POLITYKA BEZPIECZEŃSTWA PRZETWARZANIA DANYCH OSOBOWYCH W SZKOLE PODSTAWOWEJ W LECHOWIE

SPIS TREŚCI

PRZEPISY OGÓLNE

1. Informacje wstępne

Polityka ochrony danych osobowych zwana dalej „Polityką" w Szkole Podstawowej w Lechowie (dalej: „Szkoła"), opisuje zasady ochrony danych osobowych stosowane przez Administratora w celu spełnienia wymagań wynikających z:

1) Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.04.2016r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L 119, s. 1);
2) Ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych;
3) Rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych;
4) Przepisów prawa oświatowego, regulujących funkcjonowanie szkoły i przetwarzanych w ramach jej działalności danych osobowych,
5) Dobrych praktyk z zakresu bezpieczeństwa informacji oraz ochrony danych osobowych.

2. Stosowanie Polityki i zasady ochrony danych

Niniejsza Polityka ma zastosowanie do danych osobowych przetwarzanych w systemach informatycznych oraz w postaci papierowej będących w zasobach Szkoły. W związku z tym Administrator:

1) będzie przetwarzał dane osobowe zgodnie z prawem,
2) zapewnia rzetelność i przejrzystość przetwarzania danych,
3) zapewnia, że dane osobowe są zbierane w konkretnych, wyraźnych i prawnie uzasadnionych celach,
4) przetwarza dane wyłącznie w zakresie niezbędnym do realizacji celu,
5) zapewnia, że przetwarzane dane osobowe są prawidłowe i w razie potrzeby uaktualniane,
6) przetwarza dane osobowe przez okres, w jakim jest to niezbędne dla zrealizowania celów przetwarzania,
7) zapewnia bezpieczeństwo danych osobowych, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem, poprzez wdrożenie odpowiednich środków technicznych lub organizacyjnych.

3. Definicje

1) Administrator – Szkoła Podstawowa w Lechowie; oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych;
2) Dane osobowe – informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej („osobie, której dane dotyczą"); możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej;
3) Incydent – zdarzenia pojedyncze lub seria niepożądanych zdarzeń związanych z bezpieczeństwem danych osobowych, informacji, które zagrażają przetwarzaniu danych osobowych;
4) Inspektor Ochrony Danych /IOD/ – osoba, wyznaczona przez Administratora lub podmiot przetwarzający, posiadająca odpowiednie kwalifikacje zawodowe (wiedzę fachową na temat prawa i praktyk w dziedzinie ochrony danych osobowych) oraz umiejętności wymagane do wypełniania zadań związanych z ochroną danych, zwana w treści Polityki również jako „IOD";
5) Kopia zapasowa – kopia danych lub oprogramowania, której celem wykonania jest odtworzenie systemu po awarii;
6) Naruszenie ochrony danych osobowych – naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych;
7) Obsługa informatyczna – osoba lub podmiot wyznaczony przez Administratora do realizacji zadań w zakresie

zarządzania, bieżącego nadzoru nad systemami informatycznymi oraz serwisu sprzętu komputerowego;

8) **Podmiot przetwarzający** – osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, który przetwarza dane osobowe w imieniu administratora;
9) **Polityka** – niniejsza Polityka ochrony danych osobowych;
10) **Przetwarzanie** – operacje lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, takie jak zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie;
11) **Rejestr czynności przetwarzania danych –** rejestr czynności przetwarzania danych osobowych, o którym stanowi art. 30 ust. 1 RODO;
12) **Rejestr wszystkich kategorii czynności przetwarzania** – rejestr wszystkich kategorii czynności przetwarzania dokonywanych, o którym stanowi art. 30 ust. 2 RODO;
13) **RODO** – Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.04.2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych);
14) **Ryzyko** – potencjalna sytuacja, w której określone zagrożenie wykorzystując podatność aktywów lub grupy aktywów powodować może chociażby potencjalną szkodę majątkową lub niemajątkową;
15) **System informatyczny** – system przetwarzania danych, w tym danych osobowych, łącznie z zasobami technicznymi (stanowisko pracy, jednostka centralna, system zarządzania, sieć teletransmisyjna), pracownikami oraz określonym obszarem działania (pomieszczeniami);
16) **Użytkownik** - osoba posiadająca dostęp do dokumentacji zawierającej dane osobowe lub dostęp do systemu informatycznego przetwarzającego informacje lub dane osobowe;
17) **Zgoda** – dobrowolne, konkretne, świadome i jednoznaczne okazanie woli, którym osoba, której dane dotyczą, w formie oświadczenia lub wyraźnego działania potwierdzającego, przyzwala na przetwarzanie dotyczących jej danych osobowych.

