przetwarzania i kategoriach czynności przetwarzania danych osobowych w Szkole Podstawowej nr 4 im. Jana Pawła II w Łańcucie (*dalej jako Szkoła*).

2. Podstawą do opracowania i wdrożenia dokumentu są:

1) 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);
2) ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych;
3) ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne;
4) rozporządzenie Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych;
5) ustawa z dnia 21 lutego 2019 r. o zmianie niektórych ustaw w związku z zapewnieniem stosowania rozporządzenia 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 (RODO).

§ 2. 1. Przetwarzanie danych osobowych w Szkole jest dopuszczalne wyłącznie pod warunkiem przestrzegania przepisów wyżej wymienionych aktów prawnych, wydanych na ich podstawie przepisów wykonawczych oraz Zarządzeń Dyrektora Szkoły w sprawie ochrony danych osobowych i bezpieczeństwa informacji.

2. Opisane i zastosowane w niniejszej Polityce zabezpieczenia mają zapewnić:

1) poufność danych, rozumianą jako właściwość zapewniającą, że dane nie są udostępniane nieupoważnionym osobom;
2) integralność danych, rozumianą jako właściwość zapewniającą, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany;
3) rozliczalność, rozumianą jako właściwość zapewniającą, że działania osoby mogą być przypisane w sposób jednoznaczny tylko tej osobie;
4) integralność systemu, rozumianą jako nienaruszalność systemu, niemożność jakiejkolwiek manipulacji, zarówno zamierzonej jak i przypadkowej.

§3. Użyte w dalszej części dokumentu sformułowania oznaczają:

1) Dane osobowe – wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej. Osobą możliwą do zidentyfikowania jest osoba, której tożsamość można określić bezpośrednio lub pośrednio, w szczególności przez powołanie się na numer identyfikacyjny albo jeden lub kilka specyficznych czynników określających jej cechy fizyczne, fizjologiczne, umysłowe, ekonomiczne, kulturowe lub społeczne. Informacji nie uważa się za umożliwiającą określenie tożsamości osoby, jeżeli wymagałoby to nadmiernych kosztów, czasu lub działań;
2) Przetwarzanie danych – rozumie się przez to jakiekolwiek operacje wykonywane na danych osobowych, takie jak: zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, kopiowanie, udostępnianie i usuwanie, a zwłaszcza te, które wykonuje się w systemach informatycznych;
3) Administrator Danych Osobowych (ADO lub Administrator) – Szkoła, w imieniu której działa Dyrektor Szkoły;
4) Osoba upoważniona – osoba posiadająca upoważnienie nadane przez Administratora danych osobowych i dopuszczona jako użytkownik do przetwarzania danych osobowych w systemie tradycyjnym lub informatycznym w zakresie wskazanym w upoważnieniu, w tym: pracownicy, stażyści, praktykanci, przedstawiciele podmiotu zewnętrznego;
5) Pracownicy – osoby świadczące pracę na podstawie umowy o pracę lub umowy cywilnoprawnej dla Szkoły;
6) Podmiot przetwarzający – rozumie się przez to osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który przetwarza dane osobowe na rzecz i w imieniu Administratora Danych;
7) UODO – rozumie się przez to Urząd Ochrony Danych Osobowych;
8) RODO – rozumie się przez to rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z 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;
9) Profilowanie – rozumie się przez to dobrowolną formę zautomatyzowanego przetwarzania danych osobowych, które polega na wykorzystaniu danych osobowych do oceny niektórych czynników osobowych osoby fizycznej, w szczególności do analizy lub prognozy aspektów dotyczących efektów pracy tej osoby fizycznej, jej sytuacji ekonomicznej, zdrowia, osobistych preferencji, zainteresowań, zachowania lub przemieszczania się.

CZĘŚĆ II – ZASADY PRZETWARZANIA DANYCH OSOBOWYCH

§ 4. 1. Dane osobowe muszą być:

1) przetwarzane zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osoby, której dane dotyczą (zasada zgodności z prawem, rzetelności i przejrzystości);
2) zbierane w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami; dalsze przetwarzanie do celów archiwalnych w interesie publicznym lub do celów statystycznych nie jest uznawane za niezgodne z pierwotnymi celami (zasada ograniczenia celu przetwarzania);
3) adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane (zasada minimalizacji danych);
4) prawidłowe i w razie potrzeby uaktualniane; należy podjąć wszelkie rozsądne działania, aby dane osobowe, które są nieprawidłowe w świetle celów ich przetwarzania, zostały niezwłocznie usunięte lub sprostowane (zasada prawidłowości danych);
5) przechowywane w formie umożliwiającej identyfikację osoby, której dane dotyczą, przez okres nie dłuższy, niż jest to niezbędne do celów, w których dane te są przetwarzane; dane osobowe można przechowywać przez okres dłuższy, o ile będą one przetwarzane wyłącznie do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych, z zastrzeżeniem, że wdrożone zostaną odpowiednie środki techniczne i organizacyjne wymagane na mocy przepisów RODO w celu ochrony praw i wolności osób, których dane te dotyczą (zasada ograniczenia przechowywania);
6) przetwarzane w sposób zapewniający odpowiednie bezpieczeństwo danych osobowych, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem, za pomocą odpowiednich środków technicznych lub organizacyjnych (zasada integralności i poufności).

