Załącznik nr 1

POLITYKA BEZPIECZEŃSTWA INFORMACJI
W
ZESPOLE SZKÓŁ OGÓLNOKSZTAŁCACYCH
W PŁOŃSKU

PODSTAWA PRAWNA

1. Konstytucja RP (art. 47 i 51).
2. Konwencja nr 108 Rady Europy – dotycząca ochrony osób w związku z automatycznym przetwarzaniem danych osobowych.
3. Dyrektywa PE i RE z dnia 24 października 1995 r. (95/46/EC) w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych oraz swobodnego przepływu tych danych.
4. Ustawa o ochronie danych osobowych z dnia 29 sierpnia 1997 r. (Dz. U. z 2016 poz. 677).
5. Rozporządzenie MSWiA z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. z 2004 r. Nr 100 poz. 1024).

PODSTAWOWE POJĘCIA

§ 1

1. ZSO– w tym dokumencie jest rozumiana, jako Zespół szkół Ogólnokształcących, ul. Płocka 56, 09-100 Płońsk
2. Polityka – w tym dokumencie jest rozumiana jako „Polityka bezpieczeństwa” obowiązująca w ZSO w Płońsku.
3. Administrator Bezpieczeństwa Informacji (ABI) – osoba wyznaczona przez Administratora Danych Osobowych(Dyrektor ZSO w Płońsku) do nadzorowania przestrzegania zasad ochrony danych osobowych, oraz przygotowania dokumentów wymaganych przez przepisy ustawy o ochronie danych osobowych w ZSO. ABI powołany jest Zarządzenia Dyrektora ZSO w Płońsku.
4. Użytkownik – osoba upoważniona do przetwarzania danych osobowych. Użytkownikiem może być osoba zatrudniona, wykonująca pracę na podstawie umowy zlecenia lub innej umowy cywilno-prawnej, odbywająca staż.
5. Przetwarzanie danych – rozumie się to w tym dokumencie, jako jakiekolwiek operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie.
6. Zabezpieczenie danych – wdrożenie i wykorzystywanie stosownych środków technicznych i organizacyjnych zapewniających ochronę danych przed ich nieuprawnionym przetwarzaniem.

POLITYKA BEZPIECZEŃSTWA DANYCH OSOBOWYCH

I.1. Wykaz budynków, w których przetwarzane są dane osobowe

§ 2

ADRES – BUDYNEK	POMIESZCZENIA
ul. Płocka 56, 09-100 Płońsk	Szkoła
ul. Płocka 56a, 09-100 Płońsk	Internat

I.2 System przetwarzania danych osobowych

§ 3

W skład systemu wchodzą:

1) dokumentacja papierowa
2) wydruki komputerowe;
3) procedury przetwarzania danych, w tym procedury awaryjne.

I.2.1 Cele i zasady funkcjonowania polityki bezpieczeństwa

§ 4

Realizując Politykę bezpieczeństwa informacji zapewnia ich:

1) poufność – informacja nie jest udostępniana lub ujawniana nieupoważnionym osobom, podmiotom i procesom;
2) integralność – dane nie zostają zmienione lub zniszczone w sposób nie autoryzowany;
3) dostępność – istnieje możliwość wykorzystania ich na żądanie, w założonym czasie, przez autoryzowany podmiot;
4) rozliczalność – możliwość jednoznacznego przypisania działań poszczególnym osobom;
5) autentyczność – zapewnienie, że tożsamość podmiotu lub zasobu jest taka, jak deklarowana;
6) niezaprzeczalność – uczestnictwo w całości lub części wymiany danych przez jeden z podmiotów uczestniczących w tej wymianie jest niepodważalne;
7) niezawodność – zamierzone zachowania i skutki są spójne.

§ 5

Polityka bezpieczeństwa informacji w ZSO w Płońsku ma na celu zredukowanie możliwości wystąpienia negatywnych konsekwencji naruszeń w tym zakresie, to jest:

1) naruszeń danych osobowych rozumianych jako prywatne dobro powierzone ZSO;
2) naruszeń przepisów prawa oraz innych regulacji;
3) utraty lub obniżenia reputacji;
4) strat finansowych ponoszonych w wyniku nałożonych kar.

