ZATWIERDZAM

ADMINISTRATOR DANYCH OSOBOWYCH:

Szkoła Podstawowa nr 6 im. Jana Kochanowskiego w Zgierzu z Oddziałami Dwujęzycznymi i Oddziałami Sportowymi
Załącznik Nr 1 do Zarządzenia nr 10/2018

POLITYKA BEZPIECZEŃSTWA DANYCH OSOBOWYCH

SPIS TREŚCI :

§ 1 Terminologia……..3
§ 2 Deklaracja intencji……..4
§ 3 System ochrony danych osobowych……5
§ 4 Inspektor Ochrony Danych……..6
§ 5 Monitorowanie prawidłowości przetwarzania danych osobowych……7
§ 6 Minimalizacja……7
§ 7 Przetwarzanie z upoważnienia Administratora Danych……8
§ 8 Obsługa praw Podmiotu Danych……8
§ 9 Ochrona danych osobowych w fazie projektowania oraz domyślna ochrona danych……9
§ 10 Współadministratorzy Danych……10
§ 11 Podmioty Przetwarzające……10
§ 12 Rejestrowanie czynności przetwarzania……10
§ 13 Bezpieczeństwo danych osobowych……11
§ 14 Kodeks postępowania……14
§ 15 Procedura postępowania w przypadku kontroli Organu Nadzorczego……14
§ 16 Postanowienia końcowe……14

ZAŁĄCZNIKI :

Załącznik nr 1 - Wzór oświadczenia o zachowaniu w tajemnicy.
Załącznik nr 2 - Wzór upoważnienia do przetwarzania danych osobowych.
Załącznik nr 3 - Procedura nadawania i odbierania uprawnień do przetwarzania danych osobowych.
Załącznik nr 4 - Wzór ewidencji osób upoważnionych do przetwarzania danych osobowych.
Załącznik nr 5 - Wzór wniosku o nadanie uprawnień do przetwarzania danych osobowych.
Załącznik nr 6 - Klauzula informacyjna bezpośrednia.
Załącznik nr 7 - Klauzula informacyjna pośrednia.
Załącznik nr 8 - Procedura realizacji wniosku do obsługi żądań.
Załącznik nr 9 - Wzór wniosku do obsługi żądań.
Załącznik nr 10 - Wzór Rejestru Wniosków do obsługi żądań.
Załącznik nr 11 - Wzór umowy powierzenia.
Załącznik nr 12 - Procedura korzystania z mobilnego sprzętu służbowego.
Załącznik nr 13 - Procedura postępowania w przypadku wystąpienia incydentu bezpieczeństwa.
Załącznik nr 14 - Procedura tworzenia kopii zapasowych.
Załącznik nr 15 - Procedura uwierzytelniania użytkownika w systemach informatycznych.
Załącznik nr 16 - Procedura wykonywania przeglądów i konserwacji.
Załącznik nr 17 - Protokół zniszczenia nośnika z danymi osobowymi.
Załącznik nr 18 - Wzór rejestru udostępnień.
Załącznik nr 19 - Zasady pracy w systemie informatycznym.

§1
Terminologia

Występujące w niniejszym dokumencie zwroty oznaczają:

1. **Administrator Danych Osobowych lub Administrator** - podmiot, który w danym procesie przetwarzania danych decyduje o celach i sposobach przetwarzania.
2. **Dane** - dane osobowe, o ile nic innego nie wynika wyraźnie z kontekstu.
3. **Dane Niezidentyfikowane** - dane osób, których tożsamości Administrator nie zna (np. nagrania monitoringu wizyjnego) lub informacje, co do których Administrator nie wie, czy znajdują się w nich Dane, ale jest taka możliwość (np. zawartość serwera plików).
4. **Dane szczególnych kategorii** - dane wymienione w art. 9 RODO, tj. dane ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych, dane genetyczne, biometryczne przetwarzane w celu jednoznacznego zidentyfikowania osoby fizycznej lub dane dotyczące zdrowia, seksualności lub orientacji seksualnej.
5. **Eksport danych** - oznacza przekazanie danych do państwa trzeciego (czyli poza Unię Europejską, Norwegię, Lichtenstein, Islandię) (dalej EOG) lub do organizacji międzynarodowych.
6. **IOD lub Inspektor** - oznacza Inspektora Ochrony Danych.
7. **Unia** – Unia Europejska
8. **Organ Nadzorczy** - oznacza właściwy organ do wypełniania zadań i wykonywania uprawnień powierzonych mu zgodnie z RODO oraz przepisami krajowymi.
9. **Kontrola Zewnętrzna** - oznacza kontrolę prowadzoną przez podmiot zewnętrzny, a w szczególności przez Organ Nadzorczy.
10. **Osoba Przyjmująca** – Osoba, która jako pierwsza ma kontakt z przedstawicielami organu nadzorczego ds. ochrony danych osobowych
11. **Kontroler** – Osoba uprawniona przez organ nadzorczy ds. ochrony danych osobowych, do przeprowadzenia kontroli zgodności przetwarzania danych osobowych z RODO.
12. **Podmiot Danych** - oznacza osobę, której Dane dotyczą, o ile co innego nie wynika wyraźnie z kontekstu.
13. **Polityka** - niniejszy dokument, o ile nic innego nie wynika wyraźnie z kontekstu.
14. **Pracownik** - oznacza osobę, z którą został nawiązany stosunek pracy w rozumieniu art. 22 K.P., oraz osoby zatrudnione na podstawie umowy cywilno-prawnej oraz na podstawie samozatrudnienia.
15. **Profilowanie** - dowolna forma 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, wiarygodności, zachowania, lokalizacji lub przemieszczania się.
16. **Osoba Trzecia** - pracownik firmy zewnętrznej realizujący określone zadania na rzecz Administratora.
17. **Podmiot Przetwarzający lub Przetwarzający**- oznacza organizację lub osobę, której Administrator powierzył przetwarzanie Danych (np. usługodawca IT, usługodawca w zakresie księgowości).
18. **RCPD lub Rejestr** - oznacza Rejestr Czynności Przetwarzania Danych.
19. **RODO**- oznacza Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 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).
20. **Sprawdzenie** - cykliczne sprawdzenie stanu zgodności przetwarzania Danych przez IOD lub osoby do tego wyznaczone.

