ZARZĄDZENIE NR 10/2018
DYREKTORA SZKOŁY PODSTAWOWEJ
im. K. MAKUSZYŃSKIEGO w WIECHLICACH
z dnia 10 maja 2018 r.
w sprawie wdrożenia Polityk Ochrony Danych

Na podstawie art. 68 ust. 1 pkt 1 Ustawy z dnia 14 grudnia 2016 roku – Prawo oświatowe (Dz. U. z 2017 r., poz. 59 ze zm.) w związku z Rozporządzeniem 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 (Dziennik Urzędowy UE - 4.5.2016 L 119/3) oraz Ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz. U. z 2018 r., poz.1000)

Zarządza się, co następuje:

§ 1.

Wprowadzam w życie w Szkole Podstawowej im. K. Makuszyńskiego w Wiechlicach zwanej dalej szkołą, Polityki Ochrony Danych Osobowych, która stanowi załącznik 1 do zarządzenia.

§ 2.

1. Zadania związane z prawidłowością przetwarzania danych osobowych w szkole realizują wszyscy nauczyciele i pracownicy, zatrudnieni w placówce, a za skuteczne funkcjonowanie Polityki Ochrony Danych odpowiedzialny jest dyrektor szkoły.

§ 3.

Zasady ochrony danych określone są w Regulaminie Ochrony Danych, który stanowi załącznik nr 2 do zarządzenia.

§ 4.

Zobowiązuję wszystkich pracowników do zapoznania się z przepisami ochrony danych, obowiązujących w Szkole Podstawowej im. K. Makuszyńskiego w Wiechlicach oraz złożenie pisemnego oświadczenia o zapoznaniu się z Regulaminem Ochrony Danych w terminie do 14 dni roboczych od dnia wprowadzenia Zarządzenia nr 10. Wzór oświadczenia stanowi załącznik nr 7 do Polityki Ochrony Danych Osobowych.

§ 5.

Funkcję Inspektora Ochrony Danych sprawuje Michał Tylawski. Dane do kontaktu: 511 432 140, tylawski.m@spwiechlice.pl.

§ 6.

Zarządzenie wchodzi w życie z dniem 25 maja 2018 roku i podlega ogłoszeniu w Księdze Zarządzeń.

DYREKTOR SZKOŁY
mgr [illegible] Hrodzińska
.....
/ dyrektor jednostki /

Wiechlice, 25.05.2018 r.

POWOŁANIE INSPEKTORA OCHRONY DANYCH

Administrator Dyrektor Szkoły Podstawowej im. K. Makuszyńskiego Cecylia Brodzińska na podstawie Art. 37 ust. 1 Rozporządzenia Ogólnego PE I RADY UE o ochronie danych osobowych (DZ. U. UE. L. z 2016 r. 119.1)

Powołuje:

Inspektora ochrony danych osobowych (IOD)

MICHAŁ TYLAWSKI ; tylawski.m@spwiechlice.pl

Zgodnie z art. 37 ust. 1 zadania Inspektora ds. ochrony danych osobowych to nadzór nad ochroną danych osobowych i zapewnienie zgodności przetwarzania z przepisami dotyczącymi ochrony danych osobowych, a w szczególności IOD:

- zachowuje w tajemnicy lub poufności szczegóły wykonywanych zadań,
- informuje administratora, podmiot przetwarzający oraz pracowników, którzy przetwarzają dane osobowe, o obowiązkach spoczywających na nich w związku z ochroną danych osobowych,
- prowadzi działania zwiększające świadomość, szkolenia personelu uczestniczącego w operacjach przetwarzania oraz powiązane z tym audyty,
- współpracuje z organem nadzorczym,
- udziela informacji osobom, których dane dotyczą informacji zgodnie z przysługującymi im prawami,
- pełni funkcję punktu kontaktowego dla organu nadzorczego w kwestiach związanych z przetwarzaniem danych (w tym z uprzednimi konsultacjami zgodnie z art. 36).

Powołanie jest ważne od chwili podpisania i obowiązuje bezterminowo, z możliwością odwołania.

DYREKTOR SZKOŁY
mgr Cecylia Brodzińska

OŚWIADCZENIE INSPEKTORA

Oświadczam, że:

- zapoznałem się z treścią i obowiązkami wynikającymi z niniejszego upoważnienia i przepisów rozporządzenia,
- będę wypełniał swoje zadania z należytym uwzględnieniem ryzyka związanego z operacjami przetwarzania, mając na uwadze charakter, zakres, kontekst i cele przetwarzania,
- posiadam odpowiednią wiedzę i doświadczenie do wykonywania powierzonej mi funkcji.

Inspektor ochrony danych osobowych

.....

Podpis

Administrator

DYREKTOR SZKOŁY

mgr Cecylia Brodzińska

.....

Podpis

Dokumentacja Ochrony Danych Osobowych w Szkole Podstawowej im. Kornela Makuszyńskiego w Wiechlicach

Spis treści:

Konsultował:

.....
Inspektor Ochrony Danych

Opracował:

DYREKTOR SZKOŁY
mgr Cecylia Brodzińska
.....
Administrator danych

Wdrożono Zarządzeniem Dyrektora Nr10/2018
Obowiązuje od 25 maja 2018 roku.

Załącznik nr 1 do Zarządzenia nr /2018
Dyrektora Szkoły Podstawowej
im. K. Makuszyńskiego w Wiechlicach
z dnia .2018 r.

Polityka Ochrony Danych Osobowych w Szkole Podstawowej im. Kornela Makuszyńskiego w Wiechlicach

I. Wstęp

Polityka Ochrony Danych Osobowych jest dokumentem opisującym zasady ochrony danych osobowych stosowane przez Administratora danych w Szkole Podstawowej im. K. Makuszyńskiego w Wiechlicach w celu spełnienia wymagań Rozporządzenia PE i RE 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych (RODO).

Polityka stanowi jeden ze środków organizacyjnych, mających na celu wykazanie, że przetwarzanie danych osobowych odbywa się zgodnie z powyższym Rozporządzeniem.

II. Inwentaryzacja danych

1. Dane osobowe wymagające ochrony administrator danych opracował w postaci papierowej, stanowiącej załącznik nr 1 do Polityki Ochrony Danych.

2. Wykaz obejmuje zbiory ze stwierdzonym potencjalnym ryzykiem naruszenia praw lub wolności osób fizycznych.

3. Każdy ze zbiorów jest opisany w sposób umożliwiający przeprowadzenie analizy ryzyka.

4. W szkole została opracowana Polityka Zarządzaniem ryzykiem w przetwarzaniu Danych Osobowych, określająca zasady szacowania skali ryzyka i prawdopodobieństwa jego wystąpienia.