2. ADO jest odpowiedzialny za przestrzeganie przepisów ust. 1 i musi być w stanie wykazać ich przestrzeganie (zasada rozliczalności).

§ 5. Dla skutecznej realizacji niniejszej Polityki zapewnia się:

1) stosowanie odpowiednich do zagrożeń i kategorii danych objętych ochroną, środków technicznych i organizacyjnych zapewniających rzeczywiste bezpieczeństwo ich przetwarzania;
2) opracowanie, wdrożenie i aktualizowanie wymaganej przepisami prawa dokumentacji dotyczącej przetwarzania danych osobowych;
3) powołanie Inspektora Danych Osobowych;
4) szkolenia osób zaangażowanych w proces przetwarzania danych w zakresie ochrony danych osobowych;
5) okresowe szacowanie ryzyka zagrożeń dla danych osobowych;
6) monitorowanie i koordynowanie stosowanych środków ochrony i bezpieczeństwa danych osobowych.

§ 6. Zakres stosowania Polityki ochrony danych osobowych dotyczy zarówno danych osobowych przetwarzanych w sposób tradycyjny - w księgach, rejestrach, wykazach, aktach i innych zbiorach ewidencyjnych, jak i w systemach informatycznych wykorzystywanych do przetwarzania danych osobowych.

§ 7. Dane osobowe przetwarzane są w pomieszczeniach znajdujących się w budynku Szkoły. Wykaz pomieszczeń, w których przetwarzane są dane osobowe stanowi ***załącznik nr 1*** do niniejszej Polityki.

§ 8. 1. W Szkole przetwarzanie danych ograniczone jest do niezbędnego, prawem wymaganego minimum.

2. Minimalizacja przetwarzania danych odnosi się do:

a) zakresu danych czyli ilości potrzebnych danych oraz zakresu przetwarzania;
b) dostępu do danych;
c) czasu przechowywania danych.

3. Minimalizacja zakresu polega na tym, że w Szkole na bieżąco prowadzony jest przegląd ilości przetwarzanych danych i zakresu ich przetwarzania zgodnie z zasadą ochrony danych w fazie projektowania i zasadą domyślnej ochrony danych.

4. Minimalizacja dostępu polega na tym, że w Szkole stosuje się ograniczenia dostępu do danych osobowych (prawne tj. zobowiązania do poufności, zakresy upoważnień), fizyczne (zamykane pomieszczenia) oraz logiczne (hasła do komputerów).

5. Minimalizacja czasu polega na tym, że w Szkole przetwarza się dane osobowe:

a) do czasu osiągnięcia celu przetwarzania lub wycofania zgody na przetwarzanie;
b) do czasu upłynięcia terminów przewidzianych w przepisach prawa;
c) których zakres przydatności upływa - dane te są archiwizowane przez okres zgodny z ustawą o narodowym zasobie archiwalnym i archiwach.

§ 9. W Szkole nie identyfikuje się przypadków, w których dokonywane jest profilowanie przetwarzanych danych. W przypadku zastosowania profilowania zostaną wdrożone odpowiednie mechanizmy zapewniające zgodność tego procesu z przepisami prawa, a osoby, których dane będą w takim przypadku przetwarzane zostaną o tym poinformowane

CZĘŚĆ III - ZASADY OCHRONY DANYCH OSOBOWYCH

§ 10. 1. Za bezpieczeństwo danych osobowych w Szkole odpowiada Dyrektor, który w myśl przepisów RODO, obowiązany jest zastosować środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną.

2. W zakresie ochrony danych osobowych Dyrektor wykonuje nałożone przez przepisy obowiązki m.in. poprzez:

a) Inspektora Ochrony Danych;
b) pracowników, którzy realizują zadania określone w ich zakresach czynności i w przyznanych upoważnieniach oraz inne osoby upoważnione;
c) podmioty przetwarzające dane na podstawie umowy powierzenia.

3. Każda osoba upoważniona jest odpowiedzialna za zapewnienie prawidłowego przetwarzania danych osobowych, z którymi pracuje.

4. Każda osoba upoważniona ma obowiązek realizować obowiązki informacyjne określone w rozdziale III RODO, w tym w szczególności obowiązek podejmowania określonych środków i czynności, aby w sposób zrozumiały, zwięzły, jasnym i prostym językiem udzielić osobie wyczerpujących informacji na temat przetwarzania jej danych osobowych.

§ 11. 1. W celu jak najlepszej ochrony danych osobowych oraz w celu realizacji zapisów rozporządzenia powołany został Inspektor ochrony danych *(dalej także jako IOD)*.