§ 6

Realizując politykę bezpieczeństwa w zakresie ochrony danych osobowych ADO dokłada szczególnej staranności w celu ochrony interesów osób, których dane dotyczą, a w szczególności zapewnia, aby dane te były:

1) przetwarzane zgodnie z prawem,
2) zbierane dla oznaczonych, zgodnych z prawem celów i nie poddawane dalszemu przetwarzaniu niezgodnemu z tymi celami,
3) merytorycznie poprawne i adekwatne w stosunku do celu, w jakim są przetwarzane,
4) przechowywane w postaci umożliwiającej identyfikację osób, których dotyczą, nie dłużej niż jest to niezbędne do osiągnięcia celu przetwarzania.

I.2.2 Kompetencje i odpowiedzialność w zarządzaniu bezpieczeństwem danych osobowych

§ 7

Za przetwarzanie danych osobowych niezgodnie z prawem, celami przetwarzania lub przechowywanie ich w sposób niezapewniający ochrony interesów osób, których te dane dotyczą grozi odpowiedzialność karna wynikająca z przepisów ustawy o ochronie danych osobowych lub pracownicza na zasadach określonych w kodeksie pracy lub kodeksie cywilnym

§ 8

Administrator Danych Osobowych (ADO) – Dyrektor ZSO w Płońsku:

1) formułuje i wdraża warunki techniczne i organizacyjne służące ochronie danych osobowych przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem,
2) decyduje o zakresie, celach oraz metodach przetwarzania i ochrony danych osobowych,
3) odpowiada za zgodne z prawem przetwarzanie danych osobowych w ZSO.

§ 9

Administrator Bezpieczeństwa Informacji (ABI) – osoba wyznaczona przez Dyrektora ZSO w Płońsku :

1) egzekwuje zgodnie z prawem przetwarzanie danych osobowych w ZSO w imieniu ADO; wydaje upoważnienie do przetwarzania danych osobowych określając w nich zakres i termin ważności – wzór upoważnienia określa **załącznik nr 1;**
2) prowadzi ewidencji osób upoważnionych do przetwarzania danych osobowych – wzór rejestru określa **załącznik nr 2;**
3) ewidencjonuje oświadczenia osób upoważnionych o zaznajomieniu się z zasadami zachowania bezpieczeństwa danych – wzór oświadczenia określa **załącznik nr 3;**
4) prowadzi rejestr zbiorów danych osobowych, według wzoru określonego **w załączniku nr 7;**
5) określa potrzeby w zakresie stosowanych w ZSO zabezpieczeń, wnioskuje do ADO o zatwierdzenie proponowanych rozwiązań i nadzoruje prawidłowość ich wdrożenia;
6) udziela wyjaśnień i interpretuje zgodność stosowanych rozwiązań w zakresie ochrony danych osobowych z przepisami prawa;
7) bierze udział w podnoszeniu świadomości i kwalifikacji osób przetwarzających dane osobowe w ZSO i zapewnia odpowiedni poziom przeszkolenia w tym zakresie.

I.2.3 Zasady udzielania dostępu do danych osobowych

§ 10

Dostęp do danych osobowych może mieć wyłącznie osoba zaznajomiona z przepisami ustawy o ochronie danych osobowych oraz zasadami zawartymi w obowiązującej w ZSO polityce bezpieczeństwa i instrukcji zarządzania systemem informatycznym . Osoba zaznajomiona z zasadami ochrony danych potwierdza to w pisemnym oświadczeniu.

§ 11

Dostęp do danych osobowych może mieć wyłącznie osoba posiadająca pisemne oraz imienne upoważnienie wydane przez ABI.

§ 12

ABI może wyznaczyć upoważnionych do przetwarzania danych osobowych pracowników ZSO do nadzoru nad upoważnionymi pracownikami podmiotów zewnętrznych lub innymi upoważnionymi osobami przetwarzającymi dane osobowe w ZSO.

I.2.4 Udostępnianie i powierzanie danych osobowych

§ 13

Dane osobowe mogą być udostępnione osobom i podmiotom z mocy przepisów prawa lub jeżeli w sposób wiarygodny uzasadnią one potrzebę ich posiadania, a ich udostępnienie nie naruszy praw i wolności osób, których one dotyczą.

§ 14

Udostępnienie danych może nastąpić na pisemny wniosek zawierający następujące elementy:

1) adresat wniosku (administrator danych),
2) wnioskodawca,
3) podstawa prawna (wskazanie potrzeby),
4) wskazanie przeznaczenia,
5) zakres informacji.

§ 15

Administrator odmawia udostępnienia danych jeżeli spowodowałoby to naruszenie dóbr osobistych osób, których dane dotyczą lub innych osób.