5. Opis zbiorów obejmuje takie informacje, jak:
   1) nazwę zbioru;
   2) opis celów przetwarzania;
   3) charakter, zakres, kontekst, dokumentowane dane osobowe;
   4) odbiorcy;
   5) Funkcjonalny opis operacji przetwarzania;
   6) aktywa służące do przetwarzania danych osobowych (Informacje, Programy, systemy operacyjne, Infrastruktura IT, Infrastruktura, Pracownicy i współpracownicy, Outsourcing);
   7) Informacja o konieczności wpisu do rejestru czynności przetwarzania;
   8) Informacja o konieczności przeprowadzenia oceny skutków dla zbioru.

6. Administrator, w uzgodnieniu z Inspektorem Ochrony Danych, opracował karty zawierające analizę ryzyka dla poszczególnych operacji przetwarzania danych w zakresie aktywów biorących udział w przetwarzaniu danych.

III. Zapewnienie o przetwarzania danych osobowych zgodnie z prawem.

1. Administrator zapewnia, że:

   1) dane osobowe są przetwarzane legalnie na podstawie art. 6 i 9 RODO;

   2) zakres danych osobowych jest adekwatny do celów przetwarzania, z zachowaniem zasady minimalizacji danych;

   3) Administrator przechowuje dane osobowe przez konkretnie określony czas, z uwzględnieniem zasad określonych w Jednolity rzeczowym wykazie akt, zatwierdzonym przez Archiwum Państwowe w Zielonej Górze;

   4) wobec osób, których dane są przetwarzane wykonano obowiązek informacyjny (art. 12, 13, 14 RODO) wraz ze wskazaniem im: prawa dostępu do danych osobowych, sprostowania, usunięcia, ograniczenia przetwarzania, sprzeciwu, „bycia zapomnianym";

   5) osoby, których dane osobowe są przetwarzane zostały poinformowane o funkcji IOD i przekazano dane kontaktowe;

   6) zapewniono ochronę danych osobowych w przypadku powierzenia danych w postaci umów powierzenia z podmiotami przetwarzającymi (art. 28 RODO).

2. Potwierdzenie przetwarzania danych osobowych zgodnie z prawem znajduje się z załączniku 1 – Wykaz Zbiorów Danych Osobowych.

3. Wzory klauzul informacyjnych znajdują się z załączniku 2 – Klauzule Informacyjne.

IV. Upoważnienia

1. Administrator odpowiada za nadawanie / anulowanie upoważnień do przetwarzania danych w zbiorach papierowych i systemach informatycznych.

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

3. Upoważnienia nadawane są do zbiorów na wniosek przełożonych osób. Upoważnienia określają zakres operacji na danych.

4. Upoważnienia mogą być nadawane w formie poleceń, np. upoważnienia do przeprowadzenia kontroli, audytów, wykonania czynności służbowych, udokumentowanego polecenia administratora w postaci umowy powierzenia.

5. Administrator prowadzi ewidencję osób upoważnionych w celu sprawowania kontroli nad prawidłowym dostępem do danych osób upoważnionych załącznik 3 - Ewidencja osób upoważnionych.

V. Procedura analizy ryzyka i ocena skutków

1. Procedura opisuje sposób przeprowadzenia analizy ryzyka w celu zabezpieczenia danych osobowych adekwatnie do zidentyfikowanych zagrożeń.

2. Przyjęto, że analiza ryzyka przeprowadzana jest dla zbioru danych osobowych lub grupy zbiorów charakteryzujących się podobieństwem celów i sposobów przetwarzania / **odrębnie dla każdego zbioru.**

3. W przypadku konieczności przeprowadzenia oceny skutków (art. 35) wykonano następujących czynności:

   1) dokonano opisu planowanych operacji przetwarzania i celów przetwarzania – załącznik 1 – Wykaz zbiorów danych osobowych;

   2) określono zagrożenia we wszystkich aktywach biorących udział w procesie przetwarzania;

   3) dokonano oceny ryzyk, zgodnie z zasadami wskazanymi w Polityce Zarządzania Ryzykiem;

   4) sporządzono mapę ryzyk ze wskazaniem istotności ryzyka;

   5) zaplanowano środki techniczne, organizacyjne i informatyczne dla ryzyk przekraczających istotność powyżej 4.

VI. Instrukcja postepowania z incydentami

Procedura definiuje katalog podatności i incydentów zagrażających bezpieczeństwu danych osobowych oraz opisuje sposób reagowania na nie. Jej celem jest minimalizacja skutków wystąpienia incydentów bezpieczeństwa oraz ograniczenie ryzyka powstania zagrożeń i występowania incydentów w przyszłości.

1. Każda osoba upoważniona do przetwarzania danych osobowych zobowiązana jest do powiadamiania o stwierdzeniu podatności lub wystąpieniu incydentu bezpośredniego przełożonego lub Inspektora Ochrony Danych.

2. Do typowych podatności bezpieczeństwa danych osobowych 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 typowych incydentów bezpieczeństwa danych osobowych 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).

4. W przypadku stwierdzenia wystąpienia incydentu, Administrator lub IOD prowadzi postępowanie wyjaśniające w toku, którego:
   1) ustala zakres i przyczyny incydentu oraz jego ewentualne skutki;
   2) proponuje ewentualne działania dyscyplinarne;
   3) proponuje działa na rzecz przywrócenia działań organizacji po wystąpieniu incydentu;
   4) rekomenduje działania prewencyjne (zapobiegawcze) zmierzające do eliminacji podobnych incydentów w przyszłości lub zmniejszenia strat w momencie ich zaistnienia.

5. Administrator dokumentuje powyższe wszelkie naruszenia ochrony danych osobowych, w tym okoliczności naruszenia ochrony danych osobowych, jego skutki oraz podjęte działania zaradcze – załącznik 4 Formularz rejestracji incydentu.

6. Zabrania się świadomego lub nieumyślnego wywoływania incydentów przez osoby upoważnione do przetwarzania danych.

7. W przypadku naruszenia ochrony danych osobowych skutkującego ryzykiem naruszenia praw lub wolności osób fizycznych, administrator bez zbędnej zwłoki – w miarę możliwości, nie później niż w terminie 72 godzin po stwierdzeniu naruszenia – zgłasza je organowi nadzorczemu.