21. **Uprawnienia**- prawa przysługujące Osobie określone w art. 15-20 RODO tj, prawo dostępu do Danych, prawo do sprostowania Danych, prawo do usunięcia Danych, prawo do ograniczenia przetwarzania, prawo do bycia poinformowanym o sprostowaniu, usunięciu, lub ograniczeniu przetwarzania Danych, prawo do przenoszenia Danych.
22. **IT** - (ang. information technology) – całokształt zagadnień, metod, środków i działań związanych z przetwarzaniem informacji. Stanowi połączenie zastosowań informatyki i telekomunikacji, obejmuje również sprzęt komputerowy oraz oprogramowanie, a także narzędzia i inne technologie związane ze zbieraniem, przetwarzaniem, przesyłaniem, przechowywaniem, zabezpieczaniem i prezentowaniem informacji. Dostarczają one użytkownikowi narzędzia, za pomocą których może on pozyskiwać informacje, selekcjonować je, analizować, przetwarzać, gromadzić, zarządzać i przekazywać innym ludziom.
23. **Komórka Organizacyjna** – zespół powołany do wykonywania określonych części zadań w jednostce organizacyjnej, mająca ustalone miejsce w strukturze organizacyjnej Administratora Danych.

§2
Deklaracja Intencji

1. Niniejszy dokument oddaje intencje Administratora Danych Osobowych w zakresie pełnego zabezpieczenia prywatności osób, których dane osobowe przetwarza.
2. Administrator zapewnia, że prowadzi przetwarzane zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osoby, której dane dotyczą. Zbiera je w konkretnych, wyraźnych i prawnie uzasadnionych celach i nie przetwarza ich dalej w sposób niezgodny z tymi celami. Administrator oświadcza, że przetwarzane przez niego dane są adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane oraz prawidłowe i w razie potrzeby uaktualniane. Uzyskane dane przechowywane są w formie umożliwiającej identyfikację osoby, której dane dotyczą, przez okres nie dłuższy, niż jest to niezbędne do celów, w których dane te są przetwarzane.
3. Następujące zasady stanowią filary ochrony Danych w Szkole Podstawowej nr 6 im. Jana Kochanowskiego w Zgierzu z Oddziałami Dwujęzycznymi i Oddziałami Sportowymi:
   a. przetwarzanie Danych zgodnie z prawem (Legalność).
   b. zapewnienie odpowiedniego poziomu bezpieczeństwa Danych podejmując stale działania w tym zakresie (Bezpieczeństwo).
   c. umożliwienie osobom, których Dane przetwarza, wykonywanie swoich praw i prawa te realizuje (Prawa Jednostki).
   d. dokumentowanie tego, w jaki sposób spełnia obowiązki, aby w każdej chwili móc wykazać zgodność z zasadami ochrony Danych (Rozliczalność).
4. Szkoła Podstawowa nr 6 im. Jana Kochanowskiego w Zgierzu z Oddziałami Dwujęzycznymi i Oddziałami Sportowymi przetwarza Dane z poszanowaniem następujących zasad:
   a. w oparciu o podstawę prawną i zgodnie z prawem (legalizm)
   b. rzetelnie i uczciwie (rzetelność)
   c. w sposób przejrzysty dla Osoby (transparentność)
   d. w konkretnych celach i nie „na zapas” (minimalizacja)
   e. nie więcej niż potrzeba (adekwatność)
   f. z dbałością o prawidłowość Danych (prawidłowość)
   g. nie dłużej niż potrzeba (czasowość)
   h. zapewniając odpowiednie bezpieczeństwo Danych (bezpieczeństwo)
5. Szkoła Podstawowa nr 6 im. Jana Kochanowskiego w Zgierzu z Oddziałami Dwujęzycznymi i Oddziałami Sportowymi zapewnia odpowiedni poziom bezpieczeństwa Danych, w tym:
   a. przeprowadza analizy ryzyka przetwarzania Danych

b. przeprowadza oceny skutków dla ochrony Danych tam, gdzie ryzyko naruszenia praw i wolności Osób jest wysokie
c. dostosowuje środki ochrony Danych do ustalonego ryzyka
d. stosuje procedury pozwalające na identyfikację, ocenę i zgłoszenie zidentyfikowanego naruszenia ochrony Danych Organowi Nadzorczemu - zarządza incydentami
e. stosuje procedury pozwalające na ustalenie konieczności zawiadomienia Osób dotkniętych zidentyfikowanym naruszeniem ochrony Danych

6. Szkoła Podstawowa nr 6 im. Jana Kochanowskiego w Zgierzu z Oddziałami Dwujęzycznymi i Oddziałami Sportowymi przeprowadza ocenę skutków dla ochrony Danych (DPIA), o której mowa w art. 35 RODO, jeżeli przetwarza Dane Szczególnych Kategorii na dużą skalę.