2. Główne zadania Inspektora to:

a) informowanie Administratora i pracowników, którzy przetwarzają dane osobowe o obowiązkach spoczywających na nich w zakresie ochrony danych osobowych;
b) monitorowanie przestrzegania zapisów niniejszej Polityki;
c) udzielanie ustnych i pisemnych informacji klientom Szkole w zakresie zagadnień dotyczących przetwarzania danych osobowych;
d) przyjmowanie zgłoszenia o wystąpieniu naruszenia bezpieczeństwa danych osobowych przetwarzanych w Szkole;
e) zawiadamianie osób, których dane dotyczą o naruszeniu ochrony danych osobowych;
f) pełnienie funkcji punktu kontaktowego dla organu nadzorczego w kwestiach związanych z przetwarzaniem danych osobowych;
g) pomaganie Administratorowi w prowadzeniu rejestru czynności przetwarzania danych osobowych;
h) pomaganie Administratorowi w bieżącej aktualizacji „Ewidencji osób upoważnionych do przetwarzania danych osobowych".

3. Inspektor ochrony danych jest zobowiązany do zachowania tajemnicy i poufności w wykonywaniu swoich zadań.

§ 12. Każda osoba upoważniona do przetwarzania danych osobowych zobligowana jest do stosowania niezbędnych środków zapobiegających ujawnieniu tych danych, w tym do:

1) ochrony danych osobowych przed dostępem osób nieupoważnionych (osoba nie może pod rygorem odpowiedzialności służbowej i karnej - ujawniać danych, kopiować baz danych oraz przetwarzać danych w sposób inny niż opisany procedurami);
2) przetwarzania danych osobowych wyłącznie w zakresie ustalonym przez Administratora Danych Osobowych i tyko w celu wykonywania nałożonych na nią obowiązków i zadań;
3) zapoznania się z przepisami dotyczącymi ochrony danych osobowych oraz Polityką bezpieczeństwa danych osobowych i Instrukcją zarządzania systemami informatycznymi;
4) potwierdzenia zapoznania się z przepisami dotyczącymi ochrony danych osobowych oraz niniejszej Polityki w stosownym oświadczeniu o zachowaniu poufności;
5) ochrony danych przed przypadkowym lub nieumyślnym zniszczeniem, utratą lub modyfikacją;
6) zachowania w tajemnicy przetwarzanych danych osobowych, przestrzegania procedur i zasad ich przetwarzania, w tym utrzymywania w tajemnicy powierzonych identyfikatorów, haseł (również w zakresie częstotliwości ich zmiany) – także po ustaniu stosunku pracy lub odwołaniu z pełnionej funkcji;

7) stosowania określonych przez Administratora Danych Osobowych procedur oraz wytycznych mających na celu zgodne z prawem przetwarzanie danych;
8) korzystania z systemu informatycznego Administratora Danych Osobowych w sposób zgodny ze wskazówkami zawartymi w instrukcjach obsługi urządzeń, wchodzących w skład systemu informatycznego, oprogramowania i nośników;
9) dbałości o należyte zabezpieczenie wszelkich kartotek, arkuszy, rejestrów, ewidencji, akt, zawierających dane osobowe.

§ 13. Każda osoba upoważniona do przetwarzania danych osobowych jest zobowiązana do zachowania następujących zasad praktycznych podczas przetwarzania danych:

1) do przetwarzania danych osobowych dopuszczona może być wyłącznie osoba posiadająca aktualne upoważnienie nadane przez Administratora;
2) po zakończeniu pracy wszystkie dokumenty zawierające dane osobowe należy schować do szafki zamykanej na zamek, zamknąć szafkę oraz schować klucz uniemożliwiając w ten sposób dostęp do dokumentów dla osób nieuprawnionych; pomieszczenie biurowe należy zamknąć na klucz;
3) po wejściu do pomieszczenia biurowego przed rozpoczęciem pracy, pracownik ma obowiązek każdorazowo sprawdzić, czy meble biurowe są zamknięte;
4) podczas przyjmowania petentów na biurku pracownika nie mogą znajdować się żadne dokumenty, które zawierają dane osobowe inne niż dane dotyczące obsługiwanej osoby (tzw. zasada czystego biurka);
5) po przyjęciu petenta, należy zwrócić uwagę na to, czy nie zabrał on (celowo lub przypadkiem) jakiegokolwiek nie należącego do niego dokumentu;
6) podczas przenoszenia dokumentów zawierających dane osobowe należy zachować ostrożność, aby nie dopuścić do przedostania się dokumentu w niepowołane ręce (w szczególności podczas kopiowania i skanowania dokumentów);
7) zabrania się wynoszenia dokumentów zawierających dane osobowe poza pomieszczenie biurowe, w którym jest wykonywana praca, chyba że charakter pracy z danym dokumentem wymusza sytuację jego przemieszczenia;
8) podczas przemieszczania dokumentów zawierających dane osobowe, a także w trakcie wykonywania czynności służbowych, należy zachować szczególną staranność tj. nie zostawiać dokumentów bez opieki oraz chronić je przed dostępem osób nieuprawnionych;
9) w przypadku konieczności zniszczenia papierowych dokumentów zawierających dane osobowe, ich zniszczenia dokonuje się poprzez pocięcie w niszczarce.

§ 14. 1. Dyrektor odpowiada za nadawanie, zmianę i cofnięcie (odebranie) upoważnień do przetwarzania danych osobowych w Szkole.

2. Każda osoba upoważniona może przetwarzać dane wyłącznie na podstawie przepisu prawa lub na polecenie Administratora.

3. Dostęp do danych osobowych, na podstawie upoważnienia uzyskują:

a) osoby zatrudnione w Szkole, które przetwarzają dane osobowe w ramach swoich obowiązków służbowych, a także stażyści i praktykanci;
b) osoby świadczące usługi na podstawie umów cywilnoprawnych.