VII. Regulamin Ochrony Danych

Regulamin ma na celu zapewnienie wiedzy osobom przetwarzającym dane osobowe odnośnie bezpiecznych zasad przetwarzania – załącznik 5 - Regulamin Ochrony Danych Osobowych

Po zapoznaniu się z zasadami ochrony danych osobowych, osoby zobowiązane są do potwierdzenia znajomości tych zasad i deklaracji ich stosowania – załącznik 6 Oświadczenie poufności

VIII. Wykaz zabezpieczeń

1. Administrator prowadzi wykaz zabezpieczeń, które stosuje w celu ochrony danych osobowych – załącznik 7 Wykaz zabezpieczeń.

2. W wykazie wskazano stosowane zabezpieczenia proceduralne oraz zabezpieczenia jako środki techniczne, informatyczne i organizacyjne – załącznik 7 Wykaz zabezpieczeń.

3. Wykaz jest aktualizowany po każdej analizie ryzyka.

IX. Szkolenia

1. Każda osoba przed dopuszczeniem do pracy z danymi osobowymi winna być poddana przeszkoleniu i zapoznana z przepisami RODO.

2. Za przeprowadzenie szkolenia odpowiada Administrator danych.

3. Administrator dokonał szkolenia wszystkich pracowników szkoły w formie e- szkolenia.

4. Po przeszkoleniu z zasad ochrony danych osobowych, uczestnicy zobowiązani są do potwierdzenia znajomości tych zasad i deklaracji ich stosowania.

5. Zgodnie z art. 32 RODO, Administrator powinien regularnie testować, mierzyć i oceniać skuteczność środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania.

Wykaz zbiorów danych osobowych w Szkole Podstawowej im. K. Makuszyńskiego w Wiechlicach

Legenda: **A**- informacje,
B - programy operacyjne i oprogramowanie,
C - infrastruktura IT,
D - infrastruktura placówki,
E - pracownicy i podmioty współpracujące,
F - outsorcing

Lp.	Nazwa zbioru danych	Aktywa - środki i zasoby służące do przetwarzania danych		Podstawa przetwarzania	Rejestr czynności przetwarzania	Ocena skutków - tak/nie	Cel przetwarzania Rodzaj i zakres danych Odbiorcy	Opis operacji przetwarzania	Czas przechowywania
1.	Kandydaci do pracy	**A.**	Dane osobowe	Art. 6 ust.1 lit. a, c,	tak	nie	<u>Cel:</u> zatrudnienie, postępowanie rekrutacyjne dla pracowników samorządowych na stanowiska urzędnicze i kierownicze urzędnicze <u>Rodzaj danych:</u> Dane osobowe zgodnie z art. 22^1 § 1 Kp	1. Zbieranie ofert, 2. Utrwalanie, 3. Ujawnianie na BIP,	Wg kat. B2 - 2 lata
		B.	Windows 10, 7, 8, elektroniczna poczta,						
		C.	router Dasan , stacje robocze, laptopy, komputery w sekretariacie i gabinecie dyrektora, drukarka Toshiba, CCTV - kamery						
		D.	Pomieszczenie sekretariatu i specjalisty ds. kadr						
		E.	Referent, kadrowa, zastępca dyrektora, dyrektor, sekretarz, księgowość						
		F.	Nie dotyczy						

2.	Dane osobowe pracowników	A	Dane osobowe, dane do ZFŚS, dokumentacja BHP, rejestr godzin, rejestr zwolnień lekarskich	Art.6, ust 1, lit. a, c, zgodnie z Kp i KN	tak	tak – w wybranych czynnościach	Cel: realizacja umów o pracę i zadań wynikających ze stosunku pracy i świadczeń pracowniczych, Rodzaj danych: Dane osobowe zgodnie z art. 22^2 § 2 Kp, art. 22 ust. 11 ustawy o ZFŚS, Odbiorcy: ZUS, ubezpieczyciele, dostawcy świadczeń pracowniczych, SIO,	1. Zbieranie 2. Utrwalanie, 3. Przeglądanie 4. Przechowywanie, 5. Przekazywanie przez przesłanie, 6. Udostępnianie organom nadzorującemu i prowadzącemu, NIK, podmiotom kotrolującym	50 lat
		B	Windows 10, 7, 8, Płatnik, Arkusz Optivum, Vulcan, Księgowość Optivum Vulcan, SIO, serwer DELL, router Dasan, wewnętrzna sieć, drukarki, PC CCTV,						
		C.	Serwer DELL, router, stacje robocze, laptopy, komputery w sekretariacie i gabinecie dyrektora, księgowość, specjalista ds. kadr, stacje robocze, CCTV – kamery, systemy ppoż.						
		D.	Pomieszczenia działu księgowości, kadr, sekretariat, gabinet dyrektora, archiwum						
		E.	Pracownicy administracji, Komisja socjalna, komisja Zdrowotna dla Nauczycieli, składnica akt						
		F.	Poczta na np. interia.pl, niszczenie dokumentów						
3.	Uczniowie	A.	Dane osobowe uczniów i rodziców/opiekunów prawnych	Art.6, ust 1, lit. a, c,	tak	tak - w wybranych czynnościach	Cel: Realizacja zadań dydaktycznych, wychowawczych i opiekuńczych placówki oświatowej Rodzaj danych: Dane osobowe zgodnie z ustawą SIO i Ustawą – Prawo oświatowe (Dz. U. z 2017 r., poz. 59) – dane osobowe	1. Zbieranie 2. Utrwalanie, 3. Przeglądanie 4. Przechowywanie, 5. Przekazywanie przez przesłanie, 6. Udostępnianie organom nadzorującemu i	Zgodnie z JRWA – 20 lat
		B.	Microsoft Office, E-dziennik VULCAN, Arkusz						
		C.	router, stacje robocze w klasach, laptopy, komputery w sekretariacie i gabinecie dyrektora, drukarki, CCTV - kamery						
		D.	Pomieszczenia sekretariatu, gabinet dyrektora i zastępców, pokój nauczycielski, gabinet pedagoga, logopedy.						