§3
System ochrony danych osobowych

System ochrony danych osobowych zawarty w Polityce opiera się na aktywnym udziale wszystkich pracowników w systemie, w stopniu odzwierciedlającym ich odpowiedzialności i uprawnienia zarządcze określone w regulacjach wewnętrznych, a w szczególności:

1. Administrator danych odpowiada za:
    a. wdrożenie i utrzymanie zgodnego z RODO systemu ochrony danych osobowych w jednostce organizacyjnej oraz za podejmowanie decyzji o celach i środkach przetwarzania danych,
    b. Wdrożenie oraz stosowanie niniejszej Polityki,
    c. Zabezpieczenie zasobów IT przeznaczonych do przetwarzania Danych zgodnie z RODO,
    d. Zapewnienia bezpieczeństwa przetwarzania Danych w urządzeniach i systemach informatycznych,
2. IOD realizuje swoje kompetencje zgodnie z zadaniami opisanymi w § 4, również przy pomocy Zastępcy IOD lub Zespołu IOD.
3. Kierownik Komórki Organizacyjnej odpowiedzialny jest za:
    a. Stosowanie niniejszej Polityki,
    b. Nadzór nad zapoznaniem się przez Pracowników, stosowaniem i przestrzeganiem Polityki,
    c. Występowanie do IOD z wnioskiem o zgłaszanie zmian do Rejestru,
    d. Zapewnienie prawidłowej i efektywnej realizacji zadań nałożonych na IOD,
    e. Opiniowanie wniosków o nadanie, zmianę, utratę upoważnienia do przetwarzania Danych,
    f. Uzgadnianie z IOD treści odpowiedzi na wnioski o udostępnienie Danych kierowane przez osoby, których dane dotyczą,
    g. Wykonywanie zaleceń IOD w celu zapewnienia prawidłowego przetwarzania Danych
4. Podmiot zewnętrzny odpowiedzialny za obszar teleinformatyki odpowiedzialny jest za:
    a. Informowanie Administratora oraz IOD, w przypadku stwierdzenia:
        i. incydentu bądź naruszenia bezpieczeństwa Danych przetwarzanych z użyciem zasobów IT
        ii. zdarzeń mogących świadczyć o wystąpieniu incydentu dotyczącego Danych
        iii. nieprawidłowości w funkcjonowaniu zasobów IT przeznaczonych do przetwarzania Danych
    b. Realizację wniosków dotyczących uprawnień w dostępie do Danych i zasobów IT
    c. Zapewnienie Administratorowi dostępności do Danych przez utrzymywanie kopii awaryjnych baz Danych i systemów służących do przetwarzania Danych

   d. Dokonywanie czynności zabezpieczających, sprawdzeń i ustaleń dotyczących okoliczności i przyczyn incydentu bądź naruszenia ochrony Danych na wniosek IOD
   e. Bezzwłoczne odebranie bądź zablokowanie użytkownikowi dostępu do systemu przetwarzającego Dane na wniosek Administratora, IOD lub Kierownika Komórki Organizacyjnej
   f. Współpracę z IOD
5. Wszyscy Pracownicy odpowiedzialni są za:
   a. Ochronę Danych, zgodnie z postanowieniami RODO
   b. Przetwarzanie Danych w zakresie ustalonym nadanym upoważnieniem,
   c. Zachowanie w tajemnicy Danych i sposobów ich zabezpieczenia w okresie zatrudnienia, jak również po ustaniu zatrudnienia
   d. Zgłaszanie do przełożonego i IOD wszystkich przypadków wystąpień kierowanych do jednostki dotyczących wypełnienia obowiązku informacyjnego wynikającego z RODO
   e. Zgłaszanie do przełożonego i IOD wszystkich przypadków wystąpień kierowanych do jednostki dotyczących udostępnienia danych osobowych.
   f. Zgłaszanie do przełożonego i IOD przypadków incydentów i naruszeń zasad ochrony Danych
   g. Uczestnictwo w szkoleniach w zakresie ochrony Danych
   h. Stosowanie się do zaleceń przełożonego i IOD w zakresie ochrony Danych
   i. Składanie wyjaśnień IOD w sprawach dotyczących przetwarzania i ochrony Danych

§4
Inspektor Ochrony Danych

1. Status Inspektora Ochrony Danych
   a. Posiada niezależność organizacyjną,
   b. Podlega bezpośrednio Najwyższemu Kierownictwu Administratora,
   c. Jest niezwłocznie włączany przez Administratora Danych we wszystkie sprawy dotyczące ochrony danych osobowych,
   d. Jest niezależny w realizacji swoich zadań,
   e. Nie może być karany ani odwołany przez administratora lub przetwarzającego dane za wypełnianie swoich zadań,
2. Inspektor ochrony danych ma następujące zadania:
   a. informowanie administratora, podmiotu przetwarzającego oraz pracowników, którzy przetwarzają dane osobowe, o obowiązkach spoczywających na nich na mocy RODO oraz innych przepisów Unii lub państw członkowskich o ochronie danych i doradzanie im w tej sprawie;
   b. monitorowanie przestrzegania RODO, innych przepisów Unii oraz przepisów krajowych o ochronie danych oraz polityk Administratora w dziedzinie ochrony danych osobowych, w tym podział obowiązków,
   c. prowadzenie szkoleń personelu uczestniczącego w operacjach przetwarzania oraz powiązane z tym audyty;
   d. udzielanie na żądanie zaleceń co do oceny skutków dla ochrony danych oraz monitorowanie jej wykonania zgodnie z art. 35;
   e. współpraca z organem nadzorczym;
   f. pełnienie funkcji punktu kontaktowego dla organu nadzorczego w kwestiach związanych z przetwarzaniem, w tym z uprzednimi konsultacjami, o których mowa w art. 36, oraz w stosownych przypadkach prowadzenie konsultacji we wszelkich innych sprawach.

g. inspektor ochrony danych wypełnia swoje zadania z należytym uwzględnieniem ryzyka związanego z operacjami przetwarzania, mając na uwadze charakter, zakres, kontekst i cele przetwarzania.