4. Upoważnienie do przetwarzania danych osobowych jest udzielane po zapoznaniu się z przepisami prawa dotyczącymi ochrony danych osobowych oraz z obowiązującą w Szkole Polityką, jak również po podpisaniu przez osobę oświadczenia

o zachowaniu w tajemnicy przetwarzanych informacji - oświadczenia o poufności, które stanowi ***załącznik nr 2*** do niniejszej Polityki.

5. Każdy pracownik mający dostęp do danych osobowych musi posiadać pisemne upoważnienie do przetwarzania tych danych nadane przez Administratora Danych Osobowych, które stanowi ***załącznik nr 3*** do niniejszej Polityki. Upoważnienie wydawane jest w dwóch egzemplarzach - jeden zostaje wręczony pracownikowi zaś drugi składany jest do jego akt osobowych. W upoważnieniu wskazywany jest również system informatyczny, jaki może obsługiwać pracownik otrzymujący upoważnienie.

6. Podstawy do wycofania i nadania nowego upoważnienia nie stanowi w szczególności: przeniesienie na inne stanowisko pracy, zmiana nazwy stanowiska pracy, nawiązanie kolejnego stosunku pracy czy cywilnoprawnego z tą samą osobą, o ile nie wpływa na zakres danych osobowych przetwarzanych na stanowisku.

7. Na podstawie nadanych upoważnień prowadzona jest w Szkole „Ewidencja osób upoważnionych do przetwarzania danych osobowych", której wzór stanowi ***załącznik nr 4*** do niniejszej Polityki.

CZĘŚĆ IV - UDOSTĘPNIANIE DANYCH I POWIERZANIE ICH DO PRZETWARZANIA

§ 15. 1. ADO udostępnia dane osobowe przetwarzane we własnych zbiorach tylko osobom lub podmiotom uprawnionym do ich otrzymania na mocy przepisów prawa.

2. Dane osobowe mogą być udostępniane w następujących przypadkach:

1) z uwzględnieniem przepisów prawa;
2) w sytuacjach, gdy jest ono niezbędne do realizacji prawnie uzasadnionych celów Administratora;
3) za wyraźną zgodą podmiotu, którego dane dotyczą.

3. Wniosek o udostępnienie danych osobowych powinien zawierać informacje umożliwiające wyszukanie żądanych danych osobowych w zasobie oraz wskazywać ich zakres, cel i przeznaczenie.

4. W przypadku konieczności udostępnienie dokumentów i danych, wśród których znajdują się dane osobowe niemające bezpośredniego związku z celem udostepnienia, należy bezwzględnie dokonać anonimizacji tych danych osobowych.

§ 16. 1. Powierzenie przetwarzania danych osobowych może się odbyć tylko na podstawie pisemnej umowy, w której wyraźnie zostanie określony charakter i cel przetwarzania, przedmiot i czas trwania przetwarzania, rodzaj danych osobowych, a także obowiązki podmiotu przetwarzającego.

2. Dane mogą zostać powierzone wyłączenie podmiotom, które gwarantują odpowiednie środki techniczne i organizacyjne do skutecznej ochrony praw osób, których dane dotyczą.

3. Przykładowa umowa powierzenia przetwarzania danych stanowi ***załącznik nr 5*** do niniejszej Polityki.

4. Administrator prowadzi ewidencję zawartych umów powierzania danych, której wzór stanowi ***załącznik nr 6*** do niniejszej Polityki.

CZĘŚĆ IV - REJESTR CZYNNOŚCI PRZETWARZANIA DANYCH OSOBOWYCH

§ 17. 1. W Szkole prowadzony jest „Rejestr czynności przetwarzania danych osobowych". Rejestr ten powinien być na bieżąco aktualizowany.

2. Rejestr czynności przetwarzania danych osobowych zawierać powinien następujące informacje:

1) nazwę czynności przetwarzania,
2) stanowisko pracy,
3) cel przetwarzania,
4) opis kategorii osób, których dane dotyczą,
5) opis kategorii danych osobowych,
6) podstawę prawną przetwarzania danych,
7) źródło danych, z którego dane zostały pozyskane,
8) planowany termin usunięcia kategorii danych,
9) nazwę współadministratora i jego dane kontaktowe,
10) nazwę podmiotu przetwarzającego i jego dane kontaktowe,
11) kategorie odbiorców,
12) nazwa systemu lub oprogramowania,
13) ogólny opis technicznych i organizacyjnych środków bezpieczeństwa,
14) ocena skutków dla ochrony danych (DPIA),
15) transfer do kraju trzeciego lub organizacji międzynarodowej i dokumentacja odpowiednich zabezpieczeń, jeżeli dotyczy.

3. Rejestr czynności przetwarzania ma charakter dokumentu wewnętrznego i z uwagi na zawarte w nim informacje (np. o zabezpieczeniach ochrony danych osobowych) nie może być udostępniony osobom nieuprawnionym.