		E.	Pracownice sekretariatu, dyrektor, pracownicy na stanowiskach pedagogicznych, składnica akt				zwykłe i podlegające szczególnemu przetwarzaniu „dane wrażliwe"	prowadzącemu,, podmiotom kotrolującym	
		F.	Dziennik elektroniczny, niszczenie dokumentów, SIO, HERMES						
4.	Kandydaci do szkoły	A.	Wnioski rekrutacyjne, świadectwa ukończenia poprzedniego etapu edukacyjnego/ zaświadczenie o gotowości do szkoły	Art.6, ust 1, lit. a, c,	tak	tak - w wybranych czynnościach	Cel: Rekrutacja do szkoły/przedszkola Rodzaj danych: Dane osobowe zgodnie z ustawą – Prawo oświatowe Rozdział 6, art. 131- 142 *(wpisać właściwy w zależności od rodzaju placówki)*	1. Zbieranie 2. Przeglądanie	B5 – 5 lat
		B.	Microsoft Office, Acrobat Reader						
		C.	router, stacje robocze, komputery w sekretariacie i gabinecie dyrektora, drukarki, CCTV - kamery						
		D.	Pomieszczenie sekretariatu -, sala posiedzenia Komisji Rekrutacyjnej, gabinet dyrektora, Archiwum						
		E.	Pracownice sekretariatu, członkowie komisji Rekrutacyjnej,						
		F.	Nie dotyczy						
5.	Dzieci podlegające obowiązkowi szkolnemu / obowiązkowi nauki	A.	Imienny wykaz dzieci podlegających obowiązkowi szkolnemu/ nauki zamieszkałych w obwodzie szkoły	Art.6, ust 1, lit. a, c,	Nie	nie	Cel: Przyjęcie dzieci z obwodu szkoły, Nadzór nad realizacją obowiązku szkolnego Rodzaj danych: Dane osobowe: imię i nazwisko, adres zamieszkania, data urodzenia,	1. Zbieranie, 2. Przeglądanie	B2 - 2 lata
		B.	Wersja papierowa						
		C.	Nie dotyczy						
		D.	Pomieszczenie sekretariatu , składnica akt						
		E.	Pracownice sekretariatu, dyrektor szkoły/przedszkola						

		F.	Nie dotyczy				imię ojca i matki,		
6.	Wykaz osób uprawnionych do odbioru dzieci z placówki	A.	Upoważnienie pisemne – wersja papierowa	Art.6, ust 1, lit. a, c,	nie	nie	Cel: Zapewnienie bezpieczeństwa dzieciom Rodzaj danych: Dane osobowe: imię i nazwisko, wizerunek do wglądu, w dokumencie ze zdjęciem Odbiorcy: brak	1. Zbieranie, 2. Przeglądanie	Bc- 1 rok
		B.	Nie dotyczy						
		C.	CCTV - kamery						
		D.	Pomieszczenie sekretariatu, pokój nauczycielski, teczki wychowawcy, archiwum						
		E.	Sekretariat, wychowawcy świetlicy, nauczyciele						
		F.	Nie dotyczy						
7.	Rejestr korespondencji wychodzącej i przychodzącej	A.	Dane osobowe	Art.6, ust 1, lit. f	nie	nie	Cel: zarządzanie korespondencją przychodzącą i wychodzącą Rodzaj danych: dane osobowe osób z którymi prowadzona jest korespondencja Odbiorcy: brak	1.Zbieranie, 2.Utrwalanie 3. Dopasowywanie lub łączenie 4.Wykorzystywanie, 5. Przekazywanie do właściwego adresata	2 lata
		B.	Księga korespondencji, Windows 10, Microsoft Office						
		C.	stacje robocze, komputery w sekretariacie, drukarka Toshiba						
		D.	Nie dotyczy						
		E.	Pracownicy sekretariatu						
		F.	Nie dotyczy						
8.	Rejestr skarg, wniosków i zażaleń	A.	Dane osobowe, longiny, hasła	Art.6, ust 1, lit. c	nie	nie	Cel: realizacja wnoszonych zażaleń, wniosków,	1. Rejestracja skarg, wniosków,	2 lata lub do zakończe
		B.	Windows 10, Microsoft Office						

		C.	Internet, stacje robocze, laptopy, firewall, skrzynka e-mail, e- PUAP				rozpatrywanie skarg Rodzaj danych: dane osobowe osób skarżących Odbiorcy: brak		nia rozpatrywania skargi
		D.	Pomieszczenia sekretariatu, UPS, kontrola dostępu						
		E.	Pracownicy sekretariatu						
		F.	Nie dotyczy						
9.	Wolontariusze, praktykanci	A.	Dane osobowe wolontariuszy/ praktykantów, umowy wolontariatu lub umowy z uczelniami	Art.6, ust 1, lit. e	nie	nie	Cel: realizacja praktyk studenckich. Realizacja akcji charytatywnych przez uczniów Rodzaj danych: dane osobowe osób wolontariuszy lub praktykantów Odbiorcy: ubezpieczyciel	1. Rejestracja wolontariuszy lub praktykantów, 2. Zarządzanie akcjami charytatywnymi	5 lat
		B.	Windows 10,						
		C.	Stacje robocze, internet, CCTV – kamery,						
		D.	Pracownicy sekretariatu, nauczyciele						
		E.	Wicedyrektor, pracownice sekretariatu						
		F.	Nie dotyczy						
10.	Zbiór ofert do przetargów	A.	Dane oferentów, polityka bezpieczeństwa informacji	Art.6, ust 1, lit. c	nie	nie	Cel: realizacja zamówień publicznych Rodzaj danych: dane oferentów Odbiorcy: komisja rewizyjna w UM/UG	1. Realizacja konkursu ofert 2. Ujawnianie zwycięzcy konkursu	6 lat
		B.	Nie dotyczy						
		C.	Nie dotyczy						
		D.	Dział administracyjny, kierownik gospodarczy						
		E.	kierownik gospodarczy						
		F.	Niszczenie dokumentów						
11.	Kontrahen	A.	Dane dostawców, umowy,	Art.6, ust	nie	nie	Cel: realizacja zamówienia	1. Utrwalanie,	6 lat

	ci (dostawcy, wykonawcy)	**B.**	Microsoft Office, Acrobat Reader, Vulcan Optivum, witryny www	1, lit. b			Rodzaj danych: dane osobowe dostawców towarów lub usług Odbiorcy: bank	2.Dopasowanie lub łączenie,	
		C.	Faktury						
		D.	kierownik gospodarczy, CCTV – kamery,						
		E.	Sekretariat, księgowość, gabinet dyrektora, gabinet kierownika gospodarczego						
		F.	Księgowość						
12.	Najemcy	**A.**	Dane osobowe wynajmujących, polityka bezpieczeństwa informacji,	Art.6, ust 1, lit. b	nie	nie	<u>Cel:</u> realizacja zawartych umów wynajmu, <u>Rodzaj danych:</u> dane osobowe osób wynajmujących, <u>Odbiorcy:</u> brak	1. Utrwalanie, 2.Dopasowanie lub łączenie,	20 lat
		B.	Nie dotyczy						
		C.	CCTV – kamery,						
		D.	Sekretariat, księgowość, CCTV - kamery						
		E.	sekretariat						
		F.	Księgowość, bank						
13.	Darczyńcy	**A.**	Wyciągi bankowe, protokół przyjęcia środków na stan placówki	Art.6, ust 1, lit. e	nie	nie	1. zbieranie danych darczyńców 2. foundrising 3. Utrzymywanie relacji z darczyńcami	1. zbieranie danych darczyńców 2. foundrising *(kwestowanie, gromadzenie funduszy)* 3. Utrzymywanie relacji z darczyńcami	10 lat
		B.	Program księgowy,						
		C.	Serwer DELL, router, stacje robocze, drukarka, CCTV - kamery						
		D.	Pomieszczenia biurowe,						
		E.	Księgowość, kierownik gospodarczy						
		F.	Usługa foundrisingu						