§ 16

Powierzenie danych może nastąpić wyłącznie w drodze pisemnej umowy, w której podmiot przyjmujący dane zobowiązuje się do przestrzegania obowiązujących przepisów ustawy o ochronie danych osobowych. Umowa powinna zawierać informacje o podstawia prawnej powierzenia danych, celu i sposobie ich przetwarzania.

§ 17

Każda osoba fizyczna, której dane przetwarzane są w ZSO, ma prawo zwrócić się z wnioskiem o udzielenie informacji związanych z przetwarzaniem tych danych, prawo do kontroli i poprawiania swoich danych osobowych, a także w przypadkach określonych w art. 32 ust 1 pkt 7 i 8 ustawy o ochronie danych osobowych prawo wniesienia umotywowanego żądania zaprzestania przetwarzania danych oraz sprzeciwu wobec przekazywania ich innym podmiotom.

§ 18

Sprawy związane z udzielaniem informacji w tym zakresie prowadzi ABI, udzielając informacji o zawartości zbioru danych na piśmie zgodnie ze wzorem w **załączniku nr 4**.

I.2.5 Bezpieczeństwo w przetwarzaniu danych osobowych w formie tradycyjnej

§ 19

Pomieszczenia, w których znajdują się przetwarzane zbiory danych osobowych pozostają zawsze pod nadzorem upoważnionego do ich przetwarzania pracownika. Opuszczenie pomieszczenia, w których znajdują się zbiory danych osobowych musi być poprzedzone zamknięciem zbioru danych w szafie na klucz. Przy planowanej dłuższej nieobecności pracownika pomieszczenie winno być zamknięte na klucz.

§ 20

Klucze do szaf, w których przechowywane są dane osobowe mają jedynie pracownicy upoważnieni do przetwarzania danych osobowych w zakresie zgodnym z kategorią danych.

§ 21

Monitoring prowadzony jest przez Zespół Szkół Ogólnokształcących w Płońsku w celu zapewnienia bezpieczeństwa i porządku publicznego oraz ochrony osób i mienia. Obejmuje budynki szkoły, chodnik przed wejściem do szkoły, internat i miejsce rekreacyjne przy hali sportowej.

§ 22

Korzystanie ze zbiorów danych osobowych przez osoby niezatrudnione w ZSO powinno odbywać się po uzyskaniu upoważnienia lub skonsultowane z ABI w przypadku osób upoważnionych do przetwarzania tych danych na podstawie ogólnie obowiązujących przepisów.

I.3 Analiza ryzyka związanego z przetwarzaniem danych osobowych

I.3.1 Identyfikacja zagrożeń

§ 23

FORMA PRZETWARZANIA DANYCH	ZAGROŻENIA
dane przetwarzane w sposób tradycyjny	- oszustwo, kradzież, sabotaż; - zdarzenia losowe (pożar); - zaniedbania pracowników ZSO (niedyskrecja, udostępnienie danych osobie nieupoważnionej); - niekontrolowana obecność nieuprawnionych osób w obszarze przetwarzania; - pokonanie zabezpieczeń fizycznych; - podsłuchy, podglądy; - ataki terrorystyczne; - brak rejestrowania udostępniania danych; - niewłaściwe miejsce i sposób przechowywania. dokumentacji;

dane przetwarzane w systemach informatycznych	- oszustwo, kradzież, sabotaż; - **z**aniedbania pracowników ZSO (niedyskrecja, udostępnienie danych osobie nieupoważnionej); - niekontrolowana obecność nieuprawnionych osób w obszarze przetwarzania; - pokonanie zabezpieczeń informatycznych; - podsłuchy, podglądy; - ataki terrorystyczne; - pozostawienie sprzętu bez wylogowania się.

I.6.2 Sposób zabezpieczenia danych

§ 24

FORMA PRZETWARZANIA DANYCH	**STOSOWANE ŚRODKI OCHRONY**
dane przetwarzane w systemach informatycznych	- przetwarzanie danych osobowych tylko w komputerach specjalnie do tego przystosowanych, - zastosowanie haseł w dostępie do komputera; - przetwarzanie danych wyłącznie przez osoby posiadających upoważnienie nadane przez ABI; - zapoznanie pracowników z zasadami przetwarzania danych osobowych oraz obsługą - monitoring wizyjny
dane przetwarzane w sposób tradycyjny	- przechowywanie danych w pomieszczeniach zamykanych na zamki, - przechowywanie danych osobowych w szafach zamykanych na klucz, - osoby z ochrony wydające klucze tylko osobom upoważnionym, - przetwarzanie danych wyłącznie przez osoby posiadających upoważnienie nadane przez ABI, - zapoznanie pracowników z zasadami przetwarzania danych osobowych oraz obsługą systemu służącego do ich przetwarzania, - monitoring wizyjny

I.3.3 Określenie wielkości ryzyka

§ 25

Poziom ryzyka naruszenia bezpieczeństwa danych jest niski. Zastosowane techniczne i organizacyjne środki ochrony są adekwatne do stwierdzonego poziomu ryzyka dla poszczególnych systemów, rodzajów zbiorów i kategorii danych osobowych.

