ZESPÓŁ SZKÓŁ ZAWODOWYCH
im. Stefana Bobrowskiego
ul. Gen. J. Hallera 12
63-900 RAWICZ

ZARZĄDZENIE Nr ZSZ-0132-12/2022

Dyrektora Zespołu Zawodowych w Rawiczu

z dnia 19 kwietnia 2022 r.

w sprawie wprowadzenia procedur ochrony danych osobowych w Zespole Szkół Zawodowych w Rawiczu

Na podstawie art. 68 ust. 1 pkt. 1 ustawy z dnia 14 grudnia 2016 roku Prawo oświatowe (Dz. U. z 2020r., poz. 910),w związku z art. 2 oraz art. 3, a także art. 24 ust. 1 i 2 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L z 4.05.2016, str. 1-88), zwanego dalej RODO, a także w związku z art. 1 ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz. U. z 2019 r., poz. 1781), zarządzam, co następuje:

§ 1

Przetwarzanie danych osobowych w Zespole Szkół Zawodowych w Rawiczu służy realizacji obowiązków oraz uprawnień określonych przepisami prawa, w szczególności zadań statutowych szkoły, wynikających z ustawy z dnia 14 grudnia 2016r. Prawo oświatowe (Dz. U. z 2020r. poz. 910).

§ 2

1. Słownik pojęć

Ilekroć w zarządzeniu jest mowa o:

1) danych osobowych - rozumie się przez to wszelkie 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, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej;
2) przetwarzaniu - rozumie się przez to operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taką 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;

3) profilowaniu - rozumie się przez to dowolną formę zautomatyzowanego przetwarzania danych osobowych, które polega na wykorzystaniu danych osobowych do oceny niektórych czynników osobowych osoby fizycznej, w szczególności do analizy lub prognozy aspektów dotyczących efektów pracy tej osoby fizycznej, jej sytuacji ekonomicznej, zdrowia, osobistych preferencji, zainteresowań, wiarygodności, zachowania, lokalizacji lub przemieszczania się;
4) Szkole (ZSZ) - rozumie się przez to Zespół Szkół Zawodowych w Rawiczu;
5) administratorze danych osobowych (ADO) - rozumie się przez to Zespół Szkół Zawodowych w Rawiczu, zwanym dalej Szkołą, obowiązki administratora pełni Dyrektor Zespołu Szkół Zawodowych w Rawiczu, zwany dalej Dyrektorem;
6) podmiocie przetwarzającym - rozumie się przez to osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który przetwarza dane osobowe w imieniu administratora;
7) odbiorcy - rozumie się przez to osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, któremu ujawnia się dane osobowe, niezależnie od tego, czy jest stroną trzecią. Organy publiczne, które mogą otrzymywać dane osobowe w ramach konkretnego postępowania zgodnie z prawem Unii lub prawem państwa członkowskiego, nie są jednak uznawane za odbiorców; przetwarzanie tych danych przez te organy publiczne musi być zgodne z przepisami o ochronie danych mającymi zastosowanie stosownie do celów przetwarzania;
8) zgodzie osoby, której dane dotyczą - rozumie się przez to 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;
9) pracowniku - rozumie się przez to osoby zatrudnione w jednostce na podstawie umowy o pracę, umowy cywilnoprawne, stażystów;
10) naruszeniu ochrony danych osobowych - rozumie się przez to 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;
11) administratorze systemu informatycznego (ASI) - rozumie się przez to osobę

odpowiadającą za funkcjonowanie i bezpieczeństwo systemu informatycznego, zawierającego programy lub bazy danych zastosowane do przetwarzania danych osobowych, również w przypadku dostępu zdalnego i mobilnego do systemu, w szczególności z użyciem sieci Internet lub radiowej sieci bezprzewodowej, w tym z użyciem prywatnych urządzeń użytkowników, w sytuacjach gdy zostało to dozwolone przez administratora;

§ 3

1. Zespół Szkół Zawodowych w Rawiczu jest administratorem danych, w rozumieniu art. 4 pkt 7 RODO. Wobec innych administratorów, którzy powierzyli Szkole dane do przetwarzania, jest podmiotem przetwarzającym.
2. Dyrektor jest osobą podejmującą decyzje w sprawach przetwarzania danych osobowych w imieniu administratora danych.

§ 4

Dyrektor zobowiązuje do przestrzegania zasad dotyczących przetwarzania danych osobowych określonych w RODO oraz powierza realizację obowiązków w zakresie przetwarzania danych osobowych wynikających z RODO i innych przepisów o ochronie danych osobowych wszystkim pracownikom, stażystom oraz osobom i podmiotom współpracującym, biorącym udział w czynnościach przetwarzania danych osobowych.

§ 5

1. Dyrektor pełni obowiązki administratora danych, a także Szkoły jako podmiotu przetwarzającego, wynikające z RODO i innych przepisów o ochronie danych osobowych, w zakresie nadzoru, m.in. nad przestrzeganiem zasad przetwarzania danych osobowych, w tym zasady rozliczalności (możliwości wykazania, że przepisy są przestrzegane), praw osób, których dane dotyczą, zagadnień związanych z administratorem i podmiotami przetwarzającymi, określonych w Rozdziale IV RODO oraz przekazywaniem danych osobowych do państw trzecich lub organizacji międzynarodowych.
2. Członkowie organów kolegialnych i innych zespołów powołanych przez organy Szkoły upoważnieni są do przetwarzania danych osobowych w zakresie niezbędnym do pełnienia swych funkcji oraz zobowiązani do zachowania tajemnicy tych danych. Nad obowiązkiem ochrony danych osobowych podczas obrad organów kolegialnych i innych zespołów czuwa ich przewodniczący.
3. Osoby prowadzące zajęcia dydaktyczne w Szkole, są upoważnione do przetwarzania danych osobowych uczniów, rodziców, opiekunów prawnych, w zakresie niezbędnym dopełnienia swych zadań oraz zobowiązane są do zachowania w tajemnicy pozyskanych danych.
4. Przekazanie konkretnych zadań wskazanym wyżej osobom traktowane jest jak

polecenie przetwarzania, w rozumieniu art. 29 RODO, wydane przez administratora.

§ 6

1. Dyrektor wyznacza inspektora ochrony danych, który podlega mu bezpośrednio.
2. Inspektor ochrony danych ma, w szczególności, następujące zadania:

1) informowanie administratora, administratorów systemów informatycznych, administratorów sieci komputerowych, pracowników przetwarzających dane osobowe oraz podmiotów przetwarzających o obowiązkach spoczywających na nich na mocy rozporządzenia RODO oraz innych przepisów Unii lub państw członkowskich o ochronie danych i doradzanie im w tej sprawie;
2) sprawowanie stałej kontroli i sprawdzanie zgodności procesów przetwarzania danych osobowych z przepisami regulującymi zasady ochrony danych osobowych;
3) monitorowanie przestrzegania rozporządzenia RODO, innych przepisów Unii lub państw członkowskich o ochronie danych oraz polityk administratora lub podmiotu przetwarzającego w dziedzinie ochrony danych osobowych, w tym monitorowanie podziału obowiązków, działań zwiększających świadomość, szkoleń personelu uczestniczącego w operacjach przetwarzania oraz powiązane z tym audyty;
4) organizowanie szkoleń personelu uczestniczącego w operacjach przetwarzania danych osobowych;
5) udzielanie na żądanie administratora, administratorów lokalnych, administratorów systemów informatycznych oraz administratorów sieci komputerowej zaleceń codo oceny skutków dla ochrony danych oraz monitorowanie jej realizacji;
6) współpraca z organem nadzorczym;
7) pełnienie funkcji punktu kontaktowego dla organu nadzorczego w kwestiach związanych z przetwarzaniem, w tym z uprzednimi konsultacjami, o których mowa w art. 36 RODO, oraz w stosownych przypadkach prowadzenie konsultacji we wszelkich innych sprawach;
8) pełnienie funkcji punktu kontaktowego dla osób, których dane przetwarzane są w Szkole;
9) prowadzenie ewidencji osób upoważnionych do przetwarzania danych osobowych;

3. Inspektor ochrony danych upoważniony jest do przetwarzania danych osobowych w zakresie niezbędnym do pełnienia swej funkcji oraz zobowiązany do zachowania tajemnicy tych danych.

§ 7

1. W Szkole prowadzony jest rejestr czynności przetwarzania, w którym inwentaryzuje i monitoruje sposób, w jaki przetwarzane są dane osobowe, zgodnie ze strukturą i zawartością pól informacyjnych określonymi w Załączniku Nr 9 i zawierający następujące informacje,

wymagane przez RODO::

1) nazwa oraz dane kontaktowe administratora oraz wszelkich współadministratorów, w rozumieniu art. 26 RODO, a także inspektora ochrony danych;
2) cele przetwarzania;
3) opis kategorii osób, których dane dotyczą oraz kategorii danych osobowych;
4) kategorie odbiorców, którym dane osobowe zostały lub zostaną ujawnione, w tym odbiorców w państwach trzecich lub w organizacjach międzynarodowych;
5) 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;
6) jeżeli jest to możliwe, planowane terminy usunięcia poszczególnych kategorii danych;
7) jeżeli jest to możliwe, ogólny opis technicznych i organizacyjnych środków bezpieczeństwa, o których mowa w art. 32 ust. 1 RODO.

2. Rejestr stanowi formę dokumentowania czynności przetwarzania danych i jest jednym z kluczowych elementów umożliwiających Szkole rozliczanie większości obowiązków ochrony danych czyli realizację fundamentalnej zasady, na której opiera się cały system ochrony danych osobowych - zasady rozliczalności.
3. Szkoła jako podmiot przetwarzający prowadzi rejestr kategorii czynności przetwarzania dokonywanych w imieniu innego administratora zgodnie ze strukturą i zawartością pól informacyjnych określonymi w Załączniku Nr 10 i zawierający następujące informacje, wymagane przez RODO:

1) nazwa oraz dane kontaktowe administratora lub podmiotów przetwarzających oraz każdego administratora, w imieniu którego działa Szkoła, a gdy ma to zastosowanie - przedstawiciela administratora oraz inspektora ochrony danych;
2) kategorie przetwarzań dokonywanych w imieniu każdego z administratorów;
3) 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;
4) jeżeli jest to możliwe, ogólny opis technicznych i organizacyjnych środków bezpieczeństwa, o których mowa w art. 32 ust. 1 RODO.

4. Szkoła dokumentuje w Rejestrze podstawy prawne przetwarzania danych dla poszczególnych czynności przetwarzania.
5. Pracownicy Szkoły mają obowiązek znać podstawy prawne, na jakich dokonują konkretnych czynności przetwarzania danych osobowych.

§ 8

Administrator realizuje obowiązki wynikające z RODO i innych przepisów o ochronie danych osobowych w zakresie przetwarzania danych osobowych. Do zadań administratora należy m.in.:

1) identyfikowanie czynności przetwarzania danych osobowych, określenie celów przetwarzania oraz podstawy prawnej przetwarzania danych osobowych a następnie powiadomienie o tym inspektora ochrony danych ze wskazaniem informacji ujętych w rejestrze, o którym mowa w § 7 ust. 1.;
2) określanie ryzyka naruszenia praw i wolności osób w procesie przetwarzania danych osobowych oraz stwarzanie warunków organizacyjnych i technicznych umożliwiających spełnienie wymogów wynikających z obowiązywania prawa, w tym RODO,
3) w przypadku konieczności powierzenia przetwarzania danych osobowych, wybór podmiotów przetwarzających, dających gwarancję przetwarzania zgodnego z RODO i zawieranie, zgodnych z wymaganiami art. 28 RODO, umów powierzenia przetwarzania;
4) niezwłoczne, nie później niż w terminie 7 dni od daty zawarcia umowy, informowanie inspektora ochrony danych o zawarciu, w podległym obszarze, umowy o powierzeniu przetwarzania danych osobowych, na podstawie której Szkoła staje się podmiotem przetwarzającym - do informacji należy dołączyć kopię umowy lub jej skan;
5) prowadzenie rejestru umów, o których mowa w pkt 3 w formie pisemnej lub elektronicznej, zawierającego co najmniej datę zawarcia umowy i jej numer, nazwę podmiotu przetwarzającego, datę rozwiązania/wygaśnięcia umowy;
6) nadawanie i odwoływanie upoważnień do przetwarzania danych osobowych, osobom przetwarzającym dane osobowe, z zachowaniem formy pisemnej, a także przekazywanie inspektorowi ochrony danych niezwłocznie, nie później niż w terminie 7 dni od zdarzenia informacji o nadaniu, odwołaniu lub modyfikacji upoważnienia do przetwarzania danych osobowych;

§ 9

1. Pracownicy Szkoły zobowiązani są do przestrzegania zasad określonych w RODO oraz realizacji obowiązków wynikających z RODO i innych przepisów o ochronie danych osobowych w zakresie przetwarzania danych osobowych.
2. W szczególności pracownicy Szkoły zobowiązani są do:

   - zapoznania się z przepisami dotyczącymi ochrony danych osobowych, w szczególności Rozporządzenia RODO i zasadami przetwarzania danych osobowych, obowiązującymi w Zespole Szkół Zawodowych w Rawiczu,
   - przestrzegania zasad określonych w RODO oraz realizacji obowiązków wynikających z RODO i innych przepisów o ochronie danych osobowych w zakresie przetwarzania danych

osobowych,

- aktywnego uczestniczenia w czynnościach służących zachowaniu bezpieczeństwa danych osobowych,
- przekazywania informacji niezbędnych do prowadzenia rejestrów, w tym Rejestru czynności przetwarzania, rejestru umów powierzenia przetwarzania,
- współdziałanie z inspektorem ochrony danych w realizowanych przez niego zadaniach,
- niezwłocznego zgłaszania podejrzenia naruszenia danych osobowych Dyrektorowi i inspektorowi ochrony danych.