14.	Monitoring	A.	Dane wizerunkowe, dane głosowe, procedura odtworzeniowa	Art.6, ust 1, lit. f	nie	tak	Cel: zabezpieczenie obszaru działalności Rodzaj danych: dane osobowe odwiedzających szkołę Odbiorcy: Policja, Straż Miejska	1. Utrwalanie, 2. Wykorzystywanie w sytacjach związanych z naruszeniem bezpieczeństwa 3. Przekazywanie policji, 4. Przeglądanie	2 msc
		B.	rejestrator						
		C.	Serwer, wewnętrzna sieć, stacje robocze, kamery, okablowanie						
		D.	Pracownik administracji, sekretariat,						
		E.	Budynek szkoły, stanowiska monitorowania, UPS						
		F.	Dostawca usług serwisowych – wsparcie techniczne						

ZGODA NA UPOWSZECHNIANIE WIZERUNKU DZIECKA

Oświadczam, że wyrażam zgodę na umieszczanie zdjęć i materiałów filmowych zawierających wizerunek mojego dziecka zarejestrowanych podczas zajęć i uroczystości szkolnych zorganizowanych przez Szkołę Podstawową im. K. Makuszyńskiego w Wiechlicach oraz związanych z uczestnictwem w programach, projektach, zawodach, konkursach i innych uroczystościach. Ponadto wyrażam zgodę na umieszczanie i publikowanie prac wykonywanych przez moje dziecko na stronie internetowej szkoły, profilach internetowych zarządzanych przez szkołę (eTwninning, Facebook, Google dokumenty) oraz w mediach w celu informacji i promocji szkoły.

Dyrektor Szkoły Podstawowej im. K. Makuszyńskiego w Wiechlicach informuje, że:

Zgodnie z art. 13 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 *(4.5.2016 L 119/38 Dziennik Urzędowy Unii Europejskiej PL)*

1. Administratorem danych osobowych uczniów jest Szkoła Podstawowa im. K. Makuszyńskiego w Wiechlicach, ul. Brzozowa 17, 67-300 Szprotawa, reprezentowana przez Dyrektora Panią Cecylię Brodzińską tel: 68 376 75 53, mail: szkolawiechlice2@wp.pl

2. Kontakt z Inspektorem Ochrony Danych w Szkole Podstawowej im. K. Makuszyńskiego możliwy jest pod numerem tel. nr 511 432 140. lub adresem email: tylawski.m@spwiechlice.pl

3. Dane osobowe ucznia będą przetwarzane na podstawie art. 6 ust. 1 lit.,c ogólnego rozporządzenie j/w o ochronie danych w celu realizacji zadań w celu realizacji zadań ustawowych, określonych w Ustawie – Prawo oświatowe z dn. 14 grudnia 2016 r. (Dz. U. z 2017 r., poz. 59 oraz Ustawy o systemie oświaty z dnia 7 września 1991 r. (Dz. U. z 2017 r., poz. 2198) w celu realizacji statutowych zadań dydaktycznych, opiekuńczych i wychowawczych w placówce.

4. Dane osobowe ucznia przechowywane będą przez czas określony w Jednolitym Rzeczowym Wykazie Akt, zatwierdzonym przez Państwowe Archiwum w Zielonej Górze – 20 lat.

5. Posiada Pan/i / prawo do: żądania od administratora dostępu do danych osobowych, prawo do ich sprostowania, usunięcia lub ograniczenia przetwarzania.

6. Rodzicom/ uczniom/ słuchaczom przysługuje prawo wniesienia skargi do organu nadzorczego, tj. Prezesa Urzędu Ochrony Danych.

7. Podanie danych osobowych jest wymogiem ustawowym i jest obowiązkowe ze względu na przepisy prawa oświatowego j/w.

....

Podpis rodzica Podpis administratora

INFORMACJA DO RODZICÓW

Dyrektor Szkoły Podstawowej im. K. Makuszyńskiego w Wiechlicach informuje, że:

Zgodnie z art. 13 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 (*4.5.2016 L 119/38 Dziennik Urzędowy Unii Europejskiej PL)*

1. Administratorem Pani/Pana - rodzica słuchacza danych osobowych jest Szkoła Podstawowa im. K. Makuszyńskiego w Wiechlicach, ul. Brzozowa 17, 67-300 Szprotawa, reprezentowana przez Dyrektora Panią Cecylię Brodzińską tel: 68 376 75 53, mail: szkolawiechlice2@wp.pl

2. Kontakt z Inspektorem Ochrony Danych w Szkole Podstawowej im. K. Makuszyńskiego możliwy jest pod numerem tel. nr 511 432 140. lub adresem email: tylawski.m@spwiechlice.pl

3. Dane osobowe Pana/i będą przetwarzane na podstawie art. 6 ust. 1 lit.,c ogólnego rozporządzenie j/w o ochronie danych w celu realizacji zadań w celu realizacji zadań ustawowych, określonych w Ustawie – Prawo oświatowe z dn. 14 grudnia 2016 r. (Dz. U. z 2017 r., poz. 59 oraz Ustawy o systemie oświaty z dnia 7 września 1991 r. (Dz. U. z 2017 r., poz. 2198) w celu realizacji statutowych zadań dydaktycznych, opiekuńczych i wychowawczych w placówce.

4. Pana/Pani dane osobowe przechowywane będą przez okresy zakreślone w Jednolitym Rzeczowym Wykazie Akt, zatwierdzonym przez Państwowe Archiwum w Zielonej Górze.

5. Posiada Pan/i /posiadasz prawo do: żądania od administratora dostępu do danych osobowych, prawo do ich sprostowania, usunięcia lub ograniczenia przetwarzania.