I.3.4 Identyfikacja obszarów wymagających szczególnych zabezpieczeń

§ 26

Uwzględniając kategorie przetwarzanych danych oraz zagrożenia zidentyfikowane w wyniku przeprowadzonej analizy ryzyka, stosuje się wysoki poziom bezpieczeństwa. ABI przeprowadza okresową analizę ryzyka dla poszczególnych systemów i na tej podstawie przedstawiają ADO propozycje dotyczące zastosowania środków technicznych i organizacyjnych, celem zapewnienia właściwej ochrony przetwarzanym danym.

INSTRUKCJA POSTĘPOWANIA W SYTUACJI NARUSZENIA DANYCH

II.1 Istota naruszenia danych osobowych

§ 27

Naruszeniem danych osobowych jest każdy stwierdzony fakt nieuprawnionego ujawnienia danych osobowych, udostępnienia lub umożliwienia dostępu do nich osobom nieupoważnionym, zabrania danych przez osobę nieupoważnioną, uszkodzenia jakiegokolwiek elementu systemu, a w szczególności:

1) nieautoryzowany dostęp do danych;
2) nieautoryzowane modyfikacje lub zniszczenie danych;
3) udostępnienie danych nieautoryzowanym podmiotom;
4) nielegalne ujawnienie danych;
5) pozyskiwanie danych z nielegalnych źródeł.

II.2 Postępowanie w przypadku naruszenia danych osobowych

§ 28

Każdy pracownik oraz osoba pracująca na podstawie umowy cywilnej lub cywilno-prawnej w ZSO, który stwierdzi fakt naruszenia bezpieczeństwa danych przez osobę przetwarzającą dane osobowe, bądź posiada informację mogącą mieć wpływ na bezpieczeństwo danych osobowych jest zobowiązany niezwłocznie zgłosić to ABI.

§ 29

Każdy pracownik oraz osoba pracująca na podstawie umowy cywilnej lub cywilno-prawnej w ZSO, który stwierdzi fakt naruszenia bezpieczeństwa danych ma obowiązek podjąć czynności niezbędne do powstrzymania skutków naruszenie ochrony oraz ustalić przyczynę i sprawcę naruszenia ochrony.

§ 30

W przypadku stwierdzenia naruszenia bezpieczeństwa danych należy zaniechać wszelkich działań mogących utrudnić analizę wystąpienia naruszenia i udokumentowanie zdarzenia oraz nie opuszczać bez uzasadnionej potrzeby miejsca zdarzenia do czasu przybycia ABI.

§ 31

ABI podejmuje następujące kroki:

1) zapoznaje się z zaistniałą sytuacją i wybiera sposób dalszego postępowania uwzględniając zagrożenie w prawidłowości pracy ZSO;
2) może zażądać dokładnej relacji z zaistniałego naruszenia bezpieczeństwa danych osobowych od osoby powiadamiającej, jak również od każdej innej osoby, która może posiadać informacje w związku z zaistniałym naruszeniem;
3) rozważa celowość i potrzebę powiadamiania o zaistniałym naruszeniu ADO, nawiązuje kontakt ze specjalistami spoza urzędu (jeśli zachodzi taka potrzeba).

§ 32

ABI dokumentuje zaistniały przypadek naruszenia bezpieczeństwa danych osobowych sporządzając raport wg wzoru stanowiącego **załącznik nr 5** i przekazuje go ADO.

§ 33

ABI zasięga potrzebnych mu opinii i proponuje działania naprawcze (w tym także ustosunkowuje się do kwestii ewentualnego odtworzenia danych z zabezpieczeń oraz terminu wznowienia przetwarzania danych osobowych).

II.3 Sankcje karne

§ 34

Wobec osoby, która w przypadku naruszenia ochrony danych osobowych nie podjęła działania określonego w niniejszym dokumencie, a w szczególności nie powiadomiła odpowiedniej osoby zgodnie z określonymi zasadami wszczyna się postępowanie dyscyplinarne.