§ 10

1. Szkoła zapewnia realizację obowiązków wynikających z przepisów RODO w szczególności poprzez:

1) stworzenie warunków organizacyjnych i technicznych umożliwiających spełnienie wymogów wynikających z obowiązywania prawa, w tym RODO,
2) określanie zakresu indywidualnych obowiązków, uprawnień i odpowiedzialności osób zatrudnionych przy przetwarzaniu danych osobowych, w szczególności wprowadzenie ich do opisu stanowisk i zakresu obowiązków;
3) uzyskiwanie zgód, dokumentowanie/odnotowywanie oraz przechowywanie udzielonych zgód i ewentualnego cofnięcia zgody, gdy podstawę przetwarzania stanowi zgoda osoby, której dane są zbierane, a także podejmowanie stosownych działań, w przypadku odwołania pozyskanej wcześniej zgody na przetwarzanie danych osobowych; Wzory udzielania zgody na przetwarzanie danych osobowych zawarte są w załącznikach nr 14 i nr 15 do niniejszego Zarządzenia.
4) zapoznanie osób, których dane pozyskuje Szkoła, z informacjami o przetwarzaniu, gdy zbierane są nowe dane lub gdy zmienia się cel przetwarzania, a także dokumentowanie spełnienia tego obowiązku. Zakres przekazywanych informacji i przykładowy sposób poinformowania zawarte są w „Klauzuli informacyjnej" - Załącznik Nr 21;
5) udzielanie bądź odwołanie upoważnień do przetwarzania danych osobowych dla osób przetwarzających dane osobowe, nadawanie, zgodnie z przyjętymi zasadami uprawnień w systemie informatycznym, osobom upoważnionym do przetwarzania takich danych. W przypadku wygaśnięcia upoważnienia, uprawnienia są cofane;

§ 11

1. Upoważnienie do przetwarzania danych osobowych sporządza się w dwóch

egzemplarzach. Jeden egzemplarz otrzymuje osoba upoważniona. Drugi egzemplarz, w przypadku osób upoważnionych będących pracownikami, umieszcza się w aktach osobowych, a w przypadku osób upoważnionych, które nie są pracownikami, w tym upoważnienie zawarte w umowie powierzenia przetwarzania przechowuje się w odrębnym zbiorze wraz ze stosownymi umowami.

Kopia upoważnienia przekazywana jest do inspektora ochrony danych. Wzory upoważnienia dla pracowników, umowy powierzenia przetwarzania zawarte są w Załącznikach Nr 11-13 do niniejszego zarządzenia.

2. Osoby, które zostały upoważnione do przetwarzania danych osobowych, są obowiązane przetwarzać je - jedynie na polecenie administratora danych - w zakresie nadanego upoważnienia oraz zgodnie z zasadami przetwarzania danych osobowych, a także do zachowania w tajemnicy treści danych osobowych oraz informacji o sposobach ich zabezpieczenia, również po wygaśnięciu upoważnienia.

§ 12

1. Dane osobowe mogą być udostępniane wyłącznie osobom uprawnionym.
2. Dane osobowe udostępnia się na wniosek, chyba że przepis szczególny stanowi inaczej. Wniosek powinien zawierać informacje umożliwiające wyszukanie w zbiorze żądanych danych osobowych oraz wskazywać ich zakres i przeznaczenie. Wzór wniosku stanowi Załącznik Nr 1 9do niniejszego Zarządzenia.
3. Dane osobowe udostępniane są przez pracowników po uzyskaniu pisemnej zgody Dyrektora.
4. Balcerek Grzegorz prowadzi rejestr udostępnień, w którym odnotowywane są informacje o odbiorcach i udostępnieniach danych osobowych. Wzór rejestru stanowi Załącznik Nr 20 do niniejszego Zarządzenia.

§ 13

1. W Szkole prowadzony jest rejestr naruszeń ochrony danych osobowych, zgodnie z art. 34RODO.
2. Instrukcja postępowania w sytuacji naruszenia ochrony danych osobowych w Szkole stanowi Załącznik Nr 7 do niniejszego zarządzenia.

§ 14

Zarządzenie jest dokumentem wewnętrznym i **nie podlega publikacji**.

§ 15

Traci moc Zarządzenie nr ZSZ-22/2017 z dnia 28.08.2017 r.

§ 16

Zarządzenie wchodzi w życie z dniem podpisania.

Załączniki :

1) Polityka ochrony danych osobowych w Zespole Szkół Zawodowych w Rawiczu - Załącznik Nr 1
2) Wykaz budynków i pomieszczeń w budynkach tworzących obszar przetwarzania - Załącznik Nr 2
3) Instrukcja Zarządzania Systemem Informatycznym w Zespole Szkół Zawodowych w Rawiczu - Załącznik Nr 3
4) Regulamin korzystania z Systemu Librus Synergia w Zespole Szkół Zawodowych w Rawiczu - Załącznik Nr 4
5) Podstawowe zasady dotyczące zachowania bezpieczeństwa podczas pracy zdalnej– Załącznik Nr 5
6) Plan ciągłości działania na wypadek awarii systemu informatycznego – Załącznik Nr 6
7) Instrukcja postępowania w sytuacji naruszenia ochrony danych osobowych w Zespole Szkół Zawodowych w Rawiczu – Załącznik Nr 7
8) Rejestr przypadków naruszenia lub podejrzenia naruszenia bezpieczeństwa przetwarzania danych osobowych – Załącznik Nr 8
9) Rejestr czynności przetwarzania – Załącznik Nr 9
10) Rejestr kategorii czynności przetwarzania – Załącznik Nr 10
11) Upoważnienie do przetwarzania danych osobowych– Załącznik Nr 11 - 12
12) Umowa powierzenia przetwarzania danych osobowych – Załącznik Nr 13
13) Zgoda na przetwarzanie danych osobowych – Załącznik Nr 14-15
14) Rejestr wydanych upoważnień do przetwarzania danych osobowych –Załącznik Nr 16
15) Rejestr zawartych umów powierzenia przetwarzania danych osobowych – Załącznik Nr 17
16) Rejestr udzielonych zgód na przetwarzanie danych osobowych – Załącznik Nr 18
17) Wniosek o udostępnienie danych ze zbioru danych – Załącznik Nr 19
18) Rejestr udostępnień danych osobowych – Załącznik Nr 20
19) Klauzula informacyjna – wzór ogólny – Załącznik Nr 21
20) Potwierdzenie otrzymania dostępu do kont rodzica/opiekuna i ucznia/uczennicy oraz zapoznania się z zasadami funkcjonowania dziennika elektronicznego – Załącznik Nr 22.
21) Wzór zgody na korzystanie ze sprzętu stanowiącego własność pracodawcy poza miejscem pracy - Załącznik Nr 23
22) Rejestr wydania sprzętu do korzystania poza miejscem pracy - Załącznik Nr 24

23) Regulamin korzystania z kont w usłudze G Suite przez uczniów Zespołu Szkół Zawodowych im. Stefana Bobrowskiego w Rawiczu - - Załącznik Nr 25
24) Wzór zgody rodzica lub prawnego opiekuna/pełnoletniego ucznia na korzystanie z konta GSuite - Załącznik Nr 26

p.o. DYREKTORA
mgr Daria Jagła

Zał. Nr 1 do Zarządzenia Nr .....

Dyrektora Zespołu Zawodowych
w Rawiczu

Polityka ochrony danych osobowych w Zespole Szkół Zawodowych w Rawiczu

I. Dyrektor i pracownicy Zespołu Szkół Zawodowych w Rawiczu są świadomi wagi problemów związanych z ochroną prawa do prywatności, w tym w szczególności prawa osób fizycznych, powierzających Szkole swoje dane osobowe, do właściwej i skutecznej ochrony tych danych deklaruje:

- zamiar podejmowania wszystkich działań niezbędnych dla ochrony praw i wolności jednostki związanych z przetwarzaniem i bezpieczeństwem danych osobowych,
- zamiar stałego podnoszenia świadomości oraz kwalifikacji osób przetwarzających dane osobowe w Zespole Szkół Zawodowych w Rawiczu w zakresie problematyki przetwarzania i bezpieczeństwa tych danych,
- zamiar traktowania obowiązków osób zatrudnionych przy przetwarzaniu danych osobowych jako należących do kategorii podstawowych obowiązków pracowniczych oraz stanowczego egzekwowania ich wykonania przez zatrudnione osoby.

II. Dyrektor i pracownicy Zespołu Szkół Zawodowych w Rawiczu są świadomi zagrożeń związanych z przetwarzaniem przez Szkołę danych osobowych - w tym, w szczególności, zagrożeń wynikających z dynamicznego rozwoju metod i technik przetwarzania tych danych w systemach informatycznych oraz sieciach telekomunikacyjnych. Jednocześnie Dyrektor Szkoły zamierza doskonalić i rozwijać nowoczesne metody przetwarzania danych. Deklaruje, że Zespół Szkół Zawodowych w Rawiczu będzie stale doskonalił i rozwijał organizacyjne, techniczne oraz fizyczne środki ochrony danych osobowych przetwarzanych zarówno metodami tradycyjnymi jak i elektronicznie tak, aby skutecznie zapobiegać zagrożeniom, takim jak:

1) lekceważenie zasad ochrony danych polegające na pozostawianiu pomieszczenia lub stanowiska pracy bez ich zabezpieczenia;
2) dopuszczanie osób postronnych, nieuprawnionych do przetwarzania danych, do miejsc przetwarzania;
3) niekontrolowane kopiowanie danych na dyski wymienne;

4) kradzież sprzętu lub nośników z danymi;
5) niewłaściwe przekazywanie sprzętu z danymi do serwisu, oraz innym zagrożeniom mogącym wystąpić obecnie i w przyszłości, w związku z rozwojem metod i technik przetwarzania danych.
6) niewłaściwe użytkowanie sieci społecznościowych;
7) niewłaściwe przetwarzanie „w chmurze";
8) istnienie luk w komunikatorach internetowych, przez które można uzyskać dostęp do komputera;
9) podszywanie się pod inną osobę;
10) stosowanie oprogramowania do wymiany plików, mogącego służyć do łatwego skopiowania pliku z danymi;
11) instalowanie się złośliwego oprogramowania na komputerach oraz urządzeniach mobilnych;
12) spam i sieci botnet;
13) ataki z sieci uniemożliwiające przetwarzanie danych osobowych;
14) pishing - spreparowane witryny internetowe i kradzież tożsamości;
15) podsłuchiwanie sieci, w szczególności bezprzewodowych, w celu przechwycenia haseł i danych;

III. Ustala się następujące wytyczne w zakresie ochrony danych osobowych przetwarzanych w Zespole Szkół Zawodowych w Rawiczu:

1. Zgodnie z RODO obowiązują następujące zasady dotyczące przetwarzania danych osobowych. Dane osobowe muszą być:

1) przetwarzane zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osoby, której dane dotyczą („zgodność z prawem, rzetelność i przejrzystość");
2) zbierane w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami; dalsze przetwarzanie do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych nie jest uznawane w myśl art. 89 ust. 1 RODO za niezgodne z pierwotnymi celami („ograniczenie celu");
3) adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane („minimalizacja danych");
4) prawidłowe i w razie potrzeby uaktualniane; należy podjąć wszelkie rozsądne działania, aby dane osobowe, które są nieprawidłowe w świetle celów ich przetwarzania, zostały niezwłocznie usunięte lub sprostowane („prawidłowość");
5) przechowywane w formie umożliwiającej identyfikację osoby, której dane dotyczą, przez okres nie dłuższy, niż jest to niezbędne do celów, w których dane te są

przetwarzane; dane osobowe można przechowywać przez okres dłuższy, o ile będą one przetwarzane wyłącznie do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych na mocy art. 89 ust. 1 RODO, z zastrzeżeniem że wdrożone zostaną odpowiednie środki techniczne i organizacyjne wymagane na mocy RODO w celu ochrony praw i wolności osób, których dane dotyczą („ograniczenie przechowywania");

6) przetwarzane w sposób zapewniający odpowiednie bezpieczeństwo danych osobowych, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem, za pomocą odpowiednich środków technicznych lub organizacyjnych („integralność i poufność").

Administrator jest odpowiedzialny za przestrzeganie powyższych zasad i wykonując swoje obowiązki dokłada wszelkich starań, aby wykazać ich przestrzeganie („rozliczalność"), w szczególności dokumentując podejmowane działania i podejmowane decyzje w zakresie ochrony danych osobowych.

2. Zgodnie z RODO, przetwarzanie jest zgodne z prawem wyłącznie w przypadkach, gdy - i w takim zakresie, w jakim - spełniony jest co najmniej jeden z poniższych warunków:

1) osoba, której dane dotyczą **wyraziła zgodę** na przetwarzanie swoich danych osobowych w jednym lub większej liczbie określonych celów;
2) przetwarzanie jest niezbędne do wykonania umowy, której stroną jest osoba, której dane dotyczą, lub do podjęcia działań na żądanie osoby, której dane dotyczą, przed zawarciem umowy;
3) przetwarzanie jest niezbędne do **wypełnienia obowiązku prawnego** ciążącego na administratorze;
4) przetwarzanie jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby fizycznej;
5) przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi;
6) przetwarzanie jest niezbędne do celów wynikających z prawnie uzasadnionych interesów realizowanych przez administratora lub przez stronę trzecią, z wyjątkiem sytuacji, w których nadrzędny charakter wobec tych interesów mają interesy lub podstawowe prawa i wolności osoby, której dane dotyczą, wymagające ochrony danych osobowych, w szczególności gdy osoba, której dane dotyczą, jest dzieckiem.

3. Zgodnie z przepisami RODO, zabrania się przetwarzania danych osobowych ujawniających

pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych oraz przetwarzania danych genetycznych, danych biometrycznych w celu jednoznacznego zidentyfikowania osoby fizycznej lub danych dotyczących zdrowia, seksualności lub orientacji seksualnej tej osoby.
Powyższe nie ma zastosowania, jeżeli spełniony jest jeden z warunków określonych w art. 9 ust. 2 RODO (osoba, której dane dotyczą wyraziła wyraźną zgodę na przetwarzanie tych danych; przetwarzanie jest do wypełnienia obowiązków i wykonywania szczególnych praw przez administratora lub osobę, której dane dotyczą; przetwarzanie jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby fizycznej, a osoba, której dane dotyczą, jest fizycznie lub prawnie niezdolna do wyrażenia zgody; przetwarzanie dotyczy danych osobowych w sposób oczywisty upublicznionych przez osobę, której dane dotyczą itd.).

4. Zgodnie z RODO, przetwarzania danych osobowych dotyczących wyroków skazujących oraz naruszeń prawa lub powiązanych środków bezpieczeństwa na podstawie art. 6 ust. 1 RODO wolno dokonywać wyłącznie pod nadzorem władz publicznych lub jeżeli przetwarzanie jest dozwolone prawem Unii lub prawem państwa członkowskiego przewidującymi odpowiednie zabezpieczenia praw i wolności osób, których dane dotyczą. Wszelkie kompletne rejestry wyroków skazujących są prowadzone wyłącznie pod nadzorem władz publicznych.

5. Zespół Szkół Zawodowych w Rawiczu realizując politykę ochrony, dba o prawa osób, których dane dotyczą, w szczególności poprzez:
1) przejrzystość komunikacji, co oznacza dążenie, by informacje przekazywane były w zwięzłej, przejrzystej, zrozumiałej i łatwo dostępnej formie, jasnym i prostym językiem;
2) udzielanie informacji i dostępu do danych osobowych;
3) sprostowania i usuwania danych;
4) realizację prawa do sprzeciwu wobec przetwarzania ich danych.