3. Zastępcy Inspektora Danych – jeżeli zostali wyznaczeni realizują zadania IOD w czasie jego nieobecności.

§5
Monitorowanie prawidłowości przetwarzania danych osobowych

1. Administrator danych prowadzi bieżący monitoring aktywności Organu Nadzorczego w zakresie informacji dotyczących aktualnych wymagań prawych. Monitoring wymagań prawnych obejmuje w szczególności:
    a. opublikowane oraz wchodzące w życie akty prawa powszechnie obowiązującego
    b. wytyczne oraz zalecenia Organu Nadzorczego
    c. wiążące wytyczne innych organów (np. Komisja Europejska, Europejska Rada Ochrony Danych);
    d. kodeksy branżowe
    e. wytyczne do certyfikacji
    f. udokumentowane dobre praktyki stosowania prawa
    g. istotne orzecznictwo sądów i trybunałów.
2. W razie stwierdzenia zmian dotyczących uregulowań prawnych mogących wpływać na obszar przetwarzania Danych Administrator Danych odpowiada za zapewnienie zgodności obowiązującego systemu ochrony danych osobowych z tymi zmianami.

§6
Minimalizacja

1. Szkoła Podstawowa nr 6 im. Jana Kochanowskiego w Zgierzu z Oddziałami Dwujęzycznymi i Oddziałami Sportowymi dba o minimalizację przetwarzania Danych pod kątem: adekwatności Danych do celów (ilości Danych i zakresu przetwarzania – minimalizacja zakresu), dostępu do Danych – minimalizacja dostępu, czasu przechowywania Danych – minimalizacja czasu.
2. W zakresie minimalizacji Administrator Danych:
    a. w ramach procesu utworzenia Rejestru Administrator weryfikuje zakres pozyskiwanych Danych, zakres ich przetwarzania i ilość przetwarzanych Danych pod kątem adekwatności do celów przetwarzania w ramach wdrożenia RODO.
    b. dokonuje okresowego przeglądu ilości przetwarzanych Danych i zakresu ich przetwarzania.
    c. przetwarza Dane jedynie niezbędne do osiągnięcia celu przetwarzania.
    d. Rozpoczynając nową czynność przetwarzania, określa zakres Danych niezbędnych do realizacji tej czynności. Do każdej czynności przetwarzania Kierownik Komórki Organizacyjnej odpowiedzialnej za czynność przetwarzania przyporządkowuje niezbędne kategorie Danych.
    e. Przed rozpoczęciem przetwarzania, Kierownik Komórki Organizacyjnej składa wniosek do IOD o wpisanie nowej czynności przetwarzania do Rejestru.
    f. IOD weryfikuje wniosek pod względem zgodności czynności z przepisami prawa oraz z zasadą adekwatności zakresu przetwarzanych Danych. IOD może wystąpić do Kierownika Komórki Organizacyjnej wnioskującego o wpisanie nowej czynności do Rejestru o uzasadnienie zakresu przetwarzania Danych w procesie.
3. W zakresie minimalizacji dostępu Administrator Danych:

a. stosuje ograniczenia dostępu do Danych: prawne (zobowiązania do poufności, zakresy upoważnień), organizacyjne (np. zasada czystego biurka), fizyczne (strefy dostępu, zamykanie pomieszczeń) i logiczne (firewall).
b. stosuje kontrolę dostępu fizycznego do pomieszczeń i urządzeń, w których przetwarzane są Dane.
c. dokonuje aktualizacji uprawnień dostępowych przy zmianach w składzie Pracowników i Osób Trzecich i zmianach ról Pracowników i Osób Trzecich, oraz zmianach Przetwarzających.

4. W zakresie minimalizacji czasu Administrator Danych:
   a. stosuje niniejsze zasady kontroli cyklu życia Danych, w tym weryfikacji dalszej przydatności Danych względem terminów wskazanych w Rejestrze.
   b. Przy stosowaniu niniejszych zasad kontroli cyklu życia Danych, uwzględnia ustalone w Rejestrze okresy przechowywania Danych.
   c. Poprzez Kierownika Komórki Organizacyjnej dokonuje okresowego przeglądu posiadanych Danych pod kątem czasu ich przechowywania, w terminach i uzgodnionych przez niego z IOD. Po dokonaniu weryfikacji, Kierownik Komórki Organizacyjnej informuje o wynikach weryfikacji IOD.

§ 7
Przetwarzanie z upoważnienia Administratora Danych

1. Dostęp do danych osobowych posiadają jedynie upoważnieni przez Administratora Danych pracownicy.
2. Każdy upoważniony pracownik przetwarza dane osobowe wyłącznie w zakresie wynikającym z obowiązków i poleceń służbowych.
3. Dokumentem potwierdzającym nadanie uprawnień jest upoważnienie do przetwarzania danych osobowych podpisane przez Administratora Danych. Wzór upoważnienia stanowi załącznik nr 2 do niniejszej Polityki.
4. W przypadku, gdy przetwarzanie danych wymaga działań w systemach informatycznych, upoważnienie zawiera identyfikator użytkownika i rodzaje uprawnień w tych systemach.
5. Procedurę nadawania i odbierania uprawnień (w tym do systemów informatycznych służących do przetwarzania danych osobowych) opisano w załączniku nr 3 do niniejszej Polityki.