POLITYKA BEZPIECZEŃSTWA PRZETWARZANIA DANYCH OSOBOWYCH

4. Podział kompetencji w zakresie ochrony danych osobowych

Administrator

1) wdraża odpowiednie środki techniczne i organizacyjne, mające na celu zabezpieczanie przetwarzanych danych oraz zapewnianie poufności, integralności i dostępności danych,
2) wyznacza IOD, o czym zawiadamia Prezesa Urzędu Ochrony Danych Osobowych,
3) podejmuje odpowiednie działania w przypadku naruszenia lub podejrzenia naruszenia przetwarzanych danych zgodnie z procedurą stanowiącą integralną część niniejszej Polityki,
4) upoważnia poszczególne osoby do przetwarzania danych osobowych w określonym indywidualnie zakresie,
5) nadaje lub zatwierdza Użytkownikom uprawnienia do pracy w systemach informatycznych,
6) podejmuje decyzje dotyczące przeprowadzenia oceny skutków planowanych operacji przetwarzania danych po konsultacji z IOD,
7) zatwierdza Rejestr czynności przetwarzania danych osobowych oraz Rejestr kategorii czynności przetwarzania,
8) wdraża niniejszą Politykę wraz z załącznikami,
9) dopełnia wszelkie pozostałe obowiązki wymagane przez RODO i inne przepisy regulujące zasady przetwarzania danych osobowych,
10) publikuje dane kontaktowe Inspektora Ochrony Danych i zawiadamia o nich organ nadzorczy, zgodnie z art. 37 ust. 7 RODO. Publikacja danych kontaktowych odbywa się w poprzez publiczne udostępnienie przez Administratora informacji o: imieniu i nazwisku Inspektora, numerze kontaktowym lub adresie e-mail, zgodnie z art. 11 w zw. z art. 10 ust. 1 ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych.

Inspektor Ochrony Danych /IOD/

1) weryfikuje przestrzeganie przepisów o ochronie danych osobowych i informuje Administratora oraz wszystkie

osoby przetwarzające dane o obowiązkach na nich spoczywających,
2) aktualizuje dokumentację z zakresu ochrony danych osobowych,
3) opracowuje rejestr czynności przetwarzania danych oraz rejestr kategorii czynności przetwarzania we współpracy z Administratorem lub wyznaczonymi Użytkownikami i dokonuje jego bieżącej aktualizacji na każde żądanie Administratora,
4) współpracuje z Administratorem w zakresie oceny skutków planowanych operacji przetwarzania danych oraz monitoruje jej wykonanie,
5) pełni funkcję punktu kontaktowego oraz współpracuje w przypadkach opisanych w przepisach z Prezesem Urzędu Ochrony Danych Osobowych w kwestiach związanych z przetwarzaniem danych osobowych,
6) sprawuje nadzór nad zgłoszonymi do IOD naruszeniami ochrony danych osobowych,
7) na wniosek Administratora opiniuje wnioski dotyczące realizacji praw osób, których dane dotyczą,
8) we współpracy z Administratorem dokonuje systemowego sprawdzenia procesu wydawania upoważnień do przetwarzania danych osobowych i uprawnień do systemów informatycznych,
9) na wniosek Administratora opiniuje umowy powierzenia przetwarzania danych osobowych,
10) przeprowadza wewnętrzne szkolenia z zakresu ochrony danych osobowych dla osób mających dostęp do danych,
11) bierze czynny udział w audytach zewnętrznych dotyczących przetwarzania danych osobowych w Szkole.

Obsługa informatyczna - wyznaczony przez Administratora pracownik Szkoły lub osoba zatrudniona, w tym zakresie na podstawie umowy:
1) przydziela Użytkownikom identyfikator i hasło do systemu informatycznego oraz dokonuje ewentualnych modyfikacji uprawnień, a także usuwa lub wyłącza konta Użytkowników zgodnie z zasadami określonymi w niniejszej Polityce oraz właściwych przepisach prawa,
2) dokonuje naprawy i konserwacji sprzętu komputerowego,
3) podejmuje działania służące zapewnieniu niezawodności zasilania komputerów, innych urządzeń mających wpływ na bezpieczeństwo przetwarzania danych oraz zapewnieniu bezpiecznej wymiany danych w sieci wewnętrznej i bezpiecznej teletransmisji,
4) wykonuje kopie zapasowe danych lub oprogramowania,
5) prowadzi inwentaryzację sprzętu komputerowego i oprogramowania,
6) w sytuacji stwierdzenia naruszenia zabezpieczeń systemu informatycznego informuje IOD o naruszeniu i współdziała z nim przy ustalaniu i usuwaniu skutków naruszenia.

Użytkownicy

Użytkownicy dopuszczeni przez Administratora do przetwarzania danych osobowych, zobowiązani są do:
a) udziału w szkoleniach dotyczących ochrony danych osobowych,
b) zapoznania się z przepisami prawa w zakresie ochrony danych osobowych,
c) niezwłocznego zawiadomienia przełożonego o naruszeniach związanych z przetwarzaniem danych osobowych,
d) stosowania określonych przez Administratora procedur i środków mających na celu zabezpieczenie danych przed ich udostępnieniem osobom nieupoważnionym.

5. Podstawy przetwarzania danych osobowych

1. Przetwarzanie danych osobowych zwykłych dopuszczalne jest tylko wtedy, gdy zostanie spełniona jedna z przesłanek wynikających z art. 6 ust. 1 RODO.
2. W przypadku przetwarzania danych osobowych szczególnych kategorii podstawą do przetwarzania danych mogą być wyłącznie przesłanki wynikające z art. 9 ust. 2 RODO.
3. W przypadku przetwarzania danych osobowych na podstawie zgody osoby, której dane dotyczą, należy stosować oświadczenie o wyrażeniu zgody na przetwarzanie danych osobowych, którego wzór stanowi **załącznik nr 1.1** do niniejszej Polityki (wzór służy do konstruowania szczegółowych zgód na przetwarzanie danych osobowych), a wzór oświadczenia o wycofaniu zgody na przetwarzanie danych osobowych znajduje się w **załączniku nr 1.2**.