§ 35

Kara dyscyplinarna, wobec osoby uchylającej się od powiadomienia o naruszeniu danych osobowych nie wyklucza odpowiedzialności karnej tej osoby zgodnie z ustawą o ochronie danych osobowych.

Załączniki

Załącznik nr 1 – Upoważnienie do przetwarzania danych osobowych.

Załącznik nr 2 – Rejestr osób upoważnionych do przetwarzania danych osobowych.

Załącznik nr 3 – Oświadczenie pracownika dotyczące ochrony danych osobowych .

Załącznik nr 4 – Informacja o zawartości zbioru danych.

Załącznik nr 5 – Raportu z naruszenia bezpieczeństwa danych osobowych.

Załącznik nr 6 – Oświadczenia o zgodzie na przetwarzanie danych osobowych ucznia oraz wizerunku

Załącznik nr 7 – Oświadczenia o zgodzie na przetwarzanie danych osobowych oraz wizerunku

Załącznik nr 8 - Rejestr zbiorów danych osobowych.

Załącznik nr 1

……, dnia ……

UPOWAŻNIENIE NR……./20….

DO PRZETWARZANIA DANYCH OSOBOWYCH

Działając na podstawie art. 37 Ustawy o ochronie danych osobowych z dnia 29 sierpnia 1997 r. (t.j. Dz. U. z 2016 r. poz. 677),udziela się

Pani/Panu*

.....

(imię i nazwisko pracownika)

upoważnienia do przetwarzania danych osobowych, których Administratorem Danych jest Zespół Szkół Ogólnokształcących w Płońsku zawartych w zbiorze/zbiorach*:

……

Jest Pan/Pani* upoważniony/upoważniona* do przetwarzania danych osobowych wyłącznie w zakresie wynikającym z zadań oraz poleceń przełożonego.
Zobowiązuję Panią/Pana do zachowania tajemnicy o danych znajdujących się w w/w zbiorach, jak i sposobach ich zabezpieczenia. Obowiązek ten istnieje również po ustaniu zatrudnienia.

Upoważnienie traci ważność z chwilą ustania stosunku pracy.

.....

(data i podpis Administratora Bezpieczeństwa Informacji)

---

* niepotrzebne skreślić

Załącznik nr 2

REJESTR OSÓB UPOWAŻNIONYCH DO PRZETWARZANIA DANYCH OSOBOWYCH

L.p.	Imię i nazwisko	Zakres upoważnienia do przetwarzania danych osobowych	Data nadania uprawnień	Data odebrania uprawnień	Uwagi

Załącznik nr 3

.....
(data)

……
(imię i nazwisko)

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 wykonywaniem zadań i obowiązków służbowych wynikających ze stosunku pracy, zarówno w czasie trwania umowy, jak i po jej ustaniu.

Oświadczam, że zapoznałem/am się z obowiązującymi w ZSO w Płońsku zasadami dotyczącymi przetwarzania danych osobowych, określonymi w „Polityce bezpieczeństwa informacji w Zespole Szkół Ogólnokształcących w Płońsku" oraz „Instrukcji zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych" i zobowiązuję się ich przestrzegać. W szczególności oświadczam, że bez upoważnienia nie będę wykorzystywał/a danych osobowych ze zbiorów znajdujących się w ZSO.

Zapoznałem/am się z przepisami Ustawy o ochronie danych osobowych (Dz. U. 2016 r. poz. 677) oraz Rozporządzenia MSWiA w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. z 2004 r. Nr 100 poz. 1024). Niezależnie od odpowiedzialności karnej przewidzianej w wymienionych przepisach, mam świadomość, ze złamanie zasad ochrony danych osobowych, obowiązujących w ZSO w Płońsku może zostać uznane za ciężkie naruszenie podstawowych obowiązków pracowniczych i skutkować odpowiedzialnością dyscyplinarną.

……
(podpis osoby upoważnionej)

Załącznik nr 4

……, dnia …… r.

.....
(pieczęć ZSO)

..... …….
(imię i nazwisko)

..... …….