6. Rodzicom/ uczniom/ słuchaczom przysługuje prawo wniesienia skargi do organu nadzorczego, tj. Prezesa Urzędu Ochrony Danych.

7. Podanie danych osobowych jest wymogiem ustawowym i jest obowiązkowe ze względu na przepisy prawa oświatowego j/w.

.....

Podpis administratora

INFORMACJA DLA PRACOWNIKÓW

Zgodnie z art. 13 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 (*4.5.2016 L 119/38 Dziennik Urzędowy Unii Europejskiej PL)*

Dyrektor szkoły Podstawowej im. K. Makuszyńskiego w Wiechlicach informuje , że:

1. Administratorem Pani/Pana danych osobowych jest Szkoła Podstawowa im. K. Makuszyńskiego w Wiechlicach, ul. Brzozowa 17, 67-300 Szprotawa, tel. 68 376 75 53, e-mail: szkolawiechlice2@wp.pl
2. Kontakt z Inspektorem Ochrony Danych w Szkole Podstawowej im. K. Makuszyńskiego w Wiechlicach możliwy jest pod numerem telefonu 511 43 21 40 lub adresem email tylawski.m@spwiechlice.pl
3. Pana/Pani dane osobowe będą przetwarzane na podstawie art. 6 ust. 1 lit. a, c ogólnego rozporządzenia j/w o ochronie danych osobowych oraz Kodeksu Pracy – Ustawa z dnia 26 czerwca 1974 r. (t.j. Dz. U. z 2018 r., poz. 108) w celu związanym z zatrudnieniem **oraz przyznawania świadczeń socjalnych z ZFSŚ**.
4. Odbiorcami Pani/Pana danych będą wyłącznie podmioty uprawnione do uzyskania danych osobowych na podstawie przepisów prawa lub przyznania świadczeń socjalnych, np. ZUS, firma ubezpieczeniowa, organ prowadzący i nadzorujący, SIO, PIP.
5. Pana/Pani dane osobowe będą przechowywane przez okres 50 lat.
6. Posiada Pan/Pani prawo do żądania od administratora dostępu do danych osobowych , prawo do ich sprostowania, usunięcia lub ograniczenia przetwarzania oraz prawo cofnięcia zgody.
7. Przysługuje Panu/Pani prawo wniesienia skargi do organu nadzorczego tj. Prezesa Urzędu Ochrony Danych.
8. Podanie danych osobowych jest wymogiem ustawowym i jest obowiązkowe ze względu na przepisy prawa pracy, a w pozostałym zakresie jest dobrowolne.

.....

Podpis administratora

Umowa powierzenia przetwarzania danych

zwana dalej „Umową",

zawarta w ....., dnia ..... r.

pomiędzy:

.....,

zwanym dalej „Administratorem"

a

.....,

zwaną dalej „Podmiotem przetwarzającym",

zwanymi łącznie „Stronami".

Mając na uwadze, iż Strony łączy Umowa z dnia ....., przedmiotem której jest ..... zwana dalej „Umową główną", w trakcie wykonywania której przetwarzane są dane osobowe, Strony zgodnie postanowiły, co następuje:

§ 1.

Przedmiot Umowy

1. Strony postanawiają, że w celu spełnienia obowiązków wynikających z art. 28 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. zwanego dalej „Rozporządzeniem", Administrator powierza Podmiotowi przetwarzającemu do dane osobowe w celu realizacji Umowy głównej.
2. Zakres przetwarzania obejmuje ..... danych osobowych w zbiorach Administratora: .....
3. Przetwarzane dane dotyczą .....
4. Przetwarzane dane obejmują: .....

§ 2.

Obowiązki i prawa administratora

1. Administrator powierzone Podmiotowi przetwarzającemu do przetwarzania dane osobowe gromadzi zgodnie z obowiązującymi przepisami prawa oraz jest uprawniony do powierzenia przetwarzania danych osobowych.
2. Administrator zobowiązany jest do przekazywania danych zachowując zasady bezpieczeństwa w celu zachowania poufności i integralności powierzanych danych.
3. Administrator zezwala / nie zezwala na korzystanie z usług innego podmiotu przetwarzającego.
4. Administrator ma możliwość wyrażenia sprzeciwu wobec dodania lub zastąpienia innych podmiotów przetwarzających.

5. Administrator ma prawo samodzielnie lub za pomocą upoważnionych przez siebie audytorów przeprowadzić audyty lub inspekcje, których celem jest weryfikacja realizacji obowiązków wynikających z zapisów Rozporządzenia.

§ 3.

Obowiązki Podmiotu przetwarzającego

1. Podmiot przetwarzający przy przetwarzaniu powierzonych danych osobowych zobowiązany jest stosować przepisy Rozporządzenia, w tym:
   a) stosować środki techniczne i organizacyjne zapewniające bezpieczeństwo powierzanym danym, w stopniu adekwatnym do ryzyka występujących zagrożeń,
   b) powinien zabezpieczyć dane przed ich udostępnieniem osobom nieupoważnionym, utratą, uszkodzeniem lub zniszczeniem,
   c) dopuszczać do przetwarzana danych wyłącznie osoby, które zobowiązały się do zachowania tajemnicy lub podlegają odpowiedniemu ustawowemu obowiązkowi zachowania tajemnicy.
2. Podmiot przetwarzający zobowiązuje się do przetwarzania danych osobowych wyłącznie na udokumentowane polecenie Administratora.
3. Podmiot przetwarzający zgłasza Administratorowi przypadki naruszeń ochrony danych osobowych.

§ 4.

Oświadczenie Podmiotu przetwarzającego

1. Zobowiązuję się do wykorzystania powierzonych danych osobowych wyłącznie w zakresie i celu niezbędnym do realizacji obowiązków wynikających z umowy współpracy.
2. W przypadku ogólnej pisemnej zgody na korzystanie z usług innego podmiotu przetwarzającego poinformuję Administratora o wszelkich zamierzonych zmianach dotyczących dodania lub zastąpienia innych podmiotów przetwarzających.
3. W miarę możliwości będę pomagać Administratorowi poprzez odpowiednie środki techniczne i organizacyjne wywiązać się z obowiązku odpowiadania na żądania osoby, której dane dotyczą, w zakresie wykonywania jej praw.
4. W przypadku audytów lub inspekcji przeprowadzonych lub zleconych przez Administratora udostępnię wszelkie niezbędne informacje z zachowaniem czujności, czy żądane informacje nie naruszą zapisów Rozporządzenia.

§ 5.