6. Obowiązek informacyjny

1. Administrator realizuje obowiązek informacyjny w stosunku do osób od których bezpośrednio są zbierane dane osobowe zgodnie z art. 13 ust. 1 i 2 RODO oraz w stosunku do osób, których dane zostały zebrane niebezpośrednio od nich zgodnie z art. 14 ust.1 i 2 RODO.
2. Obowiązek informacyjny Szkoła realizuje poprzez umieszczenie klauzul informacyjnych w dokumentach przekazywanym pracownikom oraz odesłanie do miejsca, w którym można uzyskać pełna informację o przetwarzaniu danych: tablica ogłoszeń, strona internetowa Szkoły.
3. Wszystkie klauzule informacyjne, tworzone dla potrzeb Szkoły zawarte są w rejestrze, którego wzór stanowi załącznik nr 2 do niniejszej Polityki.

7. Prawa osób, których dane dotyczą

1. Osobie, której dane są przetwarzane, przysługują następujące prawa:
1) prawo dostępu do danych,
2) prawo do sprostowania danych,
3) prawo do usunięcia danych,
4) prawo do ograniczenia przetwarzania danych,
5) prawo do przenoszenia danych,
6) prawo do wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych.
2. Szczegółowe zasady realizowania w/w praw zostały opisane w załączniku nr 3 do niniejszej Polityki.

8. Dopuszczenie do przetwarzania danych osobowych

1. Do przetwarzania danych osobowych w Szkole mogą mieć dostęp osoby:
   - wykonujące zawód nauczyciela;
   - inne osoby wykonujące czynności wspomagające nauczyciela;
   - osoby wykonujące czynności obsługę informatyczną;
   - pracownicy administracji, wykonujący czynności kadrowo – finansowe.

   Osoby są dopuszczone do przetwarzania przez Administratora na podstawie pisemnego upoważnienia do przetwarzania danych osobowych, oraz składają oświadczenie o zachowaniu w tajemnicy danych osobowych (w poufności).
2. Upoważnienie jest przygotowywane na podstawie wzoru upoważnienia do przetwarzania danych osobowych stanowiącego załącznik nr 4.1 do niniejszej Polityki, natomiast wzór oświadczenia o zachowaniu w poufności danych osobowych stanowi załącznik nr 5.
3. Upoważnienie wygasa wraz z rozwiązaniem umowy o pracę lub zakończeniem wykonywania czynności związanych z przetwarzaniem danych osobowych określonych np. umową cywilnoprawną.
4. Administrator uprawniony jest do odwołania nadanego upoważnienia do przetwarzania danych osobowych w każdym czasie. Wzór odwołania (cofnięcia) upoważnienia stanowi załącznik nr 4.2
5. Zatwierdzone przez Administratora upoważnienie do przetwarzania danych osobowych rejestruje się w ewidencji osób upoważnionych do przetwarzania danych, której wzór stanowi załącznik nr 6 do Polityki.
6. Upoważnienia do przetwarzania danych przechowywane są w aktach osobowych pracownika.
7. W przypadku zmiany stanowiska lub zakresu obowiązków osoby upoważnionej albo w przypadku wystąpienia innych okoliczności, które wpływają bezpośrednio na rodzaj i zakres przetwarzanych danych osobowych, należy odpowiednio zmienić upoważnienie lub przygotować nowe.
8. W przypadku ustania zatrudnienia lub zaistnienia innej przyczyny skutkującej odwołaniem upoważnienia, należy odnotować te zmiany w ewidencji osób upoważnionych do przetwarzania danych osobowych. Powyższe dotyczy każdej formy zatrudnienia (umowa o pracę, umowa cywilnoprawna, staż, praktyka).

9. Rejestrowanie czynności przetwarzania

1. Wszystkie czynności przetwarzania realizowane przez Szkołę zamieszcza się w Rejestrze czynności przetwarzania danych.
2. Wszystkie czynności przetwarzania powierzone Administratorowi przez innego Administratora zamieszcza w

Rejestrze wszystkich kategorii czynności przetwarzania.

3. Szkoła przestrzega wszelkich zasad przetwarzania powierzonych jej danych nałożonych na podstawie obowiązujących przepisów prawa, umów powierzenia, oraz dokumentów określających zasady takiego przetwarzania.
4. W przypadku zmian w przepisach prawa lub nałożenia na Szkoła obowiązku wykonania zadań realizowanych w interesie publicznym lub w ramach sprawowania władzy publicznej, we współpracy z Inspektorem Ochrony Danych, dokonuje się uzupełnienia lub zmian w Rejestrze czynności przetwarzania danych.
5. W przypadku gdy Szkoła występuje jako Podmiot przetwarzający dane – na podstawie umowy powierzenia przetwarzania danych lub innego instrumentu prawnego, we współpracy z Inspektorem Ochrony Danych, dokonuje się uzupełnienia lub zmian w Rejestrze wszystkich kategorii czynności przetwarzania.
6. Rejestry, o których mowa w ust. 1 i 2 przyjmują formę pisemną, w tym formę elektroniczną.
7. Administrator jest zobowiązany do udostępnienia w/w rejestrów na żądanie organu nadzorczego. Rejestry nie stanowią dokumentów udostępnianych na podstawie Ustawy z dnia 6 września 2001 r. o dostępie do informacji publicznej.
8. IOD we współpracy z Administratorem, przygotowuje i aktualizuje rejestry, o których mowa w ust.1 i 2.