6. Szkoła wykonuje wszystkie obowiązki przewidziane w RODO i innych przepisach dotyczących ochrony danych, jako administrator lub współadministrator i gdy ma to zastosowanie, jako podmiot przetwarzający, w szczególności:
1) uwzględniając charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie i wadze zagrożenia, Szkoła wdraża odpowiednie środki techniczne i organizacyjne, aby przetwarzanie odbywało się zgodnie z RODO i aby móc to wykazać. Środki te są w razie potrzeby poddawane przeglądom i uaktualniane;
2) uwzględniana jest ochrona danych w fazie projektowania oraz domyślna ochrona danych;

3) podmiot przetwarzający oraz każda osoba działająca z upoważnienia Szkoły lub podmiotu przetwarzającego i mająca dostęp do danych osobowych przetwarzają je wyłącznie na polecenie Szkoły, chyba że wymaga tego prawo Unii Europejskiej lub prawo państwa członkowskiego;
4) poprzez podejście procesowe i rejestrowanie czynności przetwarzania oraz kategorii czynności przetwarzania;
5) poprzez podejście oparte na ryzyku i zapewnienie bezpieczeństwa danych osobowych, w tym:
    a) bezpieczeństwo przetwarzania;
    b) zgłaszanie naruszenia ochrony danych osobowych organowi nadzorczemu;
    c) zawiadamianie osoby, której dane dotyczą, o naruszeniu ochrony danych osobowych;
    d) ocenę skutków dla ochrony danych i uprzednie konsultacje z organem nadzorczym;
    e) wyznaczenie inspektora ochrony danych.

8. Szkoła przestrzega określonych w RODO zasad przekazywania danych osobowych do państw trzecich lub organizacji międzynarodowych.

9. Szkoła przestrzega norm prawnych, wynikających z przepisów RODO dotyczących szczególnych sytuacji związanych z przetwarzaniem oraz wszystkich innych przepisów odnoszących się do przetwarzania danych osobowych.

IV. Obszar przetwarzania

1. Zespół Szkół Zawodowych w Rawiczu, realizując politykę ochrony wyznacza budynki, pomieszczenia i części pomieszczeń, tworzące obszar Szkoły, w którym przetwarzane są dane osobowe (obszar przetwarzania). Obszar ten zabezpiecza się przed dostępem osób nieuprawnionych na czas nieobecności w nim osób upoważnionych do przetwarzania danych osobowych.

2. W budynkach, pomieszczeniach i częściach pomieszczeń, tworzących obszar przetwarzania mają prawo przebywać wyłącznie osoby upoważnione do przetwarzania danych osobowych oraz osoby sprawujące nadzór i kontrolę przetwarzania i ochrony tych danych. Osoby nieposiadające upoważnienia do przetwarzania danych osobowych, w tym osoby wykonujące czynności usługowe, w szczególności takie jak: remonty, ochrona budynku, mogą przebywać w budynkach, pomieszczeniach i częściach pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe, wyłącznie w obecności upoważnionego pracownika Szkoły lub na podstawie wydanego przez administratora danych dokumentu zezwalającego i określającego warunki przebywania w miejscach przetwarzania danych osobowych.

Zezwolenie na przebywanie w ww. pomieszczeniach i warunki przebywania mogą wynikać z umowy zawartej z podmiotem realizującym usługi.

3. Stacje robocze, monitory, drukarki oraz inne urządzenia służące do przetwarzania ,a zwłaszcza kopiowania danych, powinny być umiejscawiane w sposób uniemożliwiający osobom nieuprawnionym podgląd informacji oraz bezpośredni i niekontrolowany dostęp.

4. W przypadku dostępu zdalnego i mobilnego do systemu informatycznego, w szczególności z użyciem sieci Internet lub radiowej sieci bezprzewodowej, w tym z użyciem prywatnych urządzeń użytkowników w sytuacjach gdy zostało to dozwolone przez administratora danych, administrator systemu informatycznego określa zasady korzystania, ograniczenia dostępu do systemu do niezbędnego minimum oraz technologicznego zabezpieczenia urządzeń i dostępu do systemu.

5. Opuszczając pomieszczenie, w którym przetwarzane są dane osobowe, należy je zabezpieczyć przed wejściem osób niepowołanych.

6. W razie planowanej, choćby chwilowej, nieobecności pracownika upoważnionego do przetwarzana danych osobowych należy umieścić zbiory występujące w formach tradycyjnych (papierowych) w odpowiednio zabezpieczonym miejscu ich przechowywania oraz dokonać niezbędnych operacji w systemie informatycznym uniemożliwiających dostęp do danych osobom niepowołanym (np. w czasie nie przekraczającym 5 minut, powinny włączać się tzw. wygaszacze ekranów).

7. Opuszczenie przez pracownika przetwarzającego dane osobowe obszaru ich przetwarzania bez zabezpieczenia budynku i/lub pomieszczenia oraz umiejscowionych w nim zbiorów danych jest niedopuszczalne, i traktowane jest jako ciężkie naruszenie podstawowych obowiązków pracowniczych.

8. Przetwarzanie danych poza obszarem przetwarzania.

Przetwarzanie danych osobowych , w tym występujących w formach tradycyjnych (papierowych) poza obszarem przetwarzania może odbywać się po uzyskaniu upoważnienia wydanego przez ADO. Pracownik dokonujący przetwarzania danych poza obszarem przetwarzania zobowiązany jest do zapewnienia szczególnej ostrożności podczas ich transportu, przechowywania, przetwarzania w tym uniemożliwić dostęp do danych osobom niepowołanym i chronić przed bezprawnym zniszczeniem.

9. Wykaz budynków i pomieszczeń w których przetwarzane są dane osobowe podlegające nadzorowi Zespołu Szkół Zawodowych w Rawiczu zawiera załącznik Nr 3.

V. Niszczenie danych

1. Zespół Szkół Zawodowych w Rawiczu, realizując politykę ochrony, przykłada dużą wagę do prawidłowego niszczenia zbędnych danych osobowych, danych dla których minął okres przechowywania oraz danych co do których skutecznie wniesiono żądanie usunięcia na podstawie art. 17 RODO.

2. Niszczenie danych osobowych polega w szczególności na:

1) trwałym, fizycznym zniszczeniu danych wraz z ich nośnikami w stopniu uniemożliwiającym ich późniejsze odtworzenie przez osoby niepowołane przy zastosowaniu powszechnie dostępnych metod;
2) anonimizacji danych osobowych, polegającej na pozbawieniu danych osobowych cech pozwalających na identyfikację osób fizycznych, których dane dotyczą;
3) brakowaniu dokumentacji niearchiwalnej zgodnie z ustawą z dnia 14 lipca 1983r. o narodowym zasobie archiwalnym i archiwach (tekst jednolity Dz. U. 2018 poz.217 z późniejszymi zmianami) oraz przepisami wykonawczymi do ustawy.

3. Osoby przetwarzające dane osobowe w Zespole Szkół Zawodowych w Rawiczu mają obowiązek stosowania oddanych im do dyspozycji procedur i narzędzi, w tym dotyczących niszczenia danych osobowych.

VI. Zespół Szkół Zawodowych w Rawiczu, realizując politykę ochrony, zapewnia możliwość poszerzania wiedzy z zakresu problematyki przetwarzania i ochrony danych wszystkim osobom odpowiedzialnym za bieżącą realizację tej polityki.

Załącznik nr 2 do Zarządzenia
Dyrektora Zespołu Zawodowych
w Rawiczu

Wykaz budynków i pomieszczeń w budynkach Zespołu Szkół Zawodowych w Rawiczu, tworzących obszar przetwarzania

Budynek szkoły zlokalizowany przy ul. Hallera 12 - Budynek A

-gabinet wicedyrektora szkolenia praktycznego obszar za biurkiem ze wszystkimi urządzeniami oraz szafy,

-biblioteka szkolna obszar za biurkiem ze wszystkimi urządzeniami oraz szafy,

- gabinet pielęgniarki szkolnej obszar za biurkiem ze wszystkimi urządzeniami oraz szafy

- pokój nauczycielski ze sprzętem komputerowym oraz szafy

- sale lekcyjne z biurkiem nauczyciela oraz szafy (sale: 1,2,3,4,5,5a,6,7,8,9,10,11,12,13,14,15)

Budynek szkoły zlokalizowany przy ul Gen.Hallera 10 - Budynek B:

- pokój nauczycielski ze sprzętem komputerowym oraz szafy

- sale lekcyjne z biurkiem nauczyciela oraz szafy (sale: 16,17,18,19,20,21,22,23)

Budynek szkoły zlokalizowany przy ul. Gen. Hallera 8 - Łącznik, sala gimnastyczna

-wydzielona część sekretariatu Szkoły, obszar za ladą ze wszystkimi urządzeniami oraz szafy i szafy aktowe ze skarbczykiem

-gabinet Dyrektora Zespołu ze wszystkimi urządzeniami oraz szafy

-gabinet wicedyrektorów - obszar za biurkiem ze wszystkimi urządzeniami oraz szafy

-pokój nauczycielski nauczycieli wychowania fizycznego - sprzęt komputerowy oraz szafy

-kącik pamięci szkoły - przestrzeń otwarta,

serwerownia ze wszystkimi urządzeniami

Budynek szkoły zlokalizowany przy ul. Gen.Hallera 6 - Budynek C

-gabinet wicedyrektora - obszar za biurkiem ze wszystkimi urządzeniami oraz szafy

-gabinet pedagoga szkolnego - obszar za biurkiem ze sprzętem komputerowym oraz szafy

- MCI - biurka ze sprzętem komputerowym

-pokój nauczycielski wraz ze sprzętem komputerowym oraz szafy

-pomieszczenie archiwum z szafami- regałami

-sale lekcyjne z biurkiem nauczyciela oraz szafy (sale 24,25,26,27,28,29,30,31,32,33,34,35)

Budynek szkoły zlokalizowany przy ul. Grota Roweckiego 9 - Budynek G

- pokój nauczycielski wraz ze sprzętem komputerowym oraz szafy

- sale lekcyjne z biurkiem nauczyciela oraz szafy (sale: 2.3, 2.5, 2.12, 2.13, 2.14, 3.12, 3.14)

Budynki warsztatów szkolnych - ul. Sienkiewicza 27

-pokój nauczycielski wraz ze sprzętem komputerowym oraz szafy

- sale lekcyjne z biurkiem nauczyciela oraz szafy (sale: 4,5,6,7)

-pomieszczenie biurowe - obszar ze wszystkimi urządzeniami oraz szafy

Załącznik nr 3 do Zarządzenia
Dyrektora Zespołu Zawodowych
w Rawiczu

Instrukcja Zarządzania Systemem Informatycznym w Zespole Szkół Zawodowych w Rawiczu

I. Niniejsza Instrukcja ma zastosowanie do wszelkich danych osobowych znajdujących się, bądź mogących znajdować się w systemach informatycznych administratora.

II. Instrukcja określa zasady i tryb postępowania administratora danych i osób przez niego upoważnionych przy przetwarzaniu danych osobowych.

III. Integralną część niniejszej Instrukcji stanowi Procedura określająca zasady funkcjonowania Dziennika Elektronicznego – Regulamin korzystania z Systemu LIBRUS Synergia w Zespole Szkół Zawodowych w Rawiczu w zakresie ochrony danych osobowych (załącznik Nr 4).

IV. Ogólne zasady pracy w systemie informatycznym.

1. Sygnał internetowy dostarczany jest przez usługodawcę internetowego i odpowiednio zabezpieczony oprogramowaniem antywirusowym.

2. Przetwarzanie danych w systemie informatycznym może być realizowane wyłącznie poprzez licencjonowane oprogramowanie.

3. Użytkownikom zabrania się:

   a) korzystania ze stanowisk komputerowych podłączonych do sieci informatycznej poza godzinami i dniami pracy szkoły bez pisemnej zgody ADO,
   b) udostępniania stanowisk roboczych osobom nieuprawnionym,
   c) samowolnego instalowania i używania programów komputerowych,
   d) wykorzystywania sieci komputerowej szkoły w celach innych niż wyznaczone przez ADO,
   e) korzystania z nielicencjonowanego oprogramowania oraz wykonywania jakichkolwiek działań niezgodnych z ustawą o ochronie praw autorskich,
   f) umożliwiania dostępu do zasobów wewnętrznej informatycznych szkoły oraz sieci internetowej osobom nieuprawnionym,

V. Nadawanie uprawnień do przetwarzania danych osobowych oraz ich rejestrowanie w systemie informatycznym.

1. Do przetwarzania danych osobowych zgromadzonych w systemie informatycznym jak również w rejestrach tradycyjnych wymagane jest upoważnienie. Upoważnienie wydawane jest zgodnie ze wzorami stanowiącymi załączniki Nr 10-11 do zarządzenia.

2. Po nadaniu upoważnienia, ASI tworzy konta użytkowników w systemach informatycznych i przyznaje identyfikatory oraz tworzy hasła tymczasowe.

3. Uprawnienia do pracy w systemie informatycznym mogą być odbierane czasowo, poprzez zablokowanie konta na podstawie dyspozycji wydanej przez ADO.

4. Uprawnienia do przetwarzania danych osobowych odbierane są trwale w przypadku ustania stosunku pracy.
5. Osoby, które zostały upoważnione do przetwarzania danych, są obowiązane zachować w tajemnicy te dane osobowe oraz sposoby ich zabezpieczenia także po ustaniu stosunku pracy.

V. Stosowane metody i środki uwierzytelnienia oraz procedury związane i ich zarządzaniem i użytkowaniem.

1. System informatyczny przetwarzający dane osobowe wykorzystuje mechanizm identyfikatora i hasła jako narzędzi umożliwiających bezpieczne uwierzytelnienie.

2. Każdy użytkownik systemu informatycznego powinien posiadać odrębny identyfikator.

3. Hasło powinno składać się z co najmniej ośmiu znaków, zawierać co najmniej jedną literę wielką, jedną cyfrę i jeden znak specjalny.

4. Zmianę hasła należy dokonywać w miesiącach, w których następuje przetwarzanie danych osobowych.

5. Hasło nie może zawierać żadnych informacji, które można kojarzyć z użytkownikiem komputera np. osobiste dane użytkownika, tj. nazwisko, inicjały, imiona, marka lub nr rejestracyjny samochodu itp.

6. Hasło nie może być zapisywane w miejscu dostępnym dla osób nieuprawnionych. Użytkownik nie może udostępnić swojego identyfikatora oraz hasła jak również dostępu do stanowiska roboczego po uwierzytelnieniu w systemie osobom nieuprawnionym ani żadnej osobie postronnej.