Czas trwania i wypowiedzenie Umowy

1. Każda ze Stron odpowiada za szkody wyrządzone drugiej Stronie oraz osobom trzecim w związku z wykonywaniem niniejszej Umowy, zgodnie z przepisami Rozporządzenia i Kodeksu cywilnego.

2. W celu uniknięcia wątpliwości, Podmiot przetwarzający ponosi odpowiedzialność za działania swoich pracowników i innych osób, przy pomocy których przetwarza powierzone dane osobowe, jak za własne działanie i zaniechanie.

§ 6.

Czas trwania i wypowiedzenie Umowy

1. Umowa zostaje zawarta na czas obowiązywania Umowy głównej. W celu uniknięcia wątpliwości, rozwiązanie Umowy głównej skutkuje rozwiązaniem niniejszej Umowy.
2. Strony postanawiają, iż po zakończeniu przetwarzania danych Podmiot powierzający zobowiązany jest do niezwłocznego usunięcia powierzonych mu danych (i wszelkich ich istniejących kopii) lub zwrotu Administratorowi – w zależności od jego decyzji, o ile nie następuje konieczność dalszego przetwarzania danych wynikająca z przepisów odrębnych.
3. Administrator jest uprawniony do rozwiązania Umowy bez wypowiedzenia, jeżeli Podmiot przetwarzający nie podjął środków zabezpieczających powierzone dane lub nie stosował się do wymogów przewidzianych w Rozporządzeniu.
4. Każdej ze Stron przysługuje prawo rozwiązania niniejszej Umowy w trybie natychmiastowym, w przypadku naruszenia postanowień niniejszej Umowy przez drugą Stronę Umowy.

§ 7.

Postanowienia końcowe

1. Z tytułu wykonywania świadczeń określonych w niniejszej Umowie Podmiotowi przetwarzającemu nie przysługuje dodatkowe wynagrodzenie ponad to, które zostało określone w Umowie głównej.
2. Umowa wchodzi w życie z dniem jej podpisania przez Strony.
3. W sprawach nieuregulowanych niniejszą Umową zastosowanie mają powszechnie obowiązujące przepisy prawa polskiego.
4. Wszelkie zmiany lub uzupełnienia niniejszej Umowy wymagają zachowania formy pisemnej pod rygorem nieważności.
5. Sądem właściwym dla rozstrzygania sporów powstałych w związku z realizacją niniejszej Umowy jest sąd właściwy dla siedziby Administratora.
6. Umowę sporządzono w dwóch jednobrzmiących egzemplarzach, po jednym dla każdej ze Stron.

Podpisy:

.....	.....
Administrator	Podmiot przetwarzający

Formularz rejestracji incydentów

L.p.	Data zdarzenia	Opis okoliczności incydentu / naruszenia	Liczba osób dotkniętych	Skutki naruszenia danych	Wdrożone działania zaradcze	Termin zakończenia działań	Odpowiedzialny za wdrożenie

Regulamin Ochrony Danych Osobowych W Szkole Podstawowej im. Kornela Makuszyńskiego w Wiechlicach

Spis treści:

Rozdział 1
Postanowienia ogólne

1. Regulamin stanowi wykaz podstawowych obowiązków z zakresu przestrzegania zasad ochrony danych osobowych w Szkole Podstawowej im. K. Makuszyńskiego w Wiechlicach, 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 Szkole Podstawowej im. K. Makuszyńskiego w Wiechlicach jest dyrektor szkoły.

5. Funkcje Inspektora Ochrony Danych sprawuje p. Michał Tylawski

Rozdział 2
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 W tej sytuacji 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 3
Zasady korzystania z poczty elektronicznej

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

2. W przypadku przesyłania danych osobowych poza szkołę należy wykorzystywać mechanizmy kryptograficzne (hasłowanie wysyłanych dokumentów lub plików spakowanych, podpis elektroniczny).

3. 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.

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

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

6. 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.

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

8. Wszystkie przypadki e-maili budzących podejrzenie należy zgłaszać administratorowi sieci/ informatykowi.

9. 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".

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

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

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

13. 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.

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

15. Użytkownik bez zgody Pracodawcy 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.

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

Rozdział 4
Regulamin użytkowania komputerów przenośnych

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

2. W przypadku przechowywania na komputerze przenośnym danych osobowych lub stanowiących tajemnicę Pracodawcy, 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 Pracodawcy.

4. W przypadku kradzieży lub zgubienia komputera przenośnego, Użytkownik powinien natychmiast powiadomić o tym osobę odpowiedzialną za ochronę danych tj. Administratora Danych lub IOD, 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 5
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 6
Zasady tworzenia kopii zapasowych

1. Zbiory danych osobowych w systemie informatycznych są zabezpieczane przed utratą lub uszkodzeniem za pomocą:

   1) urządzeń zabezpieczających przed awarią zasilania lub zakłóceniami w sieci zasilającej,
   2) sporządzania kopii zapasowych (kopie pełne).

2. Pełne kopie zapasowe zbiorów danych tworzone są 2 razy w ciągu roku. Kopie systemu kadrowo płacowego całościowe sporządzane są raz w miesiącu, a kopie przyrostowe raz dziennie.

3. W szczególnych sytuacjach, np. przed aktualizacją lub zmianą oprogramowania lub systemu należy wykonać bezwzględnie pełną kopię zapasową systemu.

4. Kopie zapasowe zbiorów danych należy okresowo sprawdzać pod kątem ich przydatności do odtworzenia w przypadku awarii systemu. Za przeprowadzenie tych czynności odpowiada informatyk.

5. Nośniki danych po ustaniu ich użyteczności należy pozbawić danych lub zniszczyć w sposób uniemożliwiający odczyt danych.

6. Kopie całościowe przechowywane są przez 5 lat a kopie przyrostowe przez 1 miesiąc.

Rozdział 7
Tworzenie kopii bezpieczeństwa dokumentacji serwera

1) Kopie zapasowe dokumentacji serwera tworzone są w sposób zautomatyzowany w oparciu o (specjalne oprogramowanie / wykorzystanie programowej funkcji serwera);

2) Kopie bezpieczeństwa sporządzane są także dla dokumentacji gromadzonej na dyskach stacji roboczych użytkowników w wybranym katalogu (np. w katalogu C:/Operacyjne/);

3) Kopie całościowe sporządzane są raz w miesiącu, a kopie przyrostowe raz dziennie;

4) Kopie sporządzane są na wydzielonym twardym dysku wymiennym, w pomieszczeniu składnicy akt;

5) Kopie całościowe przechowywane są przez okres 5 lat a kopie przyrostowe przez 1 miesiąc;

6) Kopie przechowywane są w sejfie w pomieszczeniu składnicy akt;

Rozdział 8
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 9
Procedura 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 10
Procedura 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 11
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 12
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.