W **Rejestrze czynności przetwarzania danych** prowadzonym przez Szkołę jako Administratorze danych osobowych, zamieszcza się następujące informacje:

a) dane kontaktowe Administratora (Szkoły) oraz wszelkich współadministratorów, a także gdy ma to zastosowanie - przedstawiciela administratora oraz inspektora ochrony danych;
b) cele przetwarzania;
c) opis kategorii osób, których dane dotyczą, oraz kategorii danych osobowych;
d) kategorie odbiorców, którym dane osobowe zostały lub zostaną ujawnione, w tym odbiorców w państwach trzecich lub w organizacjach międzynarodowych;
e) gdy ma to zastosowanie, przekazania danych osobowych do państwa trzeciego lub organizacji międzynarodowej, w tym nazwa tego państwa trzeciego lub organizacji międzynarodowej, a w przypadku przekazań, o których mowa w art. 49 ust. 1 akapit drugi RODO, dokumentacja odpowiednich zabezpieczeń;
f) jeżeli jest to możliwe, planowane terminy usunięcia poszczególnych kategorii danych;
g) jeżeli jest to możliwe, ogólny opis technicznych i organizacyjnych środków bezpieczeństwa, o których mowa w art. 32 ust. 1 RODO.

W **Rejestrze wszystkich kategorii czynności przetwarzania** prowadzonym przez Szkołę, w przypadku, w którym występuje jako Podmiot przetwarzający dane osobowe, zamieszcza się następujące informacje:

a) imię i nazwisko lub nazwa oraz dane kontaktowe Podmiotu przetwarzającego lub podmiotów przetwarzających oraz każdego administratora, w imieniu którego działa Podmiot przetwarzający, a gdy ma to zastosowanie - przedstawiciela administratora lub podmiotu przetwarzającego oraz inspektora ochrony danych;
b) kategorie przetwarzań dokonywanych w imieniu każdego z administratorów;
c) gdy ma to zastosowanie - przekazania danych osobowych do państwa trzeciego lub organizacji międzynarodowej, w tym nazwa tego państwa trzeciego lub organizacji międzynarodowej, a w przypadku przekazań, o których mowa w art. 49 ust. 1 akapit drugi RODO, dokumentacja odpowiednich zabezpieczeń;
d) jeżeli jest to możliwe, ogólny opis technicznych i organizacyjnych środków bezpieczeństwa, o których mowa w art. 32 ust. 1 RODO.

10. Szkolenia z zakresu ochrony danych osobowych

1. Każdy Użytkownik, który uzyskuje upoważnienie do przetwarzania danych osobowych ma obowiązek zapoznać się z najważniejszymi informacjami o obowiązkach związanych z przetwarzaniem danych osobowych. Wzór informatora zawierającego w/w informacje stanowi **załącznik nr 7** do niniejszej Polityki.
2. Administrator utrzymuje kwalifikacje personelu na poziomie odpowiednim dla zapewnienia bezpieczeństwa przetwarzanych danych i przeprowadza wewnętrzne szkolenia z zakresu ochrony danych osobowych.
3. Pierwsze szkolenie odbywa się przed rozpoczęciem przetwarzania danych lub niezwłocznie po rozpoczęciu

przetwarzania danych.

4. Każde szkolenie wewnętrzne powinno być udokumentowane poprzez sporządzenie dokumentu potwierdzającego uczestnictwo osoby w szkoleniu (imienna karta szkolenia).

11. Powierzenie przetwarzanych danych

1. Administrator może powierzyć przetwarzanie danych osobowych podmiotom przetwarzającym.
2. W przypadku powierzenia przetwarzania danych konieczne jest albo zawarcie umowy powierzenia przetwarzania danych osobowych pomiędzy Administratorem oraz podmiotem przetwarzającym, który przetwarza dane w imieniu Administratora albo posłużenie się innym instrumentem prawnym, który podlega prawu Unii lub prawu polskiemu i wiąże zarówno podmiot przetwarzający jak i Administratora.
3. IOD przygotowuje we współpracy Użytkownikami i weryfikuje umowy powierzenia przetwarzania danych lub inne instrumenty prawne przed ich zawarciem we współpracy z Administratorem.
4. Administrator przyjął minimalne wymagania co do treści umowy powierzenia przetwarzania danych, której wzór stanowi **załącznik nr 8** do Polityki.
5. Administrator po zawarciu każdej umowy powierzenia – odnotowuje ten fakt w rejestrze zawartych umów powierzenia, którego wzór stanowi **załącznik nr 9** do niniejszej Polityki.