7. Hasło użytkownika, umożliwiające dostęp do systemu informatycznego, należy utrzymywać w tajemnicy, również po upływie jego ważności.

8. Raz użyty identyfikator nie może być przydzielony innemu użytkownikowi.

9. Hasła są zdeponowane w kasie pancernej w sekretariacie szkoły.

10. W przypadku, gdy istnieje podejrzenie, że hasło mogła poznać osoba nieuprawniona, użytkownik zobowiązany jest do natychmiastowej zmiany hasła, lub w razie problemów powiadomić o tym fakcie inspektora ochrony danych oraz ASI.

VI. Rozpoczęcie , zawieszenie i zakończenie pracy.

1. Rozpoczęcie pracy użytkownika w systemie informatycznym obejmuje wprowadzenie identyfikatora i hasła w sposób minimalizujący ryzyko podejrzenia przez osoby nieupoważnione.

2. Użytkownik systemu jest odpowiedzialny za zabezpieczenie danych wyświetlanych przez system przed osobami nie mającymi uprawnień.

3. Zawieszenie pracy polega na opuszczeniu stanowiska pracy bez wylogowania się i jest dopuszczalne tylko w przypadku pozostania w pomieszczeniu.

4. Zabrania się opuszczania stanowiska pracy bez wcześniejszego wylogowania z systemu z zastrzeżeniem pkt 3.

5. Zakończenie pracy polega na wylogowaniu się z systemu i wyłączeniu komputera.

VII. Tworzenie kopii zapasowych zbiorów danych oraz programów i narzędzi służących do ich przetwarzania.

1. Zbiory danych w systemie informatycznym są zabezpieczane przed utratą lub uszkodzeniem za pomocą:
   a) urządzeń zabezpieczających przed awarią zasilania lub zakłóceniami w sieci zasilającej,
   b) sporządzania kopii zapasowych zbiorów danych (kopie pełne).

2. Za tworzenie kopii bezpieczeństwa systemu informatycznego odpowiedzialny jest ASI.

3. W szczególnych przypadkach – przed aktualizacją lub zmianą w systemie należy bezwarunkowo wykonać pełną kopię zapasową systemu.

4. Kopie zapasowe zbiorów danych podlegają okresowym testom pod kątem ich przydatności do odtworzenia w przypadku awarii systemu. Za przeprowadzanie tej procedury odpowiedzialny jest ASI. Z przeprowadzonych testów należy sporządzić raport i przekazać ADO.

VIII. Sposób, miejsce i okres przechowywania elektronicznych nośników informacji.

1. Nośniki danych oraz programów służących do przetwarzania danych osobowych, a także danych konfiguracyjnych systemu informatycznego, przechowuje ASI w szafie pancernej w sekretariacie szkoły.

2. Przenośne nośniki danych powinny są zabezpieczone ochroną kryptograficzną.

3. Urządzenia, dyski lub inne elektroniczne nośniki informacji z danymi osobowymi przeznaczone do:

   a) **likwidacji** — pozbawia się wcześniej zapisu tych danych, a w przypadku gdy nie jest to możliwe, uszkadza się w sposób uniemożliwiający ich odczytanie,
   b) **przekazania podmiotowi nieuprawnionemu do przetwarzania danych** — pozbawia się wcześniej zapisu tych danych, w sposób uniemożliwiający ich odzyskanie,
   c) **naprawy** — pozbawia się wcześniej zapisu tych danych w sposób uniemożliwiający ich odzyskanie albo naprawia się je pod nadzorem ASI.

4. Nośniki kopii awaryjnych, które zostały wycofane z użycia, podlegają zniszczeniu po usunięciu danych osobowych.

IX. Sposób zabezpieczenia systemu przed działalnością oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego.

1. ASI zapewnia ochronę antywirusową oraz zarządza systemem wykrywającym i usuwającym wirusy i inne niebezpieczne kody. System antywirusowy jest skonfigurowany w następujący sposób:
   a) skanowanie dysków zawierających potencjalnie niebezpieczne dane następuje automatycznie po włączeniu komputera,
   b) skanowanie wszystkich informacji przetwarzanych w systemie, a zwłaszcza poczty elektronicznej jest realizowane na bieżąco.
   c) automatycznej aktualizacji wzorców wirusów.

2. W przypadkach wystąpienia infekcji użytkownik powinien niezwłocznie powiadomić o tym fakcie ASI.
3. W przypadku wystąpienia infekcji i braku możliwości automatycznego usunięcia wirusów przez system antywirusowy, ASI podejmuje działania zmierzające do usunięcia zagrożenia. W szczególności działania te mogą obejmować:
   a) usunięcie zainfekowanych plików, o ile jest to akceptowalne ze względu na prawidłowe funkcjonowanie systemu informatycznego,
   b) odtworzenie plików z kopii awaryjnych po uprzednim sprawdzeniu, czy dane zapisane na kopiach nie są zainfekowane,
   c) samodzielną ingerencję w zawartość pliku w zależności od posiadanych narzędzi i oprogramowania.

4. Użytkownicy systemu mają również obowiązek skanowania każdego zewnętrznego elektronicznego nośnika informacji przed jego wykorzystaniem.

X. Przesyłanie danych poza obszar przetwarzania.

1. Urządzenia i nośniki zawierające dane osobowe, przekazywane poza obszar przetwarzania zabezpiecza się w sposób zapewniający poufność i integralność tych danych.

2. W wypadku przesyłania danych osobowych poza sieć przystosowaną do transferu danych osobowych należy zastosować szczególne środki bezpieczeństwa, które obejmują zatwierdzenie przez ASI zakresu danych osobowych przeznaczonych do wysłania.

3. Umożliwienie wysyłania danych osobowych tylko z wykorzystaniem określonej aplikacji i tylko przez określonych użytkowników.

4. Za realizację procesów związanych z zarządzaniem aplikacjami kryptograficznymi oraz generowanie kluczy dostępowych do tych aplikacji odpowiedzialny jest operator zewnętrzny KIR. Szafir.

XI. Procedury wykonywania przeglądów i konserwacji systemów oraz nośników informacji służących do przetwarzania danych osobowych.

1. Przeglądy i konserwacje systemu oraz nośników informacji służących do przetwarzania danych mogą być wykonywane jedynie przez osoby posiadające upoważnienie wydane przez ADO.

2. Wszelkie prace związane z naprawami i konserwacją systemu informatycznego przetwarzającego dane osobowe muszą uwzględniać zachowanie wymaganego poziomu zabezpieczenia tych danych przed dostępem do nich osób nieupoważnionych, w szczególności poprzez bezpośredni nadzór prowadzony przez ASI.

3. W przypadku uszkodzenia zestawu komputerowego, nośniki danych, na których są przechowywane dane osobowe powinny zostać zabezpieczone przez ASI.

4. W przypadku konieczności przeprowadzenia prac serwisowych poza szkołą, dane osobowe znajdujące się w naprawianym urządzeniu muszą zostać w sposób trwały usunięte.

5. Jeżeli nie ma możliwości usunięcia danych z nośnika na czas naprawy komputera, należy zapewnić stały nadzór nad tym nośnikiem przez osobę upoważnioną do przetwarzania danych osobowych na nim zgromadzonych.

Załącznik nr 4 do Zarządzenia
Dyrektora Zespołu Zawodowych
w Rawiczu

Regulamin korzystania z systemu LIBRUS Synergia w Zespole Szkół Zawodowych w Rawiczu w zakresie ochrony danych osobowych

ROZDZIAŁ I. Postanowienia ogólne

1) W szkole, za pośrednictwem strony https://synergia.librus.pl funkcjonuje elektroniczny dziennik. Usługi związane z dziennikiem dostarczane są przez firmę zewnętrzną, współpracującą ze szkołą. Podstawą działania dziennika elektronicznego jest umowa podpisana przez dyrektora szkoły i uprawnionego przedstawiciela firmy dostarczającej oraz obsługującej system dziennika elektronicznego.
2) Administratorem danych osobowych zamieszczonych w Systemie LIBRUS Synergia jest Zespół Szkół Zawodowych im. S. Bobrowskiego w Rawiczu.
3) Za niezawodność działania systemu, ochronę danych osobowych umieszczonych na serwerach oraz tworzenie kopii bezpieczeństwa odpowiada firma nadzorująca pracę Systemu LIBRUS Synergia, pracownicy szkoły, którzy mają bezpośredni dostęp do przeglądania i edycji danych oraz rodzice (prawni opiekunowie) i uczniowie w zakresie udostępnionych im danych. Szczegółową odpowiedzialność wszystkich stron reguluje zawarta pomiędzy stronami umowa oraz przepisy obowiązującego w Polsce prawa.

ROZDZIAŁ IL Konta w dzienniku elektronicznym

1) Każdy użytkownik Systemu LIBRUS Synergia (szkolny administrator dziennika elektronicznego, dyrektor szkoły, wychowawca klasy, nauczyciel, pedagog, pracownik biblioteki szkolnej, pracownik sekretariatu, rodzic, uczeń) posiada własne konto dostępowe do systemu dziennika elektronicznego, za które osobiście odpowiada. Konstrukcja systemu, ze względu na bezpieczeństwo danych w systemie, wymusza na użytkowniku okresową zmianę hasła konta. Hasło dostarczone przez administratora służy tylko do pierwszego zalogowania. Hasło wprowadzone przez użytkownika powinno się składać co najmniej z 8 znaków i być kombinacją liter (dużych i małych) i cyfr.
2) Każdy użytkownik jest zobowiązany stosować się do zasad bezpieczeństwa w posługiwaniu się loginem i hasłem do systemu, które poznał na szkoleniu (nauczyciele na Radzie Pedagogicznej lub indywidualnym szkoleniu, rodzice na zebraniu z rodzicami, uczniowie na zajęciach), w szczególności do utrzymywania w tajemnicy hasła umożliwiającego dostęp do zasobów Systemu LIBRUS Synergia, również po upływie jego ważności.
3) W przypadku utraty hasła lub podejrzenia, że zostało odczytane/wykradzione przez osobę nieuprawnioną, użytkownik zobowiązany jest do niezwłocznego, osobistego poinformowania o tym fakcie szkolnego administratora dziennika elektronicznego.
4) Użytkownik, po zalogowaniu na swoim koncie, zobowiązany jest do sprawdzenia wiarygodności informacji odnośnie:
   - ostatniego udanego logowania
   - ostatniego nieudanego logowania.

   W razie stwierdzenia nieścisłości powinien osobiście o tym fakcie powiadomić szkolnego administratora dziennika elektronicznego.

ROZDZIAŁ III. Przekazywanie informacji w dzienniku elektronicznym

1) Użytkownikowi systemu dziennika elektronicznego nie wolno umożliwiać korzystania z zasobów osobom trzecim.

2) Pracownikom szkoły nie wolno udzielać osobom trzecim żadnych informacji zawartych w systemie dziennika elektronicznego. Wszystkie dane osobowe uczniów i ich rodziców są poufne.
3) Pracownikom szkoły nie wolno przekazywać żadnych informacji odnośnie loginów i haseł dostępowych do konta rodzicom i uczniom drogą telefoniczną oraz z wykorzystaniem poczty elektronicznej.
4) Rodzicowi przysługuje prawo wglądu do informacji o swoim dziecku, ale tylko w szkole. Jeśli zaistnieje taki przypadek, to (w asyście dyrektora, wychowawcy, nauczyciela przedmiotowego lub pedagoga) rodzicowi udostępnia się za pomocą komputera wszystkie informacje dotyczące jego dziecka z zachowaniem poufności danych osobowych innych uczniów.
5) Szkoła, na życzenie rodzica (prawnego opiekuna), może (z zachowaniem poufności danych osobowych) udostępnić rodzicowi (prawnemu opiekunowi) papierowe wydruki, które są przewidziane dla konta rodzica (prawnego opiekuna) w systemie dziennika elektronicznego.

ROZDZIAŁ IV. Dyrektor szkoły

1) Dyrektor szkoły jest zobowiązany dochowywać tajemnicy odnośnie postanowień zawartych w umowie dotyczącej wprowadzenia w szkole Systemu LIBRUS Synergia, mogących narazić działanie systemu informatycznego na utratę bezpieczeństwa.
2) Dyrektor szkoły dokonuje podziału zadań i obowiązków związanych z organizacją ochrony danych osobowych, w szczególności wyznacza administratora szkolnego dziennika elektronicznego oraz drugą osobę, która może w zastępstwie pełnić rolę administratora.
3) Dyrektor szkoły zobowiązany jest do stosowania podpisu elektronicznego archiwów dziennika elektronicznego za cały poprzedni rok szkolny. Archiwa wyżej wymienionych dzienników przechowywane są w szkolnym sejfie.

ROZDZIAŁ V. Szkolny administrator dziennika elektronicznego

1) Informacje o nowo utworzonych kontach (login, hasło) szkolny administrator dziennika elektronicznego ma obowiązek przekazać bezpośrednio ich właścicielom lub (w przypadku rodziców/opiekunów i uczniów) wychowawcom klas. W razie nieznajomości danej osoby, szkolny administrator dziennika elektronicznego ma obowiązek sprawdzić legitymację szkolną lub dowód osobisty celem weryfikacji tożsamości osoby.
2) Na prośbę użytkownika dziennika elektronicznego szkolny administrator przypomina loginy, generuje nowe hasła i przekazuje je, z zachowaniem zasad poufności, bezpośrednio zainteresowanym osobom lub (w przypadku rodziców/opiekunów i uczniów) wychowawcom klas.
3) Nie rzadziej niż raz na 3 miesiące szkolny administrator dziennika elektronicznego generuje dzienniki wszystkich oddziałów szkolnych jako kopie bezpieczeństwa. Przechowuje je na płycie CD w szkolnym sejfie. Po zakończeniu roku szkolnego wyżej wymienione kopie bezpieczeństwa zostają bezpowrotnie usunięte przez administratora e- dziennika.
4) Jeżeli nastąpi zablokowanie konta nauczyciela, szkolny administrator dziennika elektronicznego powinien:

- skontaktować się osobiście z nauczycielem i wyjaśnić powód blokady,
- w razie zaistnienia próby naruszenia bezpieczeństwa powiadomić firmę nadzorującą poprzez wysłanie informacji do Superadministratora,
- sprawdzić wraz z nauczycielem aktualną zawartość jego konta z tworzonymi kopiami bezpieczeństwa i jeśli jest taka potrzeba przywrócić je do prawidłowej zawartości,
- wygenerować i przekazać nowe jednorazowe hasło dla nauczyciela.