CZĘŚĆ IV - REALIZIOWANIE PRAW OSÓB, KTÓRYCH DANE PRZETWARZANE SĄ W SZKOLE

§ 18. 1. W Szkole respektuje się prawa osób, których dane są przetwarzane, a w szczególności:

a) zapewnia się osobom, których dane dotyczą możliwość wyrażenia i wycofania zgody na przetwarzanie danych osobowych;
b) informuje się osoby, których dane dotyczą o zbieraniu i przetwarzaniu tych danych;
c) prawo dostępu osobom, których dane dotyczą;
d) prawo sprostowania swoich danych;
e) prawo do usunięcia swoich danych (prawo do bycia zapomnianym);
f) prawo do przeniesienia swoich danych;
g) prawo do ograniczenia przetwarzania swoich danych.

§ 19. 1. Dane osobowe przetwarzane w Szkole mogą być pozyskiwane bezpośrednio od osób, których dotyczą lub z innych źródeł, w granicach dozwolonych przepisami prawa.

2. Zebrane dane osobowe mogą być wykorzystywane wyłącznie do celów, dla jakich były, są lub będą zbierane i przetwarzane.

3. Dane osobowe pochodzące od osób, których dotyczą, a których obowiązek podania nie wynika wprost z przepisów prawa, mogą być przetwarzane po otrzymaniu zgody tej osoby wyrażonej na piśmie (klauzula zgody). Należy przy tym wskazać cel dla jakiego dane zostają zebrane.

§ 20. W przypadku gdy dane osobowe są niekompletne, nieaktualne, nieprawdziwe lub zostały zebrane z naruszeniem przepisów RODO albo są zbędne do realizacji celu, dla którego zostały zebrane, ADO jest zobowiązany do ich: uzupełnienia, uaktualnienia, sprostowania lub usunięcia.

§ 21. 1. ADO zobowiązany jest do informowania osób, których dane przetwarza o adresie swojej siedziby, celu zbierania danych osobowych, podstawie prawnej przetwarzania, danych kontaktowych IOD oraz innych, określonych w przepisach RODO.

2. Obowiązek informacyjny względem osób, których dane są przetwarzane realizuje się poprzez:

a) przekazanie osobom (klientom) informacji wymaganych prawem – informację należy przekazać w sposób zwięzły, przejrzysty, w zrozumiałej formie, jasnym i prostym językiem. Informacji tej udziela się na piśmie bądź ustnie, w zależności od sytuacji;
b) realizacja zgłaszanych przez klientów żądań, w tym np. dostępu, usunięcia lub ograniczenia przetwarzania danych osobowych musi być zgodna z przepisami prawa, na podstawie których odbywa się przetwarzanie oraz na podstawie przepisów prawa określających zasady przetwarzania dokumentacji archiwalnej.

3. Realizacja obowiązku informacyjnego określonego w art. 13 RODO polega na udostępnianiu i stosowaniu klauzul informacyjnych i klauzul zgody, których wzór stanowi ***załącznik nr 7*** do niniejszej Polityki.

4. W celu skutecznego informowania osób, których dane osobowe są przetwarzane można stosować następujące sposoby:

a) umieszczanie informacji na stronie internetowej Szkoły;
b) umieszczenie informacji w postaci tabliczki przy stanowiskach pracy pracowników Szkoły;
c) umieszczenie informacji w odrębnym dokumencie, na którym klient może potwierdzić fakt zapoznania się z nimi;
d) ustne przekazywanie informacji obsługiwanym klientom;
e) umieszczenie informacji w korespondencji przesyłanej do klientów Szkoły.

5. Wybór sposobu uzależniony jest do charakteru prowadzonych działań i specyfiki sprawy.

6. Jakiekolwiek modyfikowanie klauzul określonych w ***załączniku nr 7*** lub tworzenie nowych klauzul - stosownie do potrzeb wynikłych ze specyfiki pracy poszczególnych

stanowisk - może odbywać się wyłącznie po uzgodnieniu z IOD i uzyskaniu jego wyraźnej zgody.

7. Wszyscy pracownicy posiadający upoważnienie do przetwarzania danych osobowych ponoszą odpowiedzialność za prawidłowe stosowanie klauzul informacyjnych i klauzul zgód.

CZĘŚĆ V - POSTĘPOWANIE W PRZYPADKACH NARUSZENIA BEZPIECZEŃSTWA DANYCH OSOBOWYCH

§ 22. 1. Zasady postępowania w przypadku naruszenia bezpieczeństwa danych osobowych obowiązują wszystkie osoby biorące udział w procesie przetwarzania danych osobowych.

2. Sytuacja zagrożenia bezpieczeństwa danych osobowych w postaci incydentów, naruszeń lub słabości systemu następuje w przypadkach:

1) podejrzenia naruszenia bezpieczeństwa danych osobowych m. in.: ze względu na stan urządzenia, ujawnione metody pracy, sposób działania programu lub jakość komunikacji w sieci komputerowej, zawartość zasobu danych osobowych w księgach, rejestrach, wykazach, aktach i innych zbiorach ewidencyjnych;
2) stwierdzenia naruszenia zabezpieczenia systemu informatycznego w obszarze danych osobowych bądź stwierdzenia naruszenia zasobu danych osobowych przetwarzanych w formie tradycyjnej.