12. Naruszenia ochrony danych osobowych

1. Administrator stosuje procedury pozwalające na identyfikację, ocenę i zgłoszenie zidentyfikowanego naruszenia ochrony danych Prezesowi Urzędu Ochrony Danych Osobowych.
2. Procedura postępowania w sytuacji naruszenia ochrony danych osobowych stanowi **załącznik nr 10** do niniejszej Polityki.

INSTRUKCJA ZARZĄDZANIA SYSTEMAMI INFORMATYCZNYMI

13. Zasady dostępu do systemów informatycznych. Identyfikator i hasło.

1. Administrator nadaje uprawnienia Użytkownikom do pracy w systemach informatycznych.
2. Do ewidencji osób upoważnionych do przetwarzania danych osobowych – **załącznik nr 6** – wpisuje się systemy informatyczne do jakich osoba upoważniona do przetwarzania danych otrzymała dostęp.
3. W przypadku dostępu Użytkowników do systemów informatycznych, należy stosować metodę uwierzytelnienia poprzez wpisanie indywidualnego identyfikatora / login'u oraz hasła.
4. Identyfikator jest przydzielany według zasady przyjętej w Szkole.
5. Hasło powinno składać się z unikalnego zestawu znaków, zawierających małe i wielkie litery, cyfry oraz znaki specjalne. Hasła powinny być regularnie zmieniane przez Użytkowników oraz niezwłocznie w przypadku podejrzenia, że hasło mogło zostać ujawnione osobie nieuprawnionej.
6. Użytkownik zobowiązany jest do zachowania hasła w poufności i niezapisywania haseł w sposób jawny.
7. Hasła administracyjne do urządzeń i systemów informatycznych, w tym baz danych, winny być przechowywane w zapieczętowanej kopercie w miejscu wskazanym przez Administratora.

14. Rozpoczęcie, zakończenie oraz zasady pracy w systemie

1. Rozpoczęcie pracy w systemie odbywa się poprzez:
   a) przygotowanie stanowiska pracy,
   b) włączenie stacji roboczej,
   c) wprowadzenie swojego identyfikatora i hasła.
2. Zakończenie pracy w systemie odbywa się poprzez:
   a) zamknięcie aplikacji,
   b) odłączenie się od zasobów systemowych,
   c) zamknięcie systemu operacyjnego,
   d) wyłączenie stacji roboczej.
3. Zabrania się użytkownikom pracującym w systemie:

a) udostępniania stacji roboczej osobom niezarejestrowanym z zastrzeżeniem lit. b,
b) udostępniania stacji roboczej do konserwacji lub naprawy bez porozumienia z obsługa informatyczną,
c) używania nielicencjonowanego oprogramowania.

4. Administrator prowadzi rejestr całego sprzętu informatycznego oraz wszystkich systemów i programów informatycznych.
5. Użytkownik zobowiązany jest korzystać ze sprzętu elektronicznego w sposób zgodny z jego przeznaczeniem i chronić go przed jakimkolwiek zniszczeniem lub uszkodzeniem.
6. Użytkownik ma obowiązek niezwłocznie zgłosić utratę lub zniszczenie powierzonego sprzętu Administratorowi.
7. Użytkownik nie może bez zgody Administratora instalować dodatkowych urządzeń (np. twardych dysków, pamięci) lub podłączać niezatwierdzonych urządzeń do systemu informatycznego.
8. Użytkownik nie może bez zgody Administratora korzystać z prywatnego sprzętu elektronicznego (np. laptopów, telefonów, aparatów fotograficznych, nośników typu pendrive) do wykonywania zadań służbowych.
9. Administrator ma prawo do monitorowania sprzętu służbowego wykorzystywanego przez Użytkowników. O fakcie monitorowania Administrator zobowiązany jest powiadomić Użytkowników, zgodnie z przepisami Ustawy z dnia 26 czerwca 1974 r. Kodeks pracy, nie później niż 2 tygodnie przed jego uruchomieniem.
10. Użytkownik zobowiązany jest do korzystania wyłącznie z oprogramowania dopuszczonego do stosowania w Szkole.
11. Użytkownik nie może instalować ani używać oprogramowania innego, niż przekazane lub udostępnione przez Administratora.