5) Szkolny administrator dziennika elektronicznego, w pierwszym tygodniu nowego roku szkolnego, generuje dzienniki poszczególnych klas za cały poprzedni rok szkolny i przekazuje je dyrektorowi szkoły.

ROZDZIAŁ VI. Wychowawca klasy

1) Na pierwszym zebraniu z rodzicami wychowawca klasy ma obowiązek osobiście rozdać rodzicom (prawnym opiekunom) loginy i hasła do ich kont oraz kont ich dzieci. Podczas godziny do dyspozycji wychowawcy, wychowawca przekazuje loginy i hasła do kont uczniowskich swoim wychowankom.
2) Wychowawca informuje rodziców (prawnych opiekunów) i uczniów o zasadach bezpiecznego korzystania z konta dziennika elektronicznego, ze szczególnym uwzględnieniem zasad ochrony danych osobowych użytkownika konta.
3) Fakt otrzymania loginów i haseł oraz zapoznania się z zasadami bezpiecznego korzystania z konta dziennika elektronicznego, rodzic (prawny opiekun) potwierdza podpisem na dokumencie (załącznik nr 22) w obecności wychowawcy klasy. Wymieniony dokument wychowawca przechowuje w teczce wychowawcy.
4) Na prośbę rodzica (prawnego opiekuna) lub ucznia administrator przypomina użytkownikowi jego login i generuje nowe hasło po czym przekazuje je wychowawcy klasy. Wychowawca przekazuje użytkownikowi wyżej wymienione dane do konta z zachowaniem następujących zasad:
   - rodzic otrzymuje login i hasło dla konta rodzica i ucznia
   - uczeń otrzymuje login i hasło dla konta ucznia

ROZDZIAŁ VII. Nauczyciel

1) Nauczyciel jest osobiście odpowiedzialny za swoje konto i zobowiązany do ochrony danych osobowych umieszczonych w systemie dziennika elektronicznego, a w szczególności:
   - chroni dane dostępowe do swojego konta (login, hasło) przed osobami trzecimi,
   - po zalogowaniu się do swojego konta sprawdza informację o ostatnim udanym i nieudanym logowaniu - w razie potrzeby niezwłocznie informuje o zagrożeniu administratora szkolnego dziennika elektronicznego,
   - nie udostępnia uczniom komputera, który służy w pracowni do korzystania z dziennika elektronicznego,
   - nie pozostawia bez nadzoru uczniów w pracowni z komputerem służącym do dostępu do dziennika elektronicznego,
   - jeżeli do dostępu do dziennika elektronicznego korzysta z laptopa, nie udostępnia go osobom trzecim,
   - dba o to, by poufne dane prezentowane na monitorze komputera nie były widoczne dla osób trzecich,
   - po zakończeniu pracy z dziennikiem elektronicznym wylogowuje się z konta,
2) Nauczyciel nie udostępnia osobom nieupoważnionym, zgromadzonych na zewnętrznych nośnikach lub wydrukach, wygenerowanych dzienników, plików świadectw szkolnych, plików generowanych w dzienniku elektronicznym statystyk itp.

ROZDZIAŁ VIII. Sekretariat

1) Za obsługę konta „sekretariat" odpowiedzialna jest wyznaczona przez dyrektora szkoły osoba, która na stałe pracuje w sekretariacie szkoły.
2) W przypadku zaistnienia takiej potrzeby, na polecenie dyrektora szkoły, szkolny administrator dziennika elektronicznego przydziela osobie pracującej w sekretariacie konto z uprawnieniami administratora.
3) Po skreśleniu ucznia z listy uczniów, pracownik sekretariatu szkoły drukuje jego kartotekę i umieszcza w arkuszu ocen.
4) Wszelkie informacje zaczerpnięte z dziennika elektronicznego, dotyczące ucznia, pracownik sekretariatu może przekazać zainteresowanemu lub jego rodzicowi wyłącznie po okazaniu przez niego legitymacji szkolnej lub dokumentu tożsamości.

ROZDZIAŁ IX. Rodzice (prawni opiekunowie)

1) Rodzice (prawni opiekunowie) mają w systemie dziennika elektronicznego swoje niezależne konto, zapewniające podgląd wyników w nauce i frekwencji ucznia na zajęciach szkolnych oraz dające możliwość komunikowania się z nauczycielami w sposób zapewniający ochronę danych osobowych innych uczniów.
2) Rodzic osobiście odpowiada za swoje konto w dzienniku elektronicznym szkoły i ma obowiązek nieudostępniania go swojemu dziecku ani innym nieupoważnionym osobom.

ROZDZIAŁ X. Uczeń

1) Uczeń ma w systemie dziennika elektronicznego swoje niezależne konto, umożliwiające podgląd swoich wyników w nauce i frekwencji, zapewniające ochronę danych osobowych innych uczniów.
2) Uczeń osobiście odpowiada za swoje konto w dzienniku elektronicznym szkoły i ma obowiązek nieudostępniania go innym, nieupoważnionym osobom.

ROZDZIAŁ XI. Postanowienia końcowe

1) Wszystkie poufne dokumenty i materiały utworzone na podstawie danych z dziennika elektronicznego, które nie będą potrzebne, należy zniszczyć.
2) Wszystkie zeskanowane i przesłane do bazy danych karty powinny być przechowywane w szkole do końca tygodnia, a następnie zniszczone z wykorzystaniem niszczarki.
3) Osoby z zewnątrz (serwisanci, osoby dokonujące przeglądów, pracownicy firm udzielających licencji na oprogramowanie itp.), jeśli jest to wymagane treścią dokumentów i stanem urządzeń do których mają dostęp, zobowiązują się do poszanowania i zachowania tajemnicy wynikającej z ustawy o ochronie danych osobowych, podpisując, obok umowy głównej dot. danych usług, umowę powierzenia przetwarzania (załącznik nr 13).
4) W razie kontroli z zewnątrz odpowiedniego organu uprawnionego do kontrolowania dokumentacji szkolnej, na polecenie dyrektora szkoły, na czas kontroli, szkolny administrator dziennika elektronicznego udostępnia wyznaczonej do tego celu osobie konto w dzienniku elektronicznym dające możliwość sprawdzenia prawidłowego prowadzenia przez nauczycieli dokumentacji bez możliwości dokonywania w dzienniku elektronicznym jakichkolwiek zmian.

Załącznik nr 5 do Zarządzenia
Dyrektora Zespołu Zawodowych
w Rawiczu

Podstawowe zasady dotyczące zachowania bezpieczeństwa podczas pracy zdalnej.

§ 1

1. Przetwarzanie danych osobowych w Zespole Szkół Zawodowych w Rawiczu podczas pracy zdalnej służy realizacji obowiązków oraz uprawnień określonych przepisami prawa, w szczególności zadań statutowych szkoły, wynikających z ustawy z dnia 14 grudnia 2016r. Prawo oświatowe (Dz. U. z 2020r. poz. 910).
2. Niniejsze zasady są częścią obowiązującej w Szkole procedury ochrony danych osobowych.

§ 2

1. W okresie czasowego ograniczenia funkcjonowania szkoły na podstawie przepisów wydanych przez ministra edukacji narodowej, dyrektor odpowiada za organizację realizacji zadań szkoły z wykorzystaniem metod i technik kształcenia na odległość lub innego sposobu realizacji tych zadań.
2. Dyrektor w szczególności:

1) ustala sposób i tryb realizacji zadań szkoły w okresie czasowego ograniczenia funkcjonowania i przekazuje informacje na ten temat rodzicom, nauczycielom i innym pracownikom;
2) koordynuje współpracę nauczycieli z rodzicami, uwzględniając potrzeby edukacyjne i możliwości psychofizyczne uczniów, w tym objętych kształceniem specjalnym;ustala sposób realizacji zadań przez statutowe organy szkoły i zasady współpracy pomiędzy nimi oraz koordynuje realizację tych zdań w okresie czasowego ograniczenia funkcjonowania szkoły;
3) ustala sposób dokumentowania realizacji zadań szkoły w tym okresie;
4) nadzoruje realizację zadań Szkoły;

3. Statutowe czynności dyrektora i innych organów, nauczycieli oraz pozostałych pracowników szkoły mogą być podejmowane w sposób ustalony przez Dyrektora adekwatnie do sytuacji i bieżących potrzeb:

1) na terenie szkoły;
2) za pomocą środków komunikacji elektronicznej lub za pomocą innych środków łączności, a w przypadku rady pedagogicznej i rady rodziców także w trybie obiegowym.

4. W okresie czasowego ograniczenia funkcjonowania szkoły rodzice i inne podmioty środowiska lokalnego współpracujące ze szkołą mogą komunikować się i załatwiać niezbędne sprawy drogą

elektroniczną lub za pomocą innych środków komunikacji.

§ 3

1. Organizacja zajęć szkolnych w formie pracy zdalnej dotyczy realizowania przez nauczycieli zajęć z wykorzystaniem metod i technik kształcenia na odległość lub innego sposobu kształcenia, w tym z wykorzystaniem środków komunikacji elektronicznej.
2. Szkoła zapewnia narzędzia umożliwiające nauczycielom prowadzenie zajęć zdalnych w ramach posiadanych zasobów oraz bezpieczną komunikację z uczniami i rodzicami, wdrażając je kompleksowo w całej jednostce.
3. Urządzenia i oprogramowanie przekazane przez pracodawcę do pracy zdalnej służą wyłącznie do wykonywania obowiązków służbowych. Dlatego też należy postępować zgodnie z przyjętą procedurą bezpieczeństwa, o której mowa poniżej.
4. Jednym z głównych obowiązków szkoły - związanych z ochroną danych osobowych – jest zabezpieczenie danych przez zastosowanie odpowiednich środków technicznych i organizacyjnych w celu zabezpieczenia danych przed udostępnieniem osobom nieupoważnionym oraz zniszczeniem, modyfikacją czy utratą.
5. W celu zabezpieczenia przetwarzanych danych stosowane będą: szyfrowanie danych, anonimizacja i pseudnimizacja.
6. W razie wykonywania obowiązków służbowych poza szkołą przetwarzanie danych musi być odpowiednio zabezpieczone, przy uwzględnieniu ryzyka naruszenia ochrony danych i wdrożeniu środków minimalizujących to ryzyko. Jeżeli nie ma takiej możliwości dyrektor umożliwia nauczycielowi pracę na terenie szkoły.
7. Do kontaktów nauczycieli z uczniami i rodzicami (opiekunami prawnymi) wykorzystywane powinny być jednynie służbowe adresy poczty elektronicznej.
8. Dane osobowe uczniów i ich rodziców (opiekunów prawnych) mogą być przetwarzane wyłącznie w celach związanych z wykonywaniem obowiązków służbowych.
9. W przypadku konieczności pozyskania danych osobowych niezbędnych dla umożliwienia komunikacji między nauczycielem a uczniami i rodzicami nie będą gromadzone dane nadmierne czy służące realizacji innych celów.

§ 4

1. Każdy pracownik musi pamiętać o bezpiecznym korzystaniu z komputerów i innych urządzeń, niezależnie czy zapewnia je pracodawca, czy są one jego prywatną własnością.
2. Wszystkie urządzenia, z których korzysta pracownik winny mieć niezbędne aktualizacje systemu operacyjnego (IOS, Android), oprogramowania oraz systemu antywirusowego.
3. Zabronione jest instalowanie dodatkowych aplikacji i oprogramowania niezgodnych

z procedurą bezpieczeństwa.

4. Możliwe jest wykorzystywanie prywatnego komputera, tabletu czy telefonu do przetwarzania danych osobowych w związku ze zdalnym wykonywaniem pracy. Urządzenia te muszą być odpowiednio zabezpieczone (np. przez program antywirusowy), a pracownicy winni bezwzględnie przestrzegać obowiązującej polityki bezpieczeństwa.
5. Jeżeli nauczyciel korzysta z własnych urządzeń powinien samodzielnie spełnić podstawowe wymogi bezpieczeństwa - sprawdzić, czy wykorzystywane urządzenie ma aktualny system operacyjny, czy używane są na nim programy, w szczególności programy antywirusowe, czy dokonane są niezbędne aktualizacje. Na bieżąco aktualizowane powinny być także zainstalowane programy antymalware i antyspyware. Należy rozważnie instalować na swoich urządzeniach oprogramowanie i pobierać je tylko z wiarygodnych źródeł (ze stron producentów).
6. Przechowując dane na sprzęcie, do którego mogą mieć dostęp inne osoby, należy bezwzględnie używać mocnych haseł dostępowych, a dodatkowo chronić je przed utratą czy dostępem osób nieuprawnionych. Zaleca się także wielopoziomowe uwierzytelnianie, co pozwoli na ograniczenia dostępu do urządzenia, a jednocześnie na ograniczenia ryzyka utraty danych w przypadku kradzieży lub zgubienia urządzenia
7. Przed odejściem od stanowiska pracy urządzenie powinno zostać zablokowane. Zalecane jest także skonfigurowanie automatycznego blokowania komputera po pewnym czasie bezczynności oraz założenie odrębnych kont użytkowników w przypadku korzystania z komputera przez wiele osób.
8. Podczas korzystania z programów lub aplikacji mobilnych należy korzystać z możliwych do zastosowania w nich mechanizmów ochrony prywatności użytkowników.
9. Gdy dane są przechowywane na urządzeniach przenośnych (np. pamięć USB), muszą być bezwzględnie szyfrowane i chronione hasłem, by zapewnić odpowiednie bezpieczeństwo danych osobowych, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem.
10. W podstawowym zakresie komunikację z uczniami i rodzicami prowadzi się poprzez wdrożone w szkole rozwiązania teleinformatyczne, przede wszystkim poprzez dzienniki elektroniczne. W takiej sytuacji nauczyciel musi nadal zachowywać podstawowe zasady bezpieczeństwa przy zdalnym łączeniu się z dziennikiem elektronicznym ze swojego urządzenia w domu.
11. Prowadzenie zajęć zdalnych może wymagać korzystania przez nauczyciela z poczty elektronicznej do kontaktu z uczniami lub rodzicami. Nauczyciel powinien prowadzić taką korespondencję ze służbowej skrzynki pocztowej, pamiętając aby korzystać z niej rozważnie i bezpiecznie.