DYREKTOR SZKOŁY
mgr Cecylia Brodzińska

Wiechlice, 25 maja 2018 roku .....

Załącznik nr 6 do Polityki Ochrony Danych Osobowych

.....
Imię i nazwisko

.....
Stanowisko

Wiechlice,.....

Oświadczenie o zachowaniu poufności i zapoznaniu się z przepisami

Ja niżej podpisany/a oświadczam, iż zobowiązuję się do zachowania w tajemnicy danych osobowych oraz sposobów ich zabezpieczenia, do których mam lub będę miał/a dostęp w związku z wykonaniem zadań i obowiązków służbowych wynikających ze stosunku pracy, zarówno w czasie trwania umowy, jak i po jej ustaniu.

Oświadczam, że zostałem/am poinformowany/a o obowiązującym w Szkole Podstawowej im. K. Makuszyńskiego w Wiechlicach zasadach dotyczących przetwarzania danych osobowych, określonych w Zarządzeniu nr 10/18 Dyrektora Szkoły Podstawowej im. K. Makuszyńskiego w Wiechlicach w sprawie wprowadzenia polityki bezpieczeństwa przetwarzania danych osobowych i instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Szkole Podstawowej im. K. Makuszyńskiego w Wiechlicach, i zobowiązuję się ich przestrzegać.
W szczególności oświadczam, że bez upoważnienia nie będę wykorzystywał/a danych osobowych ze zbiorów znajdujących się w szkole. Zostałem/am zapoznany/a z przepisami Ustawy o ochronie danych osobowych z 29 sierpnia 1997 r., Rozporządzeniem PE i RE 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych (RODO) oraz Rozporządzeniem MSWiA w sprawie dokumentacji przetwarzania danych osobowych warunków technicznych i organizacyjnych jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych.
Poinformowano mnie również o grożącej, stosownie do przepisów rozdziału 8 Ustawy o ochronie danych osobowych odpowiedzialności karnej. Niezależnie od odpowiedzialności przewidzianej w wymienionych w przepisach, mam świadomość, że złamanie zasad ochrony danych osobowych, obowiązujących w Szkole Podstawowej im. K. Makuszyńskiego w Wiechlicach może zostać uznane za ciężkie naruszenie podstawowych obowiązków pracowniczych i skutkować może odpowiedzialnością dyscyplinarną.

.....
(podpis pracownika)

Lokalizacja zbiorów oraz zabezpieczenia fizyczne w Szkole Podstawowej im. K. Makuszyńskiego w Wiechlicach

Legenda: **Dz** – dozór całodobowy, **Klim** – klimatyzacja **Gas** – gaśnice **S/ppoż** – sygnalizacja przeciwpożarowa
Kd – kontrola dostępu, **A** – alarm **CCTV** – kamery
Kr – kraty w oknach **Szaf/k** – szafa zamykana na klucz **S** – sejf
Drz/ k – drzwi zamykane na klucz **SO** – sejf ogniotrwały

Nr zbioru	Nazwa zbioru	Lokalizacja	Zabezpieczenia fizyczne
1.	Kandydaci do pracy	Sekretariat, składnica akt, dział kadr	CCTV, Gaśnica, szafa/drzwi zamykana na klucz, kontrola dostępu, kraty w oknach, sejf
2.	Dane osobowe pracowników	Sekretariat, składnica akt, dział kadrowo-płacowy, księgowość	CCTV, Gaśnica, szafa/drzwi zamykana na klucz, kontrola dostępu, kraty w oknach, alarm, sygnalizacja p/pożarowa , sejf

3.	Uczniowie	Sekretariat, składnica akt, pokój nauczycielski, gabinet pedagoga/psychologa/logopedy.	CCTV, Gaśnica, szafa/drzwi zamykana na klucz, kontrola dostępu, kraty w oknach, alarm, sygnalizacja p/pożarowa, sejf
4.	Kandydaci do szkoły	Sekretariat, składnica akt	CCTV, Gaśnica, szafa/drzwi zamykana na klucz, kontrola dostępu, sygnalizacja p/pożarowa
5.	Dzieci podlegające obowiązkowi	Sekretariat, składnica akt	CCTV, Gaśnica, szafa/drzwi zamykana na klucz, kontrola dostępu, sygnalizacja p/pożarowa
6.	Wykaz osób uprawnionych do odbioru dzieci z placówki	Sekretariat, pokój nauczycielski, szafki nauczycielskie	CCTV, Gaśnica, szafa/drzwi zamykana na klucz, kontrola dostępu, sygnalizacja p/pożarowa
7.	Rejestr korespondencji wychodzącej i przychodzącej	Sekretariat	CCTV, Gaśnica, szafa/drzwi zamykana na klucz, kontrola dostępu, sygnalizacja p/pożarowa
8.	Rejestr skarg, wniosków i zażaleń	Sekretariat	CCTV, Gaśnica, szafa/drzwi zamykana na klucz, kontrola dostępu, sygnalizacja p/pożarowa
9.	Wolontariusze, praktykanci	Sekretariat, składnica akt	CCTV, Gaśnica, szafa/drzwi zamykana na klucz, kontrola dostępu, sygnalizacja p/pożarowa, sejf

10.	Zbiór ofert do przetargów	Sekretariat, gabinet Kierownika gospodarczego	CCTV, Gaśnica, szafa/drzwi zamykana na klucz, kontrola dostępu, sygnalizacja p/pożarowa
11.	Kontrahenci (dostawcy, wykonawcy)	Sekretariat, księgowość, gabinet Kierownika gospodarczego	CCTV, Gaśnica, szafa/drzwi zamykana na klucz, kontrola dostępu, sygnalizacja p/pożarowa
12.	Najemcy	Sekretariat, księgowość gabinet Kierownika gospodarczego	CCTV, Gaśnica, szafa/drzwi zamykana na klucz, kontrola dostępu, sygnalizacja p/pożarowa
13.	Darczyńcy	Sekretariat, księgowość gabinet Kierownika gospodarczego	CCTV, Gaśnica, szafa/drzwi zamykana na klucz, kontrola dostępu, sygnalizacja p/pożarowa
14.	Monitoring	Sekretariat, gabinet pedagoga	Gaśnica, szafa/drzwi zamykana na klucz, kontrola dostępu, sygnalizacja p/pożarowa