..... ……
(adres)

INFORMACJA
o zawartości zbioru danych osobowych

W związku z Pani/Pana wnioskiem z dnia …… r. o udzielenie informacji związanych z przetwarzaniem danych osobowych w Zespole Szkół Ogólnokształcących w Płońsku działając na podstawie art. 33 ust. 1 Ustawy o ochronie danych osobowych informuję, że zbiór danych zawiera następujące Pani/Pana dane osobowe: ……

Powyższe dane przetwarzane są w Zespole Szkół Ogólnokształcących w Płońsku w celu …… z zachowaniem wymaganych zabezpieczeń i zostały uzyskane …….. *(podać sposób)*.

Powyższe dane nie były / były udostępniane …….. *(podać komu)* w celu …… *(podać cel przekazania danych)*.

Zgodnie z rozdziałem 4 ustawy o ochronie danych osobowych przysługuje Pani/Panu prawo do kontroli danych osobowych, prawo ich poprawiania, a także w przypadkach określonych w art. 32 ust. 1 pkt 7 i 8 ustawy, prawo wniesienia umotywowanego żądania zaprzestania przetwarzania danych oraz prawo sprzeciwu wobec przetwarzania danych w celach marketingowych lub wobec przekazywania danych innemu administratorowi danych osobowych.

.....
(podpis Administratora Bezpieczeństwa Informacji)

Załącznik nr 5

……., dnia …… r.

.....
(pieczęć ZSO)

RAPORT Z NARUSZENIA BEZPIECZEŃSTWA DANYCH OSOBOWYCH W ZESPOLE SZKÓŁ OGÓLNOKSZTAŁCĄCYCH W PŁOŃSKU

1. Data: ..... r. Godzina: .....
2. Osoba powiadamiająca o zaistniałym zdarzeniu: .....
   .....
   (imię, nazwisko, stanowisko służbowe, nazwa użytkownika - jeśli występuje)
3. Lokalizacja zdarzenia: .....
   .....
   (np. nr pokoju, nazwa pomieszczenia)
4. Rodzaj naruszenia bezpieczeństwa oraz okoliczności towarzyszące:
   .....
   .....
   .....
5. Przyczyny wystąpienia zdarzenia:
   .....
   .....
6. Podjęte działania:
   .....
   .....
7. Postępowanie wyjaśniające:
   .....
   .....
   .....

.....
(podpis Administratora Bezpieczeństwa Informacji)

Załącznik nr 6

……, dnia …… r.

OŚWIADCZENIE

Zgodnie z art. 24 ust. 1 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych wyrażam zgodę na przetwarzanie moich danych osobowych/mojego dziecka* ……(*imię i nazwisko ucznia*) przez administratora: Zespół Szkół O*gólnokształ*cących zlokalizowany w Płońsku, ul. Płocka 56, w celu prowadzenia działań edukacyjnych, kulturalnych i sportowych szkoły, promocji osiągnięć i utrwalania pozytywnego wizerunku placówki oraz dla zapewnienia bezpieczeństwa i porządku publicznego oraz ochrony osób i mienia.

Dane będą przetwarzane w zbiorze danych osobowych o nazwie:
……

Wiem, że podanie danych jest dobrowolne oraz, że mam prawo dostępu do treści swoich danych i ich poprawiania.
Informuję, że wyrażona zgoda może zostać w każdym czasie odwołana.

……..
(podpis pełnoletniego ucznia lub rodziców/opiekunów)

*niepotrzebne skreślić

OŚWIADCZENIE

Wyrażam zgodę na wykorzystanie mojego wizerunku/mojego dziecka* ……(*imię i nazwisko ucznia*) przez administratora: Zespół Szkół O*gólnokształ*cących zlokalizowany w Płońsku, ul. Płocka 56, w celu prowadzenia działań edukacyjnych, kulturalnych i sportowych szkoły, promocji osiągnięć placówki oraz dla zapewnienia bezpieczeństwa i porządku publicznego oraz ochrony osób i mienia.

……..
(podpis pełnoletniego ucznia lub rodziców/opiekunów)

Załącznik nr 7

……, dnia ……

……
(Imię i nazwisko)

OŚWIADCZENIE

Zgodnie z art. 24 ust. 1 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych wyrażam zgodę na przetwarzanie moich danych osobowych przez administratora: Zespół Szkół Ogólnokształcących zlokalizowany w Płońsku, ul. Płocka 56, w celu:
……

Dane będą przetwarzane w zbiorze danych osobowych o nazwie:
……..

Wiem, że podanie danych jest dobrowolne oraz, że mam prawo dostępu do treści swoich danych i ich poprawiania.

Informuję, że wyrażona zgoda może zostać w każdym czasie odwołana.

.....
(podpis)