§8
Obsługa praw Podmiotu Danych

1. Komunikacja z Podmiotem Danych:
   a. Administrator Danych komunikuje się w formie pisemnej (tradycyjnej lub elektronicznej), na adres wskazany przez Podmiot Danych. Formę ustną stosuje się na wyraźne żądanie Podmiotu Danych, potwierdzone stosowną notatką służbową.
   b. Każda forma komunikacji z Podmiotem Danych jest dokumentowana:
      i. Dla formy pisemnej tradycyjnej, archiwizuje się komunikat w formie pisemnej lub jego skan na serwerze firmowym.
      ii. Dla formy pisemnej elektronicznej, archiwizuje się komunikat w formie elektronicznej na serwerze firmowym.
      iii. Dla formy ustnej, notatkę z przekazania komunikatu archiwizuje się w formie pisemnej lub elektronicznej z oznaczeniem daty przekazania komunikatu oraz sposobu potwierdzenia tożsamości Podmiotu Danych.
2. Obowiązek informacyjny względem Podmiotu Danych:
   a. Administrator Danych realizuje obowiązek informacyjny względem Podmiotu Danych w formie pisemnej (tradycyjnej lub elektronicznej).

   b. Podczas zbierania danych osobowych bezpośrednio od Podmiotu Danych zakres klauzuli informacyjnej zgodny jest z załącznikiem nr 6 do niniejszej Polityki.
   c. Podczas pozyskiwania danych osobowych z innego niż Podmiot Danych źródła zakres klauzuli informacyjnej zgodny jest z załącznikiem nr 7 do niniejszej Polityki.
   d. W przypadku wystąpienia incydentu związanego z ochroną danych osobowych, który mógł powodować wysokie ryzyko naruszenia praw lub wolności Podmiotu Danych, Administrator Danych w miarę możliwości i bez zbędnej zwłoki zawiadamia Podmiot Danych, o takim naruszeniu.
3. Obsługa żądań Podmiotu Danych w związku z przysługującymi mu prawami:
   a. Wszelkie żądania Podmiotu Danych odnośnie przysługujących mu praw realizowane są na podstawie pisemnego wniosku złożonego w siedzibie Administratora Danych celem potwierdzenia tożsamości Podmiotu Danych.
   b. Wzór wniosku dla obsługi żądań Podmiotu Danych stanowi załącznik nr 9 do niniejszej Polityki.
   c. Procedura realizacji wniosku dla obsługi żądań Podmiotu Danych stanowi załącznik nr 8 do niniejszej Polityki.
   d. Odpowiedź na żądanie przekazuje się Podmiotowi Danych niezwłocznie po ich otrzymaniu, nie później niż w ciągu 1 miesiąca od ich otrzymania przez Administratora Danych.
   e. W razie potrzeby termin wskazany w ust.3 lit d. może zostać wydłużony o kolejne dwa miesiące z uwagi na skomplikowany charakter żądania lub liczbę żądań. W terminie miesiąca od otrzymania żądania Administrator Danych informuje Podmiot Danych o takim przedłużeniu terminu, z podaniem przyczyn opóźnienia.
4. Podmiot danych ma prawo do:
   a. sprostowania swoich danych osobowych;
   b. usunięcia swoich danych osobowych;
   c. ograniczenia przetwarzania swoich danych osobowych;
   d. przenoszenia swoich danych osobowych;
   e. sprzeciwu wobec przetwarzania dotyczących go danych osobowych
5. W przypadku realizacji uprawnienia Podmiotu Danych opisanego w ust. 4 lit a,b,c, Administrator Danych informuje o tym fakcie każdego odbiorcę, któremu ujawniono dane osobowe, chyba że okaże się to niemożliwe lub będzie wymagać niewspółmiernie dużego wysiłku. Na żądanie Podmiotu Danych Administrator Danych informuje go o tych odbiorcach.
6. Administrator Danych w procesie przetwarzania danych osobowych nie stosuje zautomatyzowanego podejmowania decyzji w indywidualnych przypadkach oraz profilowania.

§9
Ochrona danych osobowych w fazie projektowania oraz domyślna ochrona danych.

1. Administrator Danych, uwzględniając stan wiedzy technicznej, koszt oraz charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności Podmiotów Danych, wdraża odpowiednie środki techniczne w celu skutecznej realizacji zasad ochrony danych już w fazie projektowania procesu przetwarzania.
2. W celu oceny czy dany (planowany) proces wiąże się z przetwarzaniem danych osobowych, Administrator danych konsultuje z IOD wszystkie nowe inicjatywy mające związek z przyszłą działalnością już w fazie ich projektowania.
3. Jeżeli przyszła działalność ma związek z przetwarzaniem danych osobowych IOD wykonuje swoje zadania zgodnie z zapisami §4 niniejszej Polityki.

4. Administrator Danych, w konsultacji z IOD, wdraża odpowiednie środki techniczne i organizacyjne, aby domyślnie przetwarzane były wyłącznie te dane osobowe, które są niezbędne dla osiągnięcia każdego konkretnego celu przetwarzania.

§10
Współadministratorzy Danych

Administrator Danych nie współpracuje z innymi administratorami danych przy ustalaniu celów i sposobów przetwarzania danych osobowych.

§11
Podmioty Przetwarzające

1. Administrator Danych korzysta wyłącznie z usług takich Podmiotów Przetwarzających, które zapewniają gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie spełniało wymogi RODO i chroniło prawa Podmiotu Danych. Weryfikacja Podmiotów Przetwarzających odbywa się za pomocą referencji, certyfikatów, opisu kompetencji lub innych dostępnych środków.
2. Przetwarzanie przez Podmiot Przetwarzający odbywa się na podstawie umowy, której wzór stanowi załącznik nr 11 do niniejszej Polityki.
3. Zapisy umowy (o której mowa w ust. 2) zapewniają, że Podmiot Przetwarzający nie korzysta z usług innego Podmiotu Przetwarzającego bez uprzedniej pisemnej zgody Administratora Danych.