15. Obsługa poczty elektronicznej

1. Użytkownik jest zobowiązany do korzystania z przyznanego mu adresu mailowego wyłącznie w celu prowadzenia korespondencji służbowej.
2. Użytkownik nie może używać służbowego adresu mailowego do celów prywatnych.
3. Użytkownik nie może używać służbowego adresu mailowego w celu rozpowszechniania treści o charakterze obraźliwym, niemoralnym lub niestosownym wobec powszechnie obowiązujących zasad postępowania.
4. Użytkownik powinien zachować szczególną ostrożność przy wpisywaniu adresu odbiorcy wiadomości.
5. Użytkownik podczas wysyłania maili do wielu adresatów jednocześnie, powinien użyć metody „Ukryte do wiadomości – UDW". Zabronione jest rozsyłanie maili do wielu adresatów z użyciem opcji „Do wiadomości".
6. Użytkownik powinien zastosować zabezpieczenia kryptograficzne przy przesyłaniu załączników do wiadomości. Wysyłając wiadomość należy zaszyfrować hasłem przesyłany plik w formie załącznika, a hasło powinno być przekazane adresatowi za pośrednictwem innego źródła, tj. sms, bądź podczas rozmowy telefonicznej po uprzednim zweryfikowaniu tożsamości adresata.
7. Użytkownik powinien zachować szczególną ostrożność podczas odbierania poczty elektronicznej, a w szczególności nie powinien otwierać plików i linków w niej zawartych, ani otwierać załączników jeżeli nie ma pewności co do autentyczności adresata wiadomości. Tego typu maile w większości przypadków mogą zawierać załączniki ze szkodliwym oprogramowaniem, które po „kliknięciu" infekują komputer Użytkownika.
8. W wyniku działania takiego szkodliwego oprogramowania może dojść do poważnych incydentów, łącznie z pełną utratą danych osobowych lub zaszyfrowaniem. W takim przypadku Użytkownik powinien poinformować o zdarzeniu Administratora.
9. Użytkownik powinien regularnie przeglądać folder spam i usuwać niepotrzebne wiadomości pocztowe.

16. Korzystanie z Internetu

1. Użytkownik powinien korzystać z dostępu do sieci Internet wyłącznie w celach niezbędnych do wykonywania zadań służbowych.
2. Użytkownik nie powinien otwierać stron internetowych zawierających treści nie związane bezpośrednio z wykonywaną pracą, ze względu na możliwość przypadkowego pobrania złośliwego kodu, który może automatycznie zainfekować system operacyjny komputera.
3. Użytkownik ponosi pełną odpowiedzialność za szkody spowodowane przez oprogramowanie instalowane z

Internetu.

4. Użytkownik nie może korzystać ze stron internetowych, na których prezentowane są treści o charakterze przestępczym, hackerskim, pornograficznym lub innym zakazanym przez prawo (na większości stron tego typu może być zaimplementowany złośliwy kod, który może automatycznie zainfekować system operacyjny komputera w sposób niewidoczny dla Użytkownika).
5. Użytkownik nie może pobierać aplikacji z sieci Internet bez wcześniejszej zgody Administratora.
6. Użytkownik w przypadku korzystania z szyfrowanego połączenia przez przeglądarkę internetową, powinien zwrócić uwagę na pojawienie się odpowiedniej ikony (kłódka) oraz adresu www rozpoczynającego się frazą ”https:”. Dla pewności należy „kliknąć” na ikonkę kłódki i sprawdzić, czy właścicielem certyfikatu jest wiarygodny właściciel.
7. Użytkownik powinien zachować szczególną ostrożność w przypadku podejrzanego żądania lub prośby zalogowania się na stronę (np. na stronę banku) lub podania naszych loginów i haseł, PIN-ów, numerów kart płatniczych przez Internet.

17. Praca na odległość

1. Komunikacja z zewnątrz powinna być realizowana tylko poprzez mechanizmy zapewniające odpowiednie bezpieczeństwo (np. VPN, Team Viewer). W przypadku firm zewnętrznych dokonujących czynności serwisowych, dostęp taki jest nadzorowany przez Obsługę informatyczną oraz każdorazowo powinien być poprzedzony autoryzacją (np. podaniem hasła do Team Viewer, które wygasa po skończonej sesji).
2. Administrator wprowadza obowiązek logowania połączeń wykonywanych za pomocą sieci bezprzewodowej w celu rejestracji działań Użytkowników w sieci i zmniejszenia ryzyka użytkowania sieci niezgodnie z przeznaczeniem.
3. Komunikację należy prowadzić tylko za pomocą bezpiecznych metod transmisji, w tym włączenie transmisji szyfrowanej lub przeniesienie usług sieciowych na serwer posiadający taką możliwość.

18. Zabezpieczanie sprzętu i systemu informatycznego

1. Komputery stacjonarne i przenośne powinny być zabezpieczone programem antywirusowym, który sprawuje ciągły nadzór (ciągła praca w tle) nad pracą systemu.
2. Sprawdzanie obecności wirusów komputerowych w systemie informatycznym oraz ich usuwanie powinno odbywać się przy wykorzystaniu ww. oprogramowania zainstalowanego na stacjach roboczych oraz komputerach przenośnych.
3. Użytkownik jest obowiązany każdorazowo zawiadomić Obsługę informatyczną o pojawiających się komunikatach, wskazujących na wystąpienie zagrożenia wywołanego szkodliwym oprogramowaniem – wirusa lub w przypadku sygnalizowanych problemów z działaniem oprogramowania antywirusowego.
4. Użytkownik, który posiada dostęp do systemów informatycznym powinien mieć zablokowaną możliwość instalowania nieautoryzowanego oprogramowania.

19. Używanie elektronicznych nośników danych

1. Użytkownik może korzystać wyłącznie z elektronicznych nośników danych przeznaczonych do użytku służbowego, w szczególności: pendriv, dysk zewnętrzny, CD-R, DVD itp.
2. Użytkownik korzystający z elektronicznych nośników danych w całym okresie użytkowania odpowiedzialny jest za bezpieczeństwo danych.
3. Użytkownik korzystający z ww. urządzeń zobowiązany jest do:
   1) przechowywania danych na dysku szyfrowanym zabezpieczonym hasłem,
   2) transportu nośnika w sposób minimalizujący ryzyko kradzieży lub zniszczenia oraz stosownego zabezpieczenia nośnika przed uszkodzeniem,
   3) zdecydowanego i skutecznego uniemożliwienia skorzystania z nośnika osobom nieuprawnionym (np. rodzina, dzieci, znajomi).