§ 23. Z uwagi na wymogi RODO, w tym krótki okres na zgłoszenie naruszenia bezpieczeństwa danych osobowych (72 godziny od stwierdzenia wykrycia naruszenia) informacje w tym zakresie muszą być przekazywane ADO natychmiastowo, bez zbędnej zwłoki.

§ 24. 1. ADO jest odpowiedzialny za analizę sytuacji zagrożeń ochrony danych osobowych oraz stosownie do potrzeb – zgłoszenie naruszenia ochrony danych osobowych organowi nadzorczemu oraz zawiadomienie osoby, której dane dotyczą, o naruszeniu bezpieczeństwa danych osobowych.

2. Typowymi źródłami informacji o incydentach, zagrożeniach lub słabościach systemu są:

1) zgłoszenia od pracowników i osób upoważnionych;
2) wiedza IOD;
3) wyniki kontroli wewnętrznych IOD, audytów, kontroli zewnętrznych UODO, NIK, PIP i pozostałych instytucji uprawnionych.

§ 25. 1. W przypadku naruszenia ochrony danych osobowych sporządza się raport o naruszeniu, którego wzór stanowi ***załącznik nr 8*** do niniejszej Polityki.

2. Typowe sytuacje, o których pracownik powinien powiadomić Administratora danych osobowych oraz Inspektora ochrony danych:

1) ślady na drzwiach, oknach i szafach wskazujące na próbę włamania;
2) zniszczenie dokumentacji zawierającej dane osobowe bez użycia niszczarki;
3) fizyczna obecność w budynku lub pomieszczeniu osób zachowujących się podejrzanie;
4) otwarte drzwi do pomieszczeń lub szaf, w których przechowywane są dane osobowe;
5) ustawienie monitorów pozwalające na wgląd osób postronnych w dane osobowe;
6) wynoszenie danych osobowych w wersji papierowej i elektronicznej na zewnątrz Szkoły bez zgody ADO;
7) udostępnienie danych osobowych osobom nieupoważnionym w formie papierowej, elektronicznej lub ustnej;
8) telefoniczne próby wyłudzenia danych osobowych;
9) kradzież komputerów lub CD, twardych dysków, pendriv`e z danymi osobowymi;
10) e-maile zachęcające do ujawnienia identyfikatora i/lub hasła;
11) pojawienie się wirusa komputerowego lub niestandardowe zachowanie komputerów;
12) przechowywanie haseł do systemów w pobliżu komputera.

CZEŚĆ VI. SPRAWDZENIE ZGODNOŚCI PRZETWARZANIA DANYCH OSOBOWYCH Z PRZEPISAMI PRAWA

§ 26. 1. Celem sprawdzenia jest weryfikacja czynności podejmowanych przy przetwarzaniu danych osobowych pod kątem zgodności z przepisami o ochronie danych osobowych, ocena obowiązywania niniejszej Polityki oraz opracowanie w tym zakresie sprawozdania dla Administratora Danych Osobowych.

2. Sprawdzenie może odbyć się w formie audytu wewnętrznego, spełniającego wymogi rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych.

3. Za przeprowadzenie sprawdzenia odpowiada IOD.

§ 27. 1. IOD przygotowuje plan sprawdzeń uwzględniając zakres oraz termin przeprowadzenia poszczególnych sprawdzeń oraz sposób i zakres ich dokumentowania. IOD prowadzi sprawdzenia zgodnie z planem lub podejmuje sprawdzenia doraźne na skutek podejrzenia naruszenia lub naruszenia wymagań ochrony danych osobowych.

2. IOD może dokumentować przebieg sprawdzeń w postaci danych i wydruków z kontrolowanych systemów (programów) oraz poprzez sporządzanie: notatek z czynności, protokołów odebrania ustnych wyjaśnień, protokołów z oględzin, kopii dokumentów, logów systemowych, zapisów konfiguracji technicznych środków zabezpieczeń systemów. Z całości przeprowadzonego sprawdzenia IOD sporządza protokół.

4. W przypadku ujawnienia nieprawidłowości w procesie przetwarzania danych IOD zawiadamia o tym fakcie Administratora, wskazując przy tym działania korygujące jakie powinien on podjąć w celu doprowadzenia procesu przetwarzania do zgodności z przepisami prawa i wyznaczając mu odpowiedni termin do wdrożenia zaleconego postępowania. Po upływie tego terminu IOD dokonuje ponownego sprawdzenia, oceniając skuteczność podjętych działań.

CZĘŚĆ VII – INSTRUKCJA ZARZĄDZANIA SYSTEMAMI INFORMATYCZNYMI

§ 28. 1. Przyznanie uprawnień do przetwarzania danych osobowych w systemie informatycznym polega na przekazaniu dostępu w postaci identyfikatora, hasła oraz ustalenia zakresu dostępnych danych.

2. Za wygenerowanie identyfikatora i hasła użytkownikowi odpowiada Administrator danych przy współpracy z informatykiem obsługującym działanie systemu informatycznego w Szkole.

§ 29. 1. Dostęp do danych osobowych przetwarzanych w systemie informatycznym użytkownik otrzymuje po podaniu identyfikatora i hasła.