§12
Rejestrowanie czynności przetwarzania

1. Zgodnie z art. 30 RODO Szkoła Podstawowa nr 6 im. Jana Kochanowskiego w Zgierzu z Oddziałami Dwujęzycznymi i Oddziałami Sportowymi prowadzi RCPD, który stanowi formę dokumentowania czynności przetwarzania danych.
2. W Rejestrze, zgodnie z art. 30 RODO, dla każdej czynności przetwarzania danych, odnotowuje się co najmniej:
    a. cel przetwarzania,
    b. opis kategorii osób,
    c. opis kategorii danych,
    d. opis kategorii odbiorców danych,
    e. przewidywane terminy usunięcia poszczególnych kategorii danych
    f. ogólny opis technicznych i organizacyjnych środków ochrony danych.
3. Rejestr zawiera także dodatkowe informacje ułatwiające Administratorowi Danych zarządzanie zgodnością z zasadami przetwarzania i ochrony danych osobowych oraz rozliczenie się z nich.
4. Rejestr prowadzony jest w formie elektronicznej.
5. Rejestr prowadzony jest przez IOD, który jest zobowiązany do aktualizowania Rejestru. IOD dokonuje zmian w Rejestrze na wiosek Administratora Danych.
6. IOD udostępnia RCPD na żądanie Organu Nadzorczego. Organ Nadzorczy w przypadku prowadzenia Kontroli Zewnętrznej w siedzibie Szkoły Podstawowej nr 6 im. Jana Kochanowskiego w Zgierzu z Oddziałami Dwujęzycznymi i Oddziałami Sportowymi ma prawo

dostępu do sprzętu, gdzie prowadzony jest Rejestr, przeglądania Rejestru oraz sporządzania kopii czy wydruków obrazów z ekranu komputerowego.

§13
Bezpieczeństwo danych osobowych

1. Szkoła Podstawowa nr 6 im. Jana Kochanowskiego w Zgierzu z Oddziałami Dwujęzycznymi i Oddziałami Sportowymi zapewnia stopień bezpieczeństwa odpowiadający ryzyku naruszenia praw i wolności Osób w skutek przetwarzania Danych.
2. Administrator zapewnia bezpieczeństwo Danych zgodnie z przyjętymi regulacjami w tym zakresie, obejmującymi zarówno metodykę w zakresie analizy ryzyka ochrony danych (jako element zarządzania ryzykiem bezpieczeństwa informacji), jak i metodykę prowadzenia oceny skutków dla ochrony Danych w sytuacjach tego wymagających.
3. Administrator przeprowadza i dokumentuje analizy adekwatności środków bezpieczeństwa Danych. W tym celu Szkoła Podstawowa nr 6 im. Jana Kochanowskiego w Zgierzu z Oddziałami Dwujęzycznymi i Oddziałami Sportowymi:
   a. zapewnia sobie odpowiedni stan wiedzy o bezpieczeństwie informacji, cyberbezpieczeństwie i ciągłości działania - wewnętrznie lub ze wsparciem podmiotów wyspecjalizowanych.
   b. kategoryzuje Dane oraz czynności przetwarzania pod kątem ryzyka, które przedstawiają.
   c. przeprowadza analizy ryzyka naruszenia praw lub wolności osób fizycznych dla czynności przetwarzania Danych lub ich kategorii. Analizuje możliwe sytuacje i scenariusze naruszenia ochrony Danych uwzględniając charakter, zakres, kontekst i cele przetwarzania, ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia w sytuacjach tego wymagających.
   d. ustala możliwe do zastosowania organizacyjne i techniczne środki bezpieczeństwa i ocenia koszt ich wdrażania. W tym ustala przydatność i decyduje co do zastosowania takich środków jak: pseudonimizacja, szyfrowanie Danych, innych środków cyberbezpieczeństwa składających się na zdolność do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów i usług przetwarzania
   e. określa środki zapewnienia ciągłości działania i zapobiegania skutkom katastrof, czyli zdolności do szybkiego przywrócenia dostępności Danych i dostępu do nich w razie incydentu fizycznego lub technicznego.
4. Administrator dokonuje oceny skutków dla ochrony Danych tam, gdzie zgodnie z analizą ryzyka, ryzyko naruszenia praw i wolności osób jest wysokie.
5. Administrator stosuje środki bezpieczeństwa ustalone w ramach analiz ryzyka i adekwatności środków bezpieczeństwa oraz ocen skutków dla ochrony Danych.
6. Szkoła Podstawowa nr 6 im. Jana Kochanowskiego w Zgierzu z Oddziałami Dwujęzycznymi i Oddziałami Sportowymi planując nowe rozwiązania informatyczne, weryfikuje możliwość wykorzystania pseudonimizacji lub anonimizacji do ograniczenia dostępu do Danych i zwiększenia ich bezpieczeństwa. W szczególności, gdy znajomość tożsamości konkretnych Osób nie jest konieczna (np. przy budowie założeń nowej kampanii marketingowej), w miarę możliwości ogranicza dostęp do Danych poprzez ich spseudonimizowanie lub zanonimizowanie.
7. Administrator będzie wprowadzać w miarę możliwości i uzasadnienia zasady ochrony Danych w przesyle (Dane na laptopach, telefonach komórkowych, pendrive'ach, płytach cd, kartach

pamięci, przesyłanych emailem), w tym w szczególności zasady co do szyfrowania lub rezygnacji z szyfrowania takich Danych lub nośników, na których się znajdują.