12. Przed wysłaniem wiadomości e-mail należy upewnić się, że treść i załączniki są właściwie szyfrowane. Należy unikać używania danych osobowych lub poufnych informacji w temacie wiadomości.
13. Przed wysłaniem wiadomości należy sprawdzić, że wysyłana jest ona do właściwego adresata, zwłaszcza jeśli wiadomość zawiera dane osobowe lub dane wrażliwe. Ponadto trzeba sprawdzić, czy w nazwie adresu e-mail adresata nie ma np. przestawionych lub pominiętych znaków tak, aby nie wysłać takiej wiadomości do osób nieupoważnionych. Podczas wysyłania korespondencji zbiorczej powinno się korzystać z opcji „UDW", dzięki której odbiorcy wiadomości nie będą widzieć wzajemnie swoich adresów e-mail.
14. Nigdy nie należy przesyłać mailem informacji zaszyfrowanej razem z hasłem, nawet w osobnej wiadomości.
15. Przy odbieraniu korespondencji - należy sprawdzić nadawcę maila - wiadomości od nieznanych adresatów nie powinny być otwierane, a zwłaszcza załączniki. Nie powinno się klikać w link zawarty w takiej wiadomości. To może być atak phishingowy.

§ 5

1. W zdalnym prowadzeniu zajęć nauczyciel powinien wykorzystywać te platformy edukacyjne lub narzędzia do e-learningu, które zostały wdrożone w szkole.
2. W wyjątkowych sytuacjach, biorąc pod uwagę konieczność natychmiastowego rozpoczęcia zajęć zdalnych, nauczyciel może wykorzystywać narzędzia wdrożone samodzielnie, ale tylko i wyłącznie po uzgodnieniu z dyrektorem szkoły lub wyznaczonym przez niego koordynatorem pracy zdalnej. Takie rozwiązanie może być stosowane wyłącznie jako tymczasowe.
3. Przy wyborze aplikacji lub innych narzędzi wykorzystywanych do zdalnej edukacji bądź komunikacji z uczniami każdorazowo należy się zastanowić, czy jest niezbędne, aby przetwarzały one dane osobowe, a jeżeli tak, czy można zminimalizować ich zakres, bądź wykorzystywać tylko pseudonimy (np. pierwsza litera imienia itp.) Należy także sprawdzić zasady świadczenia usługi i zasady przetwarzania danych przez usługodawcę (politykę prywatności).
4. Nauczyciel w porozumieniu z dyrektorem szkoły powinien uwzględnić, jakie realne możliwości komunikowania się z nim mają uczniowie lub rodzice, pod warunkiem, że wskazany przez nich konkretny rodzaj komunikatora internetowego zapewnia bezpieczeństwo komunikacji.
5. Nauczyciel zobowiązany jest przestrzegać przyjętych przez szkołę instrukcji i procedur dotyczących ochrony danych osobowych oraz zachować podstawowe zasady bezpieczeństwa przy zdalnym łączeniu się z taką platformą ze swojego urządzenia w domu.

§ 6

1. Przed przystąpieniem do pracy, nauczyciel powinien przygotować swoje stanowisko pracy tak, aby osoby postronne nie miały dostępu do dokumentów, nad którymi pracuje.
2. W przypadku utraty urządzenia, wykorzystywanego do pracy lub jego kradzieży należy natychmiast podjąć odpowiednie kroki, aby o ile to możliwie, zdalnie wyczyścić jego pamięć.
3. Przy pracy związanej z dostępem do sieci lub chmury należy używać tylko zaufanego urządzenia oraz przestrzegać wszelkich zasad i procedur organizacyjnych dotyczących logowania i udostępniania danych.

§ 7

1. Szkoła może wymagać od ucznia jedynie danych niezbędnych do założenia przez niego konta w odpowiednim systemie zdalnego nauczania oraz w celu realizacji obowiązku nauki w formie zdalnej (na podstawie art. 35 ustawy – Prawa oświatowego w związku z art. 6 ust. 1 lit e RODO).
2. Rodzic (opiekun prawny) ma prawo wiedzieć, jak szkoła jako administrator będzie przetwarzała dane osobowe jego dziecka w trakcie nauki zdalnej oraz jakie w związku z tym przysługują mu prawa.

Załącznik nr 6 do
Zarządzenia
Dyrektora Zespołu Zawodowych
w Rawiczu

Plan ciągłości działania na wypadek awarii systemu informatycznego.

§1.

Celem procedury jest minimalizacja zakłóceń w realizacji działalności szkoły w związku z zaistnieniem awarii systemu informatycznego w Zespole Szkół Zawodowych w Rawiczu.

§2.

1. Przedmiotem procedury jest postępowanie w przypadku zaistnienia zdarzeń mających wpływ (również potencjalny) na bezpieczeństwo informacji oraz ciągłość działania szkoły.
2. Do zakresu stosowania należy zdefiniowanie działań koniecznych do podjęcia w przypadku awarii systemu informatycznego.
3. Działania zapewniające przywrócenie zdolności realizacji działalności Szkoły:

Lp.	Funkcja	Opis działań	Potrzebne zasoby
1.	Zweryfikować zasadność zgłoszenia od użytkownika	Sprawdzić, czy zgłoszenie dotyczy zdarzenia spowodowanego awarią systemu informatycznego	Zapewnić dostęp do infrastruktury informatycznej na stanowisku, skąd pochodzi zgłoszenie
2.	Ustalić źródła awarii	Ustalić co jest przyczyną awarii: - przerwa w zasilaniu prądem, - brak połączenia z siecią Internet, - brak połączenia z siecią LAN, - wadliwe działanie sprzętu, - wadliwe działanie aplikacji, - wadliwe działanie systemu, na którym uruchomiona jest aplikacja, - wadliwe działanie serwera	Zapewnić: - dostęp do sprzętu, który uległ awarii oraz serwera z zainstalowanym oprogramowaniem, - kontakt z osobą, która może otworzyć budynek poza godzinami pracy, - w przypadku blokady zamka wezwać konserwatora, - w przypadku awarii zasilania energetycznego wezwać pogotowie energetyczne.
3.	Określić skalę awarii	Ustalić, czy awaria powoduje zatrzymanie pracy: - jednej osoby, - jednego pomieszczenia pracy, - kilku pomieszczeń pracy	Zapewnić: - kontakt z kluczowymi pracownikami
4.	Ustalić czy wznawianie usługi może odbywać się w dotychczasowej lokalizacji	Działanie ma na celu zweryfikowanie, czy wznawiane usługi uruchamiane będą w dotychczasowej lokalizacji, czy w lokalizacjach alternatywnych	Zapewnić: - możliwość uruchomienia dowolnych usług w innej lokalizacji - infrastrukturę sieciową,

			zasilanie prądem.
5.	Ustalić czas wznawiania usługi	Działanie ma na celu określenie potencjalnego czasu w jakim usługa zostanie wznowiona do pełnej sprawności	
6.	Zakupić niezbędne elementy wyposażenia, dokonać naprawy (wymiany) urządzeń, uruchomić aplikację	W przypadku braku możliwości zakupu należy znaleźć rozwiązanie alternatywne (np. zdecydować o przeniesieniu aplikacji na inny serwer)	Zapewnić: - środki na zakup elementów niezbędnych do ponownego uruchomienia systemu
7.	Zweryfikować sposób usunięcia awarii	Należy zdecydować czy podjąć próbę naprawy awarii natychmiastowo czy przygotować serwer zastępczy, a następnie podjąć próbę naprawy	Zapewnić: - kontakt z kluczowymi pracownikami
8.	Zweryfikować możliwość przeniesienia aplikacji na inny serwer	Sprawdzić czy aplikacja może być uruchomiona na którymś z działających poprawnie serwerów	
9.	Przygotować serwer zastępczy	Jako serwer zastępczy można wykorzystać inny serwer lub komputer typu desktop, który należy odpowiednio skonfigurować. Po uruchomieniu aplikacji na serwerze zastępczym należy przetestować jej działanie	Zapewnić: - serwer zastępczy lub komputer typu desktop, który w podstawowym zakresie pozwoli na uruchomienie podstawowych usług
10.	Podjąć decyzję o terminie odtworzenia uszkodzonej maszyny	W razie konieczności należy skontaktować się z właściwymi pracownikami	Zapewnić: - kontakt z kluczowymi pracownikami
11.	Przywrócić funkcjonowanie aplikacji/systemu	Spróbować usunąć przyczynę nieprawidłowego działania. W razie konieczności należy odtworzyć aplikację z kopii zapasowej	Zapewnić: - dostęp do najbardziej aktualnej wersji aplikacji, - dostęp do aktualnej bazy danych, - dostęp do ostatniej poprawnej kopii zapasowej
12.	Sprawdzić działanie aplikacji/systemu	Po usunięciu przyczyny awarii/odzyskaniu kopii zapasowej należy zweryfikować prawidłowe działanie aplikacji/systemu zainstalowanego na serwerze	Zapewnić: - kontakt z kluczowymi pracownikami
13.	Uruchomienie usługi w systemie informatycznym	Po uruchomieniu usługi należy powiadomić właściwych pracowników o tym fakcie	Zapewnić: - kontakt z kluczowymi pracownikami

§3.

Działania mające na celu przywrócenie sprawności systemu informatycznego po awarii zasilania prądem:

1) włączenie zasilaczy awaryjnych UPS,
2) uruchomienie kontrolera domeny,
3) włączenie zasilania w routerach, firewallu, przełącznikach sieciowych,

4) uruchomienie macierzy danych,
5) uruchomienie serwerów klastrów pracy awaryjnej,
6) uruchomienie pozostałych serwerów,
7) zweryfikowanie poprawności pracy systemu informatycznego oraz dostępu do danych,
8) zweryfikowanie poprawności pracy systemu tworzenia kopii zapasowej.

§4.

1. Testowanie działania:

Lp.	Opis testu	Termin realizacji	Oczekiwany wynik
	Symulacja wyłączenia serwera danej aplikacji, brak możliwości wykonywania usług, symulacja na podstawie scenariusza zawartego w protokole	3 dni	Wznowienie działania usługi, możliwie na nowej maszynie

2. Uczestnicy planu są zapoznawani z jego treścią każdorazowo przed przeprowadzeniem jego testowania.

3.Plan aktualizowany jest każdorazowo w przypadku niepowodzenia w jego testowaniu.

Załącznik nr 7 do Zarządzenia
Dyrektora Zespołu Zawodowych
w Rawiczu

Instrukcja postępowania w sytuacji naruszenia ochrony danych osobowych w Zespole Szkół Zawodowych w Rawiczu

1. Szkoła prowadzi rejestr naruszeń ochrony danych osobowych.
2. 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 informatycznego, a w szczególności:
   a) nieautoryzowany dostęp do danych,
   b) nieautoryzowane modyfikacje lub zniszczenie danych,
   c) udostępnienie danych nieautoryzowanym podmiotom,
   d) nielegalne ujawnienie danych,
   e) pozyskiwanie danych z nielegalnych źródeł.
3. Każdy (w tym podmiot przetwarzający), kto uzna, że określone zdarzenie należy zakwalifikować jako zdarzenie, które może prowadzić do naruszenia ochrony danych osobowych, a w konsekwencji do naruszenia praw i wolności osób, których dane dotyczą, niezwłocznie zawiadamia o tym Szkołę, wysyłając zgłoszenie na adres; iod@powiatrawicki.pl. Zgłoszenia dokonane w innej formie, przekazywane są niezwłocznie do inspektora ochrony danych.
4. Inspektor ochrony danych niezwłocznie powiadamia Dyrektora.
5. Dyrektor niezwłocznie po otrzymaniu powiadomienia o zdarzeniu:
   1) podejmuje wraz z inspektorem ochrony danych oraz Administratorem Systemu Informatycznego działania interwencyjne i zabezpieczające, a następnie działania przywrócenia normalnego stanu;
   2) przeprowadza analizę w celu ustalenia:
      a) czy doszło do naruszenia ochrony danych osobowych,
      b)czy zachodzi konieczność zgłoszenia naruszenia ochrony danych osobowych organowi nadzorczemu, zgodnie z art. 33 RODO,
      c)czy zachodzi konieczność zawiadomienia osoby, której dane dotyczą, o naruszeniu ochrony danych osobowych, zgodnie z art. 34 RODO.
6. Jeśli doszło do naruszenia danych osobowych, należy :
   1)oznaczyć w rejestrze dane zdarzenie jako naruszenie,
   2)jeśli zachodzi przesłanka wskazana w ust. 4 pkt 2 lit. b) przygotować stosowne zgłoszenie do Prezesa Urzędu Ochrony Danych Osobowych,
   3)jeśli zachodzi przesłanka wskazana w ust. 4 pkt. 2 lit. c) przygotować zawiadomienie

do osoby, której dane dotyczą,

7. Dyrektor dokonuje zgłoszenia lub zawiadomienia w imieniu Szkoły jako administratora danych.
8. Zgłaszanie naruszenia ochrony danych osobowych organowi nadzorczemu następuje bez zbędnej zwłoki - w miarę możliwości, nie później niż w terminie 72 godzin po stwierdzeniu naruszenia. Do zgłoszenia przekazanego Prezesowi Urzędu Ochrony Danych Osobowych po upływie 72 godzin dołącza się wyjaśnienie przyczyn opóźnienia.
9. Zawiadamianie osoby, której dane dotyczą, o naruszeniu ochrony danych osobowych następuje bez zbędnej zwłoki.
10. Po przywróceniu normalnego stanu, przeprowadza się szczegółową analizę zdarzenia, w celu określenia przedsięwzięcia kroków mających na celu wyeliminowanie podobnych zdarzeń w przyszłości. Jeżeli przyczyną zdarzenia był błąd osoby, należy przeprowadzić dodatkowe szkolenie; w przypadku świadomego działania lub zaniedbania, należy wyciągnąć konsekwencje wynikające z obowiązujących w Szkole przepisów wewnętrznych oraz przepisów prawa powszechnego. Wyniki analizy przekazywane są Dyrektorowi.
11. Po wyjaśnieniu wszelkich okoliczności zdarzenia Dyrektor uzupełnia informacje, które zostały pierwotnie przekazane Prezesowi Urzędu Ochrony Danych Osobowych. Zawiadamia również o podjętych działaniach zapobiegawczych i ewentualnie o wszczęciu postępowania lub ukaraniu osoby (osób) odpowiedzialnej.