2. Identyfikator jest w sposób jednoznaczny przypisany użytkownikowi. Użytkownik jest odpowiedzialny za wszystkie czynności wykonane przy użyciu swojego identyfikatora.

3. Użytkownik otrzymuje swoje hasło początkowe z chwilą przystąpienia do pracy w systemie informatycznym. Hasło przydzielone do użytkownika musi być zmienione po pierwszym udanym zalogowaniu się do systemu informatycznego.

4. Hasło jest zmieniane przez użytkownika po upływie 30 dni od ostatniej zmiany.

5. Hasło składa się z co najmniej 6 znaków i powinno zawierać co najmniej jedną dużą literę i jeden znak specjalny.

6. Hasło nie może być zapisane w miejscu dostępnym dla osób nieuprawnionych i należy je zachować w tajemnicy.

7. Użytkownik nie może udostępniać osobom nieuprawnionym swojego identyfikatora oraz hasła. Po uwierzytelnieniu w systemie użytkownik nie może udostępniać swojego stanowiska pracy osobom nieupoważnionym. Niedopuszczalne jest by dwóch lub większa liczba użytkowników wykorzystywała wspólnie jedno konto użytkownika.

8. W przypadku gdy istnieje podejrzenie, że hasło mogła poznać osoba nieuprawniona, użytkownik zobowiązany jest niezwłocznie zmienić hasło oraz powiadomić o tym Administratora danych osobowych.

§ 30. Procedury rozpoczęcia, zawieszenia i zakończenia pracy przeznaczone dla użytkowników systemu przebiegają następująco:

1) Przed rozpoczęciem pracy, w trakcie rozpoczynania pracy z systemem informatycznym oraz w trakcie pracy każdy pracownik zobowiązany jest do zwrócenia uwagi, czy nie wystąpiły symptomy mogące świadczyć o naruszeniu ochrony danych osobowych.
2) Użytkownik rozpoczynając pracę na komputerze loguje się do systemu informatycznego.
3) Przebywanie osób nieuprawnionych w pomieszczeniach znajdujących się na obszarze, w którym przetwarzane są dane osobowe, jest dopuszczalne tylko w obecności osoby upoważnionej do ich przetwarzania.

4) Pomieszczenia, w których przetwarzane są dane osobowe, należy zamykać na czas nieobecności osób upoważnionych, w sposób uniemożliwiający dostęp do nich osobom nieupoważnionym.
5) Monitory stanowisk komputerowych, na których przetwarzane są dane osobowe, znajdujące się w pomieszczeniach, gdzie przebywają osoby, które nie posiadają upoważnień do przetwarzania danych osobowych, powinny być ustawione w taki sposób, aby uniemożliwiały tym osobom wgląd w dane.
6) W sytuacji opuszczenia stanowiska pracy przez użytkownika na odległość uniemożliwiającą jego obserwację należy wylogować się z systemu.
7) Przed opuszczeniem stanowiska pracy użytkownik zobowiązany jest wywołać wygaszacz ekranu bądź wylogować się z systemu informatycznego.
8) Kończąc pracę użytkownik obowiązany jest wylogować się z systemu informatycznego, a następnie wyłączyć sprzęt komputerowy.
9) Wszelką dokumentację oraz nośniki magnetyczne i optyczne, na których znajdują się dane osobowe, przechowuje się w szafkach zamykanych na klucz.
10) Przesyłanie danych osobowych z użyciem wiadomości e-mail poza organizację jest co do zasady zabronione. Może zostać dokonane wyłącznie przez osobę wyraźnie do tego upoważnioną przez Administratora. W takim przypadku przesyłane pliki z danymi są zabezpieczone hasłem.
11) Zakazane jest przesyłanie korespondencji służbowej na prywatne skrzynki pocztowe.
12) Podczas wysyłania e-maili do wielu adresatów jednocześnie należy używać metody „Ukryte do wiadomości - UDW"; zabronione jest rozsyłanie maili do wielu adresatów - nie będących pracownikami Szkoły - z użyciem opcji „Do wiadomości - DW".

§ 31. Procedury tworzenia kopii zapasowych przebiegają następująco:

1) Dane osobowe przetwarzane w systemie informatycznym podlegają zabezpieczeniu poprzez tworzenie kopii zapasowych.
2) Za tworzenie kopii zapasowych odpowiedzialny jest każdy użytkownik systemu informatycznego.
3) Kopie zapasowe zbiorów danych są tworzone co najmniej dwa razy w roku, w szczególnych przypadkach – przed aktualizacją lub zmianą w systemie.
4) Nośniki kopii zapasowych, które zostały wycofane z użycia należy pozbawić zapisanych danych za pomocą specjalnego oprogramowania do bezpiecznego usuwania zapisanych danych; w przeciwnym wypadku podlegają fizycznemu zniszczeniu w sposób uniemożliwiający odczytanie zapisanych na nich danych.
5) Kopie zapasowe przechowywane są w szafkach zamykanych na klucz.