8. Administrator tworzy kopie zapasowe Danych z uwzględnieniem następujących podstawowych zasad:
   a. zasadniczo powinny być tworzone kopie zapasowe Danych
   b. zdolność przywrócenia Danych z kopii zapasowych powinna być testowana
   c. kopie archiwalne również uważa się za kopie zapasowe
   d. okres przydatności (przechowywania) kopii zapasowych powinien być ograniczony – w szczególności nie wolno przechowywać kopii zapasowych Danych, co do których nie istnieje już podstawa prawna przetwarzania
   e. kopie zapasowe po upływie okresu przydatności powinny być niszczone
   f. dostęp do kopii zapasowych powinien być ograniczony
   g. należy określić sposób realizacji praw jednostki względem kopii zapasowych
9. Udostępnianie danych osobowych:
   a. Pracownicy nie są upoważnieni do udostępniania danych osobowych.
   b. Dane osobowe przetwarzane w Szkole Podstawowej nr 6 im. Jana Kochanowskiego w Zgierzu z Oddziałami Dwujęzycznymi i Oddziałami Sportowymi może udostępnić innemu podmiotowi wyłącznie Administrator Danych.
   c. Dane osobowe udostępnia się tylko i wyłącznie na pisemny, umotywowany wniosek przekazany bezpośrednio Administratorowi Danych.
   d. Wniosek o udostępnienie danych osobowych wpisuje się do rejestru, którego wzór stanowi załącznik nr 18 do niniejszej Polityki.
   e. Wniosek o udostępnienie danych osobowych dołącza się do dokumentacji przetwarzania danych osobowych.
10. W obszarze przetwarzania danych osobowych przetwarzanie ma formę zarówno tradycyjną (papierową) jak i elektroniczną.
11. Na obszar przetwarzania danych osobowych w Spółce składają się pomieszczenia w następujących lokalizacjach:
    a. Siedziba: ul. 3 Maja 46a, 95-100 Zgierz
12. Osoby nieuprawnione do przetwarzania danych osobowych przebywają w obszarze przetwarzania danych osobowych tylko i wyłącznie w obecności i pod nadzorem osoby upoważnionej do przetwarzania tych danych.
13. W obszarze przetwarzania danych osobowych praca na tych danych odbywa się w sposób uniemożliwiający do nich dostęp osobom nieupoważnionym, również w formie podglądu.
14. W obszarze przetwarzania danych osobowych, dokumenty i inne nośniki zawierające dane osobowe przechowywane są w szafach lub szufladach zamykanych na klucz.
15. Przetwarzanie w formie elektronicznej opiera się o infrastrukturę sieciową z dostępem do sieci Internet oraz bazę danych SQL.
16. Szczegółowe informacje dotyczące działania, platformy sprzętowej oraz oprogramowania systemów informatycznych służących do przetwarzania danych osobowych w znajdują się w instrukcjach tych systemów.
17. Systemy informatyczne przetwarzające dane osobowe zabezpieczone są przed uszkodzeniem i utratą danych, stosując urządzenia podtrzymujące zasilanie przynajmniej do momentu wylogowania się użytkownika z systemu.
18. Stacje robocze wchodzące w skład systemów informatycznych służących do przetwarzania danych osobowych zabezpieczone są licencjonowanym oprogramowaniem antywirusowym wspieranym przez zaporę sieciową.
19. Systemy informatyczne wykorzystywane do przetwarzania danych osobowych użytkowane są tylko i wyłącznie w oparciu o licencjonowane oprogramowanie systemowe i narzędziowe.

20. Przetwarzanie danych osobowych ma miejsce jedynie na nośnikach i w systemach informatycznych będących własnością Szkoły Podstawowej nr 6 im. Jana Kochanowskiego w Zgierzu z Oddziałami Dwujęzycznymi i Oddziałami Sportowymi.
21. Aktualizacja baz danych poprogramowania antywirusowego wykonywana jest automatycznie, to znaczy w chwili udostepnienia przez producenta oprogramowania nowych definicji wirusów.
22. Konfiguracja systemów operacyjnych stacji roboczych wymusza instalację krytycznych poprawek bezpieczeństwa w sposób automatyczny.
23. Przy konfiguracji urządzeń połączonych z siecią publiczną (routerów), uwzględnia się konieczność:
    a. zmiany ustawień domyślnych (fabrycznych) urządzenia:
    b. identyfikatora i hasła administracyjnego urządzenia
    c. rezerwacji adresów IP dla adresów MAC kart sieciowych stacji roboczych.
    d. ograniczenia puli adresów DHCP do ilości stacji roboczych korzystających z urządzenia.
24. W przypadku korzystania z sieci radiowej (Wi-Fi) uwzględnia się następujące zasady konfiguracji urządzenia dostępowego:
    a. wyłączenie rozgłaszania nazwy sieci,
    b. ustawienie standardu szyfrowania jako WPA2,
    c. ustanowienia minimum 10 znakowego hasła dostępu do sieci uwzględniającego małe i duże litery, cyfry oraz znaki specjalne,
    d. włączenie filtrowania urządzeń, które korzystają z sieci radiowej po adresach MAC karty sieciowej.
25. Możliwość zmiany ustawień BIOSu stacji roboczej zabezpieczona jest hasłem.
26. Hasła kont administracyjnych stacji roboczych oraz BIOSu i hasła administracyjne innych urządzeń wchodzących w skład systemu informatycznego tworzone są według zasad :
    a. mają długość przynajmniej 10 znaków
    b. zawierają małe i duże litery oraz cyfry i znaki specjalne
    c. są zmieniane przynajmniej co 30 dni
27. Nie stosuje się takich samych haseł kont administracyjnych stacji roboczych, BIOSu oraz identyfikatorów i haseł administracyjnych innych urządzeń wchodzących w skład systemu informatycznego dla różnych jednostek urządzeń i stacji roboczych.
28. Hasła kont administracyjnych stacji roboczych oraz BIOSu i hasła administracyjne innych urządzeń wchodzących w skład systemu informatycznego przechowywane są w bezpiecznym, wskazanym przez Administratora Danych miejscu.
29. Konta służbowej poczty elektronicznej pracowników mogą być zawarte wyłącznie w domenach, których właścicielem jest Szkoła Podstawowa nr 6 im. Jana Kochanowskiego w Zgierzu z Oddziałami Dwujęzycznymi i Oddziałami Sportowymi**.**
30. Służbowe konta poczty elektronicznej wykorzystywane są tylko i wyłącznie do prowadzenia korespondencji związanej z działalnością Administratora.
31. Niszczenia wycofanych z eksploatacji elektronicznych nośników z danymi osobowymi dokonuje się u profesjonalnych dostawców tego typu usług i potwierdza protokołem.
32. Niszczenia dokumentów tradycyjnych z danymi osobowymi dokonuje się przy pomocy niszczarki spełniającej wymagania przynajmniej poziomu 2 normy DIN 32757 i potwierdza protokołem.
33. Wzór protokołu z niszczenia nośnika/dokumentu stanowi załącznik nr 17 do niniejszej Polityki.
34. Zasady korzystania z mobilnego sprzętu służącego do przetwarzania danych osobowych opisuje procedura stanowiąca załącznik nr 12 do niniejszej Polityki.
35. Zasady korzystania ze sprzętu informatycznego opisuje procedura stanowiąca załącznik nr 19 do niniejszej Polityki.
36. Zasady uwierzytelniania użytkowników w systemach informatycznych opisuje procedura stanowiąca załącznik nr 15 do niniejszej Polityki.