Załącznik Nr 8 do Zarządzenia
Dyrektora Zespołu Zawodowych
w Rawiczu

Rejestr przypadków naruszenia lub podejrzenia naruszenia bezpieczeństwa przetwarzania danych osobowych - wzór

Lp.	Data zgłoszenia naruszenia, dzień i godzina	Zgłaszający	Rodzaj naruszenia	Miejsce naruszenia jeżeli dotyczy - nazwa i dane kontaktowe podmiotu przetwarzajacego)	Opis naruszenia	Skutki naruszenia	Czy naruszenie podlega zgłoszeniu do organu nadzorczego	Czy naruszenie podlega zgłoszeniu osobie, której dane dotyczą	Podjęte działania – sposób usunięcia naruszenie	Data zakończenia czynności	Status

Załącznik Nr 9 do Zarządzenia
Dyrektora Zespołu Zawodowych
w Rawiczu

Rejestr czynności przetwarzania - wzór

Rejestr czynności przetwarzania w Zespole Szkół Zawodowych w Rawiczu

Administrator danych: Zespół Szkół Zawodowych (Rawicz, ul. Hallera 12 63-900 Rawicz), IOD: .....(e-mail: iod@powiatrawicki.pl);

L p.	Nazwa czynności przetwarzania	Cel przetwarzania	Kategorie osób	Kategorie danych	Podstawa prawna	Źródło danych	Planowany termin usunięcia kategorii danych *(jeżeli jest to możliwe)*	Nazwa współadministratora i dane kontaktowe *(jeśli dotyczy)*	Nazwa podmiotu przetwarzającego i dane kontakowe *(jeśli dotyczy)*	Kategorie odbiorców *(innych niż podmiot przetwarzajacy)*	Nazwa systemu lub oprogramowania	Ogólny opis technicznych i organizacyjnych srodków bezpieczeństwa zgodnie z art. 32 ust. 1 *(jeżeli jest to możliwe)*	DPIA (jeśli tak, lokalizacja raportu)	Transfer do kraju trzeciego lub org. międzynarodowej	
														Transfer do kraju trzeciego lub organizacji międzynarodowej (nazwa kraju i podmiotu)	Jeśli transfer i art. 49 ust. 1 akapit drugi - dokumentacja odpowiednich zabezpieczeń
		Art. 30 ust. 1 pkt b	Art. 30 ust. 1 pkt c	Art.30 ust. 1 pkt c			Art. 30 ust. 1 pkt f	Art. 30 ust. 1 pkt a	Art. 30 ust. 1 pkt d	Art. 30 ust. 1 pkt d		Art. 30 ust. 1 pkt g		Art. 30 ust. 1 pkt e	Art. 30 ust. 1 pkt e

Załącznik Nr 10 do Zarządzenia
Dyrektora Zespołu Zawodowych
w Rawiczu

Rejestr kategorii czynności przetwarzania - wzór

Lp.	Kategorie przetwarzań (art. 30 ust. 2 lit. b)	Ogólny opis technicznych i organizacyjnych środków bezpieczeństwa (jeżeli jest to możliwe) (art. 30 ust. 2 lit d, art. 32 ust. 1)	Administrator				Czas trwania przetwarzania	Nazwy państw trzecich lub organizacji międzynarodowych, do których dane są przekazywane (art. 30 ust. 2 lit. c)	Dokumentacja odpowiednich zabezpieczeń danych osobowych przekazywanych na podstawie art. 49 (art. 30 ust. 2 lit. c)	Podprzetwarzający (podwykonawca) - jeśli dotyczy a i dane kontaktowe podprzetwarzającego	Uwagi Kategorie podpowierzonych
			Nazwa i dane kontaktowe administratora	Nazwa i dane kontaktowe współadministratora (jeśli dotyczy)	Nazwa i dane kontaktowe przedstawiciela administratora (jeśli wyznaczono)	Inspektor ochrony danych administratora					

Załącznik Nr 11 do Zarządzenia
Dyrektora Zespołu Zawodowych
w Rawiczu
wzór

Rawicz, dnia.....

Upoważnienie do przetwarzania danych osobowych – wzór (dla pracowników pedagogicznych)

Na podstawie art. 29 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE(ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L z 4.05.2016, str. 1-88),

upoważniam Panią/Pana:

.....

(imię i nazwisko)

do przetwarzania danych osobowych na okres: od ..... do.....
(wpisać datę lub „traci moc z dniem rozwiązania bądź wygaśnięcia stosunku pracy")

Niniejsze upoważnienie może być w każdej chwili odwołane.

Zakres upoważnienia:
Dane osobowe uczniów i rodziców (opiekunów prawnych), niezbędne do prowadzenia dokumentacji szkolnej, w tym elektronicznego dziennika oraz dla celów przeprowadzenia egzaminów.
Przetwarzanie danych - na polecenie Administratora Danych Osobowych lub z konieczności spełnienia wymogów prawa - w celu realizacji zadań Zespołu Szkół Zawodowych w Rawiczu oraz udziału w procesach, w których przetwarzane są dane osobowe, w zakresie adekwatnym charakteru wykonywanej pracy, wynikających z umowy łączącej strony, zgodnie z nadanymi uprawnieniami, umożliwiającymi realizację celu przetwarzania. Przydział konkretnych zadań traktowany jest jako wydanie polecenia przetwarzania danych w zakresie niezbędnym do ich realizacji;

Kategorie osób, których dane dotyczą: uczniowie, rodzice (opiekunowie prawni)

Oświadczam, że zapoznałam/-em się z przepisami dotyczącymi ochrony danych osobowych, w szczególności Rozporządzeniem RODO i zasadami przetwarzania danych osobowych, obowiązującymi w Zespole Szkół Zawodowych w Rawiczu.

Zobowiązuję się do:

- przetwarzania danych - jedynie w zakresie nadanego upoważnienia i na polecenie administratora, zgodnie z zasadami przetwarzania danych osobowych określonymi w Zarządzeniu Nr .../2021 Dyrektora Zespołu Szkół Zawodowych z dnia ....2021 r. w sprawie wprowadzenia Procedury ochrony danych osobowych, z którym się zapoznałam/-em,
- przestrzegania zasad i procedur ochrony danych określonych w ww. dokumentach oraz przestrzegania przepisów dotyczących ochrony danych osobowych,
- zachowania w tajemnicy treści danych osobowych oraz informacji o sposobach ich zabezpieczenia, również po wygaśnięciu upoważnienia.

.....

(pieczęć i podpis Dyrektora)

.....

(data i czytelny podpis osoby upoważnionej)

Data wygaśnięcia upoważnienia:.....

.....

Pieczęć i podpis Dyrektora

Załącznik Nr 12 do Zarządzenia
Dyrektora Zespołu Zawodowych
w Rawiczu

Upoważnienie do przetwarzania danych osobowych – wzór (dla pracowników niepedagogicznych)

Rawicz, dnia.....

Na podstawie art. 29 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE(ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L z 4.05.2016, str. 1-88),

upoważniam Panią/Pana:

.....

(imię i nazwisko)

do przetwarzania danych osobowych na okres: od ..... do.....
(wpisać datę lub „traci moc z dniem rozwiązania bądź wygaśnięcia stosunku pracy")

Niniejsze upoważnienie może być w każdej chwili odwołane.

Zakres upoważnienia:

.....

Przetwarzanie danych - na polecenie Administratora Danych Osobowych lub z konieczności spełnienia wymogów prawa - w celu realizacji zadań Zespołu Szkół Zawodowych w Rawiczu oraz udziału w procesach, w których przetwarzane są dane osobowe, w zakresie adekwatnym do zakresu obowiązków lub charakteru wykonywanej pracy, wynikających z umowy łączącej strony, zgodnie z nadanymi uprawnieniami, umożliwiającymi realizację celu przetwarzania. Przydział konkretnych obowiązków/zadań traktowany jest jako wydanie polecenia przetwarzania danych w zakresie niezbędnym do ich realizacji;

Kategorie osób, których dane dotyczą:.....
(np. pracownicy i byli pracownicy; kontrahenci)

Oświadczam, że zapoznałam/-em się z przepisami dotyczącymi ochrony danych osobowych, w szczególności Rozporządzeniem RODO i zasadami przetwarzania danych osobowych, obowiązującymi w Zespole Szkół Zawodowych w Rawiczu.

Zobowiązuję się do:

- przetwarzania danych - jedynie w zakresie nadanego upoważnienia i na polecenie administratora, zgodnie z zasadami przetwarzania danych osobowych określonymi w Zarządzeniu Nr .../2021 Dyrektora Zespołu Szkół Zawodowych z dnia ....2021 r. w sprawie wprowadzenia Procedury ochrony danych osobowych, z którym się zapoznałam/-em,
- przestrzegania zasad i procedur ochrony danych określonych w ww. dokumentach oraz przestrzegania przepisów dotyczących ochrony danych osobowych,
- zachowania w tajemnicy treści danych osobowych oraz informacji o sposobach ich zabezpieczenia, również po wygaśnięciu upoważnienia.

.....

(pieczęć i podpis Dyrektora)

.....

(data i czytelny podpis osoby upoważnionej)

Data wygaśnięcia upoważnienia:.....

.....

Pieczęć i podpis Dyrektora

Załącznik Nr 13 do Zarządzenia

Dyrektora Zespołu Zawodowych
w Rawiczu

Wzór

Umowa powierzenia przetwarzania danych osobowych
stanowiąca uzupełnienie Umowy nr .....

zawarta w dniu ..... w ....., pomiędzy:

.....
reprezentowanym przez:

.....
zwanym w dalszej części umowy „Administratorem"
a

.....
reprezentowanym przez:

.....
zwanym w dalszej części umowy „Przetwarzającym"
łącznie zwani w dalszej części umowy „Stronami".

§ 1. Powierzenie przetwarzania danych osobowych

1. Administrator powierza Przetwarzającemu, w trybie art. 28 ogólnego rozporządzenia o ochronie danych z dnia 27 kwietnia 2016 r. (zwanego w dalszej części „RODO") dane osobowe do przetwarzania, na zasadach i w celu określonym w niniejszej Umowie.
2. Przetwarzający zobowiązuje się przetwarzać powierzone mu dane osobowe zgodnie z niniejszą umową, RODO oraz z innymi przepisami prawa powszechnie obowiązującego, które chronią prawa osób, których dane dotyczą.
3. Przetwarzający oświadcza, iż stosuje środki bezpieczeństwa spełniające wymogi RODO.

§ 2. Zakres i cel przetwarzania danych

1. Przetwarzający będzie przetwarzał, powierzone na podstawie umowy dane *(podać rodzaj danych)* ..... np. dane zwykłe w postaci ..... *(np. imion i nazwisk, adresu zamieszkania, nr PESEL itd.).*
2. Powierzone przez Administratora dane osobowe będą przetwarzane przez Przetwarzającego wyłącznie w celu ..... *(podać cel przetwarzania danych przez podmiot przetwarzający, np. realizacji umowy z dnia ..... nr ..... w zakresie prowadzenia kadr).*

§ 3. Obowiązki Przetwarzającego

1. Przetwarzający zobowiązuje się, przy przetwarzaniu powierzonych danych osobowych, do ich zabezpieczenia poprzez stosowanie odpowiednich środków technicznych i organizacyjnych zapewniających adekwatny stopień bezpieczeństwa odpowiadający ryzyku związanym z przetwarzaniem danych osobowych, o których mowa w art. 32 RODO.
2. Przetwarzający zobowiązuje się dołożyć należytej staranności przy przetwarzaniu powierzonych danych osobowych.

3. Przetwarzający zobowiązuje się do nadania upoważnień do przetwarzania danych osobowych wszystkim osobom, które będą przetwarzały powierzone dane w celu realizacji niniejszej umowy.
4. Przetwarzający zobowiązuje się zapewnić zachowanie w tajemnicy, (o której mowa w art. 28 ust 3 lit. b RODO) przetwarzanych danych przez osoby, które upoważnia do przetwarzania danych osobowych w celu realizacji niniejszej umowy, zarówno w trakcie zatrudnienia ich u Przetwarzającego, jak i po jego ustaniu.
5. Przetwarzający po zakończeniu świadczenia usług związanych z przetwarzaniem usuwa/zwraca Administratorowi wszelkie dane *osobowe (należy wybrać czy Przetwarzający ma usunąć czy zwrócić dane)* oraz usuwa wszelkie ich istniejące kopie, chyba że prawo Unii lub prawo państwa członkowskiego nakazują przechowywanie danych osobowych.
6. W miarę możliwości Przetwarzający pomaga Administratorowi w niezbędnym zakresie wywiązywać się z obowiązku odpowiadania na żądania osoby, której dane dotyczą oraz wywiązywania się z obowiązków określonych w art. 32-36 RODO.
7. Przetwarzający po stwierdzeniu naruszenia ochrony danych osobowych bez zbędnej zwłoki zgłasza je administratorowi w ciągu ..... *(można wskazać np. w ciągu 24 h).*

§ 4. Prawo kontroli

1. Administrator zgodnie z art. 28 ust. 3 lit. h RODO ma prawo kontroli, czy środki zastosowane przez Przetwarzającego przy przetwarzaniu i zabezpieczeniu powierzonych danych osobowych spełniają postanowienia umowy.
2. Administrator realizować będzie prawo kontroli w godzinach pracy Przetwarzającego i z minimum ..... *(wpisać z ilu dniowym wyprzedzeniem Administrator informuje o kontroli)* jego uprzedzeniem.
3. Przetwarzający zobowiązuje się do usunięcia uchybień stwierdzonych podczas kontroli w terminie wskazanym przez Administratora nie dłuższym niż ... dni *(administrator termin może określić dowolnie, np. 7 dni).*
4. Przetwarzający udostępnia Administratorowi wszelkie informacje niezbędne do wykazania spełnienia obowiązków określonych w art. 28 RODO.

§ 5. Dalsze powierzenie danych do przetwarzania

1. Przetwarzający może powierzyć dane osobowe objęte niniejszą umową do dalszego przetwarzania podwykonawcom jedynie w celu wykonania umowy po uzyskaniu uprzedniej pisemnej zgody Administratora.
2. Przekazanie powierzonych danych do państwa trzeciego może nastąpić jedynie na pisemne polecenie Administratora chyba, że obowiązek taki nakłada na Przetwarzającego prawo Unii lub prawo państwa członkowskiego, któremu podlega Przetwarzający. W takim przypadku przed rozpoczęciem przetwarzania Przetwarzający informuje Administratora o tym obowiązku prawnym, o ile prawo to nie zabrania udzielania takiej informacji z uwagi na ważny interes publiczny.
3. Podwykonawca, o którym mowa w ust. 1 umowy winien spełniać te same gwarancje i obowiązki jakie zostały nałożone na Przetwarzającego w niniejszej umowie.
4. Przetwarzający ponosi pełną odpowiedzialność wobec Administratora za nie wywiązanie się ze spoczywających na podwykonawcy obowiązków ochrony danych.