§ 32. Sposób, miejsce i okres przechowywania wydruków elektronicznych nośników danych zawierających dane osobowe oraz kopii zapasowych:

1) Użytkownicy nie mogą wynosić z budynku Szkoły wydruków, nośników z danymi osobowymi bez zgody Administratora danych osobowych.
2) Wydruki archiwalne lub bieżące przechowywane mogą być wyłącznie w pomieszczeniach uniemożliwiających dostęp do nich osobom nieupoważnionym.
3) Kopie zapasowe na nośnikach optycznych i magnetycznych przechowywane są w szafce zamykanej na klucze, do którego ma dostęp wyłącznie Administrator danych osobowych.

4) Za bezpieczeństwo danych zapisanych w komputerze odpowiada użytkownik komputera.
5) Zbędne wydruki zawierające dane osobowe natychmiast po wykorzystaniu muszą zostać zniszczone w niszczarce dokumentów.
6) Przeznaczone do likwidacji elektroniczne i optyczne nośniki informacji, zawierające dane osobowe pozbawia się w sposób trwały zapisu tych danych, a w przypadku gdy nie jest to możliwe, niszczy lub uszkadza się w sposób trwale uniemożliwiający ich odczytanie.
7) Kopie zapasowe przechowuje się przez okres dwunastu miesięcy po okresie sporządzenia kopii.

§ 33. Sposób zabezpieczenia systemu informatycznego przed działaniem oprogramowania, którego celem jest uzyskanie dostępu do systemu informatycznego:

1) W celu przeciwdziałania zagrożeniom systemów informatycznych, oprócz odpowiedniego poziomu komplikacji haseł dostępu stosuje się ochronę antywirusową na stacjach roboczych komputerów wykorzystywanych do przetwarzania danych osobowych.
2) System antywirusowy zainstalowany jest w każdym komputerze.
3) Program antywirusowy jest uaktywniony przez cały czas pracy każdego komputera w systemie informatycznym.
4) Wszystkie pliki otrzymane z zewnątrz, jak również wysyłane na zewnątrz, podlegają automatycznemu sprawdzeniu przez system antywirusowy pod kątem występowania wirusów.
5) Do ochrony antywirusowej stosuje się najnowszą dostępną wersję programu antywirusowego.
6) W przypadku pojawienia się wirusa, użytkownik obowiązany jest zaprzestać wykonywania jakichkolwiek czynności w systemie i niezwłocznie powiadomić o tym administratora danych.
7) Niedozwolone jest otwieranie wiadomości poczty elektronicznej i załączników od „niezaufanych" nadawców.
8) Niedozwolone jest wyłączanie, blokowanie i odinstalowywanie programów antywirusowych.

§ 34. Procedury wykonywania przeglądów i konserwacji systemów oraz nośników służących do przetwarzania danych:

1) Wszelkie prace związane z naprawami i konserwacją systemu informatycznego przetwarzającego dane osobowe muszą uwzględniać wymagany poziom zabezpieczenia tych danych przed dostępem do nich osób nieupoważnionych.
2) Zmiana konfiguracji sprzętu komputerowego, na którym znajdują się dane osobowe lub zmiana jego lokalizacji, może być dokonana tylko za wiedzą i zgodą Administratora danych osobowych.
3) Prace serwisowe na terenie Szkoły prowadzone w zakresie przeglądów i konserwacji systemów informatycznych mogą być wykonywane wyłącznie przez pracowników Szkoły lub przez upoważnionych przedstawicieli wykonawców zewnętrznych znajdujących się w towarzystwie pracowników Szkoły.
4) Przed rozpoczęciem prac serwisowych przez osoby spoza Szkoły konieczne jest potwierdzenie tożsamości serwisantów.

5) Urządzenie, dyski lub inne elektroniczne nośniki informacji, zawierające dane osobowe przeznaczone do likwidacji bądź naprawy, pozbawia się wcześniej zapisu tych danych w sposób uniemożliwiający ich odzyskanie albo naprawia się je pod nadzorem osoby upoważnionej przez Administratora danych osobowych.

CZĘŚĆ VIII - POSTANOWIENIA KOŃCOWE

§ 35. Polityka bezpieczeństwa jest dokumentem wewnętrznym i nie może być udostępniania osobom i instytucjom postronnym w żadnej formie bez zgody IOD.

§ 36. Polityka będzie aktualizowana stosownie do potrzeb wynikłych z przeprowadzonych sprawdzeń lub audytów, oceny rocznej i zmian w przepisach prawa.

§ 37. Przypadki, nieuzasadnionego zaniechania obowiązków wynikających z niniejszego dokumentu mogą zostać potraktowane jako ciężkie naruszenie obowiązków pracowniczych i skutkować mogą odpowiedzialnością dyscyplinarną, przewidzianą w odrębnych przepisach.

§ 38. Naruszenie przepisów o ochronie danych osobowych jest zagrożone sankcjami karnymi, określonymi w art. 107 ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych oraz w art. 266-269 ustawy z dnia 6 czerwca 1997 r. Kodeks karny.

§ 39. W sprawach nieuregulowanych w niniejszej Polityce bezpieczeństwa mają zastosowanie przepisy RODO, ustawy z dnia 18 maja 2018 r. o ochronie danych osobowych oraz wydanych na jej podstawie aktów wykonawczych i innych aktów prawnych wymienionych na wstępie.

p.o. DYREKTOR SZKOŁY

mgr Agnieszka Słysz

.....

podpis Administratora Danych Osobowych