37. Zasady tworzenia kopii zapasowych opisuje procedura stanowiąca załącznik nr 14 do niniejszej Polityki.
38. Zasady wykonywania konserwacji i napraw sprzętu informatycznego opisuje procedura stanowiąca załącznik nr 16 do niniejszej Polityki.
39. Zasady postępowania w przypadku wystąpienia incydentu bezpieczeństwa opisuje procedura nr 13 do niniejszej Polityki.
40. Opisane w niniejszym paragrafie od ust.14 do ust. 39 środki bezpieczeństwa stosowane są przez Administratora od 2011 r., kiedy zorganizowany został system ochrony danych osobowych zgodny z obowiązującymi wtedy przepisami prawa. Nie odnotowano do dnia dzisiejszego incydentów bezpieczeństwa związanych z naruszeniem praw lub wolności osób fizycznych w rozumieniu RODO. Ocenia się zatem, że ryzyko wystąpienia incydentu bezpieczeństwa przy zastosowaniu opisanych środków jest mało prawdopodobne.
41. W związku z zapisami ust. 1 do 8 oraz ust.40 oraz zapisami §5 niniejszej Polityki, Administrator Danych uznaje obecny poziom zabezpieczenia przetwarzania danych osobowych w Szkole Podstawowej nr 6 im. Jana Kochanowskiego w Zgierzu z Oddziałami Dwujęzycznymi i Oddziałami Sportowymi za wystarczający, aby przetwarzanie odbywało się zgodnie z RODO.

§14
Kodeks postępowania

Szkoła Podstawowa nr 6 im. Jana Kochanowskiego w Zgierzu z Oddziałami Dwujęzycznymi i Oddziałami Sportowymi nie jest objęta kodeksem postępowania przy przetwarzaniu danych osobowych.

§15
Procedura postępowania w przypadku kontroli Organu Nadzorczego

W przypadku kontroli ze strony Organu Nadzorczego, Szkoła Podstawowa nr 6 im. Jana Kochanowskiego w Zgierzu z Oddziałami Dwujęzycznymi i Oddziałami Sportowymi postępuje zgodnie z następującymi zasadami w tym zakresie:

1. W przypadku, gdy Kontrolerzy stawią się w siedzibie Administratora Danych, Osoba Przyjmująca natychmiast informuje o tym fakcie:
    a. Administratora Danych
    b. IOD
    c. Inną osobę wyznaczoną do tego celu przez Administratora Danych
2. Osoba Przyjmująca powinna poprosić Kontrolerów o wstrzymanie rozpoczęcia Kontroli aż do chwili przybycia Administratora Danych.
3. Administrator Danych weryfikuje tożsamość oraz upoważnienie Kontrolującego, w szczególności zakres upoważnienia do Kontroli.
    a. Weryfikacja pozytywna, kontynuacja procedury
    b. Weryfikacja negatywna, zakończenie procedury
4. Osoby wskazane w ust.1 biorą czynny udział w procesie kontrolnym oraz umożliwiają Kontrolerom przeprowadzenie przez nich kontroli, w szczególności wskazują, gdzie znajdują się potrzebne Kontrolerom informacje oraz udzielają żądanych wyjaśnień.
5. W trakcie kontroli, administrator Danych wyznacza osobę odpowiedzialną za sporządzenie wykazu przeglądanych przez Kontrolerów dokumentów z uwzględnieniem, czy dokument (zarówno w formie tradycyjnej jak i elektronicznej) został przez Kontrolerów jedynie przejrzany, czy został skopiowany. W razie możliwości, w wykazie umieszcza się uwagi Kontrolerów dotyczące tych dokumentów. Osoba wyznaczona sporządza oprócz wykazu notatkę z Kontroli, w której na bieżąco dokumentuje czynności Kontrolerów.

§16
Postanowienia końcowe

1. Wszelkie zmiany wprowadzane do niniejszej Polityki wymagają zatwierdzenia Administratora Danych.
2. Administrator Danych wdraża niniejszą Politykę aktem zarządu wewnętrznego.
3. Wszyscy pracownicy zobowiązani są do bezwzględnego przestrzegania regulacji zawartych w niniejszej Polityce.
4. Ogólne warunki nakładania administracyjnych kar pieniężnych opisane są w art. 83 RODO
5. Niezależnie od odpowiedzialności karnej i administracyjnej, naruszenie zasad ochrony danych osobowych obowiązujących w Spółce może zostać uznane za naruszenie podstawowych obowiązków pracowniczych i skutkować odpowiedzialnością dyscyplinarną.