20. Przeglądy i konserwacje sprzętu elektronicznego i nośników danych

1. Obsługa informatyczna dokonuje przeglądu i konserwacji sprzętu elektronicznego i nośników danych.

2. Użytkownik nie może samodzielne dokonywać napraw sprzętu elektronicznego, wymiany jego podzespołów oraz wykonywanie innych czynności nie związanych bezpośrednio z jego eksploatacją lub nie dopuszczonych do wykonywania przez producenta sprzętu w instrukcji obsługi.
3. W przypadku serwisowania zasobów informatycznych przez podmioty zewnętrzne, Obsługa informatyczna wymontowuje dyski twarde przed oddaniem ich do serwisu. W sytuacji, gdy do serwisu należy oddać cały zasób Administrator winien podpisać stosowną umowę powierzenia danych z firmą serwisową.
4. Użytkownik ma obowiązek niezwłocznie powiadomić Obsługę informatyczną o wszelkich nieprawidłowościach i awariach sprzętu informatycznego, mogących prowadzić do próby naruszenia lub naruszenia bezpieczeństwa danych osobowych.
5. W przypadku awarii systemu informatycznego i utraty informacji lub w przypadku zaistnienia możliwości uszkodzenia informacji Obsługa informatyczna jest zobowiązana do:
   1) przetestowania sieci informatycznej, systemu informatycznego oraz aplikacji służącej do przetwarzania danych,
   2) ocenić zasadność odtworzenia danych przy wykorzystaniu aktualnej kopii zapasowej lub kilku kopii zapasowych, a w przypadku uzasadnionej konieczności odtworzyć dane przy wykorzystaniu aktualnej kopii zapasowej lub kilku kopii zapasowych.

21. Utylizacja i serwis sprzętu elektronicznego

1. W przypadku wycofania sprzętu elektronicznego z użycia, dane osobowe na nim zapisane powinny być kasowane przy użyciu dedykowanego oprogramowania do bezpiecznego usuwania danych.
2. W przypadku braku możliwości programowego usunięcia danych ze sprzętu elektronicznego podlega on fizycznemu zniszczeniu.
3. Zniszczenie sprzętu elektronicznego powinno być potwierdzane protokołem zniszczenia.
4. W przypadku przekazywania stacji roboczej z dyskiem albo innych nośników danych do naprawy, dysk lub nośnik powinien zostać zdemontowany lub pozbawiany danych, naprawa powinna być dokonywana w obecności osoby upoważnionej przez Administratora lub powinna zostać zawarta umowa powierzenia przetwarzania danych.

22. Zasady bezpiecznej pracy

Każdy Użytkownik zobowiązany jest do stosowania następujących zasad bezpieczeństwa:

1) polityki „czystego biurka” - w trakcie pracy Użytkownik powinien mieć na biurku tylko te materiały, które są niezbędne do wykonywania obowiązków służbowych. W przypadku opuszczenia stanowiska pracy materiały zawierające dane, wymagające szczególnej ochrony powinny być zabezpieczone przed dostępem osób nieuprawnionych. Po zakończeniu dnia pracy każdy, Użytkownik zobowiązany jest do zabezpieczenia wszelkich dokumentów i nośników zawierających istotne dane, w celu uniemożliwienia dostępu do nich osób nieupoważnionych,
2) polityki „czystego ekranu” - w przypadku chwilowego opuszczenia stanowiska pracy Użytkownik zobowiązany jest do wylogowania się z systemu bądź zablokowania dostępu do pulpitu stacji roboczej w celu uniemożliwienia dostępu do systemu operacyjnego lub aplikacji przez osoby niepowołane. Ponadto w trakcie pracy Użytkownik powinien mieć otwarte tylko te aplikacje, które są niezbędne do wykonywania obowiązków służbowych,
3) takiego ustawienia monitora, aby osoby niepowołane nie mogły zapoznać się z informacjami wyświetlanymi na monitorze,
4) bieżącego niszczenia w niszczarce niepotrzebnej dokumentacji papierowej oraz przechowywania pozostałej dokumentacji papierowej w zabezpieczonych szafach, zamykanych przynajmniej na klucz,
5) niepozostawiania osób postronnych w pomieszczeniu, w którym przetwarzane są dane osobowe, bez obecności osoby upoważnionej,
6) zachowania w poufności wszelkich informacji, w tym danych osobowych poprzez złożenie stosownego oświadczenia,
7) niepozostawiania klucza w drzwiach po zewnętrznej stronie pomieszczenia,
8) niepozostawiania pomieszczeń biurowych bez opieki.