§ 6. Odpowiedzialność Przetwarzającego

1. Przetwarzający jest odpowiedzialny za udostępnienie lub wykorzystanie danych osobowych niezgodnie z treścią umowy, a w szczególności za udostępnienie powierzonych do przetwarzania danych osobowych osobom nieupoważnionym.
2. Przetwarzający zobowiązuje się do niezwłocznego poinformowania Administratora o jakimkolwiek postępowaniu, w szczególności administracyjnym lub sądowym, dotyczącym przetwarzania przez Przetwarzającego danych osobowych określonych w umowie, o jakiejkolwiek decyzji administracyjnej lub orzeczeniu dotyczącym przetwarzania tych danych, skierowanych do

Przetwarzającego, a także o wszelkich planowanych, o ile są wiadome, lub realizowanych kontrolach i inspekcjach dotyczących przetwarzania u Przetwarzającego tych danych osobowych, w szczególności prowadzonych przez inspektorów upoważnionych przez Prezesa Urzędu Ochrony Danych Osobowych. *Niniejszy ustęp dotyczy wyłącznie danych osobowych powierzonych przez Administratora.*

§ 7. Czas obowiązywania umowy

1. Niniejsza umowa obowiązuje od dnia jej zawarcia przez czas nieokreślony/określony od ..... do .....
2. Każda ze Stron może wypowiedzieć niniejszą umowę z zachowaniem ..... okresu wypowiedzenia.

§ 8. Rozwiązanie umowy

1. Administrator może rozwiązać niniejszą umowę ze skutkiem natychmiastowym gdy Przetwarzający:
a) pomimo zobowiązania go do usunięcia uchybień stwierdzonych podczas kontroli nie usunie ich w wyznaczonym terminie,
b) przetwarza dane osobowe w sposób niezgodny z umową,
c) powierzył przetwarzanie danych osobowych innemu podmiotowi bez zgody Administratora.

§ 9. Zasady zachowania poufności

1. Przetwarzający zobowiązuje się do zachowania w tajemnicy wszelkich informacji, danych, materiałów, dokumentów i danych osobowych otrzymanych od Administratora i od współpracujących z nim osób oraz danych uzyskanych w jakikolwiek inny sposób, zamierzony czy przypadkowy w formie ustnej, pisemnej lub elektronicznej („dane poufne").
2. Przetwarzający oświadcza, że w związku ze zobowiązaniem do zachowania w tajemnicy danych poufnych nie będą one wykorzystywane, ujawniane ani udostępniane bez pisemnej zgody Administratora w innym celu niż wykonanie umowy, chyba że konieczność ujawnienia posiadanych informacji wynika z obowiązujących przepisów prawa lub umowy.

§10. Postanowienia końcowe

1. Umowa została sporządzona w dwóch jednobrzmiących egzemplarzach dla każdej ze Stron.
2. W sprawach nieuregulowanych zastosowanie będą miały przepisy Kodeksu cywilnego oraz RODO.
3. Sądem właściwym dla rozpatrzenia sporów wynikających z niniejszej umowy będzie sąd właściwy Administratora (lub Przetwarzającego w zależności od postanowień stron).

.....	.....
Administrator	Przetwarzający

Załącznik Nr 14 do Zarządzenia

Dyrektora Zespołu Zawodowych
w Rawiczu

Wzór ogólny

ZGODA NA PRZETWARZANIE DANYCH OSOBOWYCH

Wyrażam zgodę na przetwarzanie moich danych osobowych w zakresie .....(wskazać rodzaj danych: imię i nazwisko, adres zamieszkania, PESEL, imiona rodziców, dane kontaktowe itp.) przez Zespół Szkół Zawodowych w Rawiczu, ul. ....., na potrzeby/ w celu .....(podać cel przetwarzania np. proces rekrutacji do pracy, proces rekrutacji do szkoły itp.)

Informacja od Administratora – Zespół Szkół Zawodowych w Rawiczu:

Ma Pan/Pani prawo do dostępu do swoich danych osobowych, do ich sprostowania, żądania ich usunięcia lub wniesienia sprzeciwu z powodu szczególnej sytuacji. Ma Pan/Pani również prawo do żądania od Nas ograniczenia przetwarzania Pana/Pani danych, a także do ich przenoszenia.

Jeżeli uzna Pan/Pani, że dane osobowe są przetwarzane niezgodnie z wymogami prawa ma Pan/Pani prawo wnieść skargę do organu nadzorczego, którym jest Prezes Urzędu Ochrony Danych Osobowych.

Podstawą prawną przetwarzania Pani/Pana danych osobowych jest art. 6 ust. 1 lit a RODO, tj. osoba, której dane dotyczą wyraziła zgodę na przetwarzanie swoich danych osobowych w jednym lub większej liczbie określonych celów.

Pana/Pani dane osobowe będą przechowywane przez okres niezbędny do realizacji celów....., lecz nie krócej niż okres wskazany w przepisach o archiwizacji (.....lat)

Pana/Pani dane osobowe będą przetwarzane w sposób częściowo zautomatyzowany, ponieważ będziemy w pewnym stopniu je przetwarzać na zasobach komputerowych. Jednakże w ramach przetwarzania danych nie stosujemy metod polegających na zautomatyzowanym podejmowaniu decyzji, w tym profilowania.

Podanie danych jest dobrowolne, jednak jest ono konieczne dla załatwienia sprawy.

.....

(podpis osoby wyrażającej zgodę/rodzica/opiekuna/pełnoletniego ucznia)

Załącznik Nr 15 do Zarządzenia

Dyrektora Zespołu Szkół Zawodowych w Rawiczu

....., dnia ..... r.

.....

(pieczęć Administratora)

ZGODA NA PRZETWARZANIE DANYCH OSOBOWYCH UCZNIA

.....

(imię i nazwisko rodzica/opiekuna niepełnoletniego ucznia)

.....

(imię i nazwisko ucznia)

Na podstawie art. 6 ust. 1 lit. a Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych osobowych, tzw. RODO), wyrażam zgodę na przetwarzanie moich danych osobowych, w tym rozpowszechniania, przez Administratora – Zespół Szkół Zawodowych w Rawiczu:

CEL PRZETWARZANIA	TAK	NIE	PODPIS
Prowadzenie strony internetowej Administratora/Facebooka (zakres przetwarzanych danych: imię, nazwisko, wizerunek, klasa)			
Realizacja projektów/wymian uczniowskich (zakres przetwarzanych danych: imiona, nazwisko, wizerunek, miejsce zamieszkania, numer telefonu, data i miejsce urodzenia, imiona i nazwiska rodziców, adres zamieszkania rodziców, nr telefonu rodziców, nr PESEL, klasa)			
Działania promocyjne, w tym prowadzenie kroniki szkolnej (prasa i inne media) (zakres przetwarzanych danych: imię, nazwisko, klasa, wizerunek)			
Udział w konkursach, wycieczkach, imprezach i innych wydarzeniach szkolnych i publikowanie informacji o tych wydarzeniach (zakres przetwarzanych danych: imię, nazwisko, klasa, wizerunek, miejsce zamieszkania, numer telefonu)			
Przygotowanie identyfikatora uczniowskiego (imię, nazwisko, klasa, wizerunek)			
Prowadzenie tablic i gablot informacyjnych (imię i nazwisko, klasa, wizerunek)			
Realizacja umów partnerskich, porozumień itp. (zakres przetwarzanych danych: imiona, nazwisko, wizerunek, miejsce zamieszkania, numer telefonu, data i miejsce urodzenia, nr PESEL)			

Oświadczam, że dane osobowe podaję dobrowolnie i oświadczam, że zapoznałem(-am) się z treścią klauzuli informacyjnej umieszczonej na stronie internetowej Administratora lub w siedzibie Administratora, w tym z informacją o celach i sposobach przetwarzania danych osobowych oraz prawie dostępu do treści swoich danych i prawie ich poprawiania. Ponadto Administrator poinformował mnie, że:

- niniejsza zgoda może zostać cofnięta w dowolnym momencie poprzez złożenie oświadczenia w tej samej formie, w jakiej zgoda została wyrażona. Wycofanie zgody nie wpływa na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej wycofaniem,
- dane osobowe przetwarzane na podstawie niniejszej zgody nie będą podlegały zautomatyzowanemu podejmowaniu decyzji, w tym profilowaniu.

.....
..... *(podpis rodzica/opiekuna/pełnoletniego ucznia)*

Załącznik Nr 16 do Zarządzenia

Dyrektora Zespołu Zawodowych
w Rawiczu

Rejestr zawartych umów powierzenia przetwarzania danych osobowych – wzór

Lp.	Nazwa i dane kontaktowe podmiotu z którym zawarto umowę	Data zawarcia umowy	Czas trwania przetwarzania	Rodzaj danych osobowych i kategoria osób których dotyczą

Załącznik Nr 17 do Zarządzenia

Dyrektora Zespołu Zawodowych
w Rawiczu

Rejestr zawartych umów powierzenia przetwarzania danych osobowych – wzór

Lp.	Ir	Nazwa i dane kontaktowe podmiotu z którym zawarto umowę	Data zawarcia umowy	Czas trwania przetwarzania	Rodzaj danych osobowych i kategoria osób których dotyczą

Załącznik Nr 18 do Zarządzenia

Dyrektora Zespołu Zawodowych
w Rawiczu

Rejestr zgód na przetwarzanie danych osobowych - wzór

Lp	Imię i nazwisko osoby, której dane dotyczą	Rodzaj danych osobowych	Data udzielenia zgody	Data wycofania/wygaśniecia zgody

Załącznik Nr 19 do Zarządzenia

Dyrektora Zespołu Zawodowych
w Rawiczu

WNIOSEK
O UDOSTĘPNIENIE DANYCH ZE ZBIORU DANYCH - wzór

1. Wniosek do..... – Administrator Danych Osobowych

2. Wnioskodawca.....

3. Podstawa prawna upoważniająca do pozyskania danych

   .....

4. Wskazanie przeznaczenia dla udostępnienia danych

   .....

5. Oznaczenie lub nazwa zbioru, z którego mają być udostępnione dane

   .....

6. Zakres żądanych informacji ze zbioru

   .....

7. Informacje umożliwiające wyszukanie w zbiorze żądanych danych

   .....

Załącznik Nr 20 do Zarządzenia

Dyrektora Zespołu Zawodowych
w Rawiczu

Rejestr udostępnień danych osobowych - wzór

Lp	Wnioskodawca	Data złożenia wniosku	Rodzaj danych osobowych i kategorie osób których dotyczą	Data udostępnienia danych bądź odmowy udostępnienia

Załącznik Nr 21 do Zarządzenia

Dyrektora Zespołu Zawodowych
w Rawiczu

Wzór ogólny

KLAUZULA INFORMACYJNA

Zgodnie z art. 13 ust. 1 i 2 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz.Urz. UE z 2016 r., seria L, nr 119) informujemy, że:

I. Administratorem danych osobowych przetwarzanych w Zespole Szkół Zawodowych w Rawiczu jest Zespół Szkół Zawodowych, siedziba w Rawiczu, ul. .....;

II. Inspektorem Ochrony Danych jest ....., e-mail: inspektor@powiat-miedzychodzki.pl;

III. Dane osobowe są przetwarzane w celu realizacji zadań wynikających z przepisów prawa;

IV. Dane osobowe mogą być przekazywane innym organom i podmiotom wyłącznie na podstawie przepisów prawa.

V. Dane osobowe mogą być przetwarzane przez okres wynikający z kategorii archiwalnej (okres przechowywania dokumentacji, zgodnie z zał. Nr 3 do Rozporządzenia Prezesa Rady Ministrów z dnia 18 stycznia 2011r. w sprawie instrukcji kancelaryjnej, jednolitych rzeczowych wykazów akt oraz instrukcji w sprawie organizacji i zakresu działania archiwów zakładowych);

VI. Każdy ma prawo dostępu do treści swoich danych osobowych, ich poprawiania i sprostowania;

VII. Każdy, którego dane osobowe są przetwarzane w Zespole Szkół Zawodowych w Rawiczu ma prawo wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych, gdy przetwarzanie jego danych naruszałoby przepisy ogólnego rozporządzenia o ochronie danych osobowych z dnia 26 kwietnia 2016r. (RODO);

VIII. Podanie danych osobowych jest obowiązkiem ustawowym. Każdy zainteresowany zobowiązany jest do podania swoich danych osobowych, których zakres wynika z przepisów prawa, a konsekwencją niepodania danych osobowych będzie pozostawienie sprawy bez rozpatrzenia.

IX. Pani/Pana dane nie będą przetwarzane w sposób zautomatyzowany, w tym również nie będą profilowane.

Załącznik Nr 22 do Zarządzenia

Dyrektora Zespołu Zawodowych
w Rawiczu

Potwierdzenie otrzymania dostępu do kont rodzica/opiekuna i ucznia/uczennicy oraz zapoznania się z zasadami funkcjonowania dziennika elektronicznego.

Potwierdzam otrzymanie dostępu (loginów i haseł) do swoich kont (rodzica/prawnego opiekuna oraz ucznia/uczennicy) oraz zapoznanie mnie z zasadami funkcjonowania dziennika elektronicznego w Zespole Szkół Zawodowych im. S. Bobrowskiego w Rawiczu .

Klasa: .....
Rok szkolny: .....

Rodzic musi podpisać się czytelnie, pełnym imieniem i nazwiskiem, gdyż podpis ten będzie traktowany jako wzór podpisu rodzica/opiekuna dziecka.

Lp.	Imię i nazwisko ucznia/uczennicy	Imię i nazwisko rodzica/opiekuna	Czytelny podpis rodzica lub prawnego opiekuna
1.			
2.			
3.			
4.			
5.			
6.			
7.			
8.			
9.			
10.			

Załącznik Nr 23

do Zarządzenia Nr .....
Dyrektora Zespołu Szkół Zawodowych w
Rawiczu

.....
(pieczęć Administratora)

Zgoda na korzystanie ze sprzętu stanowiącego własność pracodawcy poza miejscem pracy

Mając na uwadze potrzeby Administratora związane z organizacją prowadzonej przez niego działalności, **niniejszym wyrażam:**

Pani/Panu .....
(imię i nazwisko)

zgodę na korzystanie i wynoszenie następującego sprzętu IT poza miejsce pracy:

LP	Nr zgody na korzystanie ze sprzętu IT	Nr w rejestrze wydania sprzętu IT	Rodzaj/typ sprzętu IT	Powody wyrażenia zgody	Miejsca, w które może być wynoszony sprzęt

na czas wykonywania następujących obowiązków lub poleceń Administratora:
.....
.....
.....
to jest do dnia .....
zgodnie z przepisami prawa i zasadami ochrony danych osobowych wprowadzonymi przez Administratora.
Środki organizacyjne, gwarantujące przetwarzanie danych osobowych zgodnie z przepisami prawa i zasadami ochrony danych osobowych wprowadzonymi przez Administratora, w szczególności w sposób chroniący prawa osób, których dane dotyczą są zapewnione, jeśli co najmniej:

- jedyną osobą mającą dostęp do sprzętu IT, którego dotyczy udzielona zgoda, jest użytkownik, który tę