23. Wydruki

1. Użytkownik sporządzający wydruki, które zawierają dane osobowe jest odpowiedzialny za zachowanie szczególnej ostrożności przy korzystaniu z nich, a zwłaszcza za zabezpieczenie ich przed dostępem osób nie posiadających imiennego upoważnienia oraz nieuprawnionych do wglądu.
2. W stosunku do dokumentów papierowych stanowiących wydruki z systemu informatycznego Szkoły, Użytkowników obowiązują następujące środki ostrożności:
   1) wydruki z systemu informatycznego i wszelkie dokumenty zawierające dane osobowe powinny być niedostępne dla osób trzecich,
   2) wydruki z systemu informatycznego i wszelkie dokumenty zawierające dane osobowe nie mogą być pozostawione w drukarce lub kserokopiarce ogólnodostępnej,
   3) wydruki niepotrzebne i nieprzydatne powinny być na bieżąco niszczone za pomocą niszczarki,
   4) dokumenty zawierające dane osobowe, których nie można zniszczyć z przyczyn technicznych lub formalnych, powinny być składowane w miejscu z ograniczonym dostępem, systematycznie weryfikowane, a następnie archiwizowane zgodnie z obowiązującymi w tym zakresie przepisami.

24. Postępowanie z kluczami

1. Wszystkie pomieszczenia biurowe w Szkole stanowią obszar przetwarzania danych osobowych.
2. Dodatkowo Administrator określił szczególne obszary przetwarzania danych objęte dodatkowymi zabezpieczeniami, do których dostęp mają tylko osoby upoważnione przez Administratora.
3. Opis środków technicznych służących do zabezpieczenia danych osobowych oraz wskazanie obszaru przetwarzania zawiera załącznik nr 11 do niniejszej Polityki.
4. Klucze do poszczególnych pomieszczeń osoby upoważnione pobierają i zdają po zakończonym dniu pracy zgodnie z ustaleniami Dyrektora. Od momentu pobrania kluczy do momentu ich zdania na tych osobach spoczywa pełna odpowiedzialność za ich zabezpieczenie. Po otwarciu pomieszczeń biurowych, przed przystąpieniem do pracy, Użytkownicy sprawdzają stan zastosowanych zabezpieczeń.
5. Zapasowe klucze do wszystkich pomieszczeń winny zostać odpowiednio zabezpieczone i przechowywane. Każdorazowe użycie klucza zapasowego powinno być zgłoszone do osoby upoważnionej przez Administratora.
6. Zabrania się pozostawiania kluczy do pomieszczeń z obszaru przetwarzania danych w drzwiach lub w miejscach ogólnie dostępnych. Pomieszczenia te powinny być zamknięte na klucz się na czas nieobecności osób upoważnionych w sposób uniemożliwiający dostęp do nich osobom trzecim.
7. Zabrania się dorabiania kluczy do pomieszczeń, kłódek, szaf biurowych itp. bez zgody Administratora.
8. Zabrania się pozostawiania osób trzecich w pomieszczeniach biurowych bez nadzoru osób upoważnionych przez Administratora.

25. Analiza ryzyka

1. Administrator analizuje możliwe sytuacje i naruszenia ochrony danych osobowych uwzględniając charakter, zakres, kontekst i cele przetwarzania, ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia, zwane dalej „analizami ryzyka".
2. Administrator przeprowadza analizy ryzyka naruszenia praw lub wolności osób fizycznych dla czynności przetwarzania danych lub ich kategorii.
3. Analiza ryzyka powinna zapewniać:
   1) zidentyfikowanie ryzyka,
   2) oszacowanie ryzyka z punktu widzenia następstw dla działalności Szkoły oraz prawdopodobieństwa wystąpienia takiego ryzyka,
   3) informowanie o następstwach wystąpienia ryzyka,
   4) ustanowienie priorytetów w postępowaniu z ryzykiem,
   5) regularne monitorowanie i przegląd różnych typów ryzyka oraz procesu zarządzania ryzykiem,
   6) zbieranie informacji w celu doskonalenia podejścia do zarządzania ryzykiem.
4. Administrator dokumentuje wykonaną analizę ryzyka w postaci raportu.
5. Administrator dokonuje oceny skutków planowanych operacji przetwarzania dla ochrony danych osobowych

w przypadkach, w których zgodnie z analizą ryzyka, ryzyko naruszenia praw i wolności osób jest wysokie oraz w każdym przypadku, gdy wymagają tego obowiązujące przepisy prawa i wytyczne Prezesa Urzędu Ochrony Danych Osobowych.

26. Audyt bezpieczeństwa informacji (KRI)

1. Administrator zapewnia przeprowadzenie okresowego audytu wewnętrznego w zakresie bezpieczeństwa informacji nie rzadziej niż raz na rok lub częściej zgodnie z powszechnie obowiązującymi w tym zakresie przepisami.
2. Administrator dokumentuje wyniki wykonanego audytu w postaci sprawozdania.

POSTANOWIENIA KOŃCOWE

1. Każda osoba mająca dostęp do danych osobowych w Szkole zobowiązana jest zapoznać się z niniejszą Polityką oraz potwierdzić to oświadczeniem w zał. nr 5.
2. Niniejsza Polityka winna podlegać przeglądom dokonywanym we współpracy z Inspektorem Ochrony Danych na polecenie Administratora.
3. Dokument Polityki przechowywany jest w wersji tradycyjnej (papierowej) i Administrator udostępnia niniejszą Politykę każdemu Użytkownikowi na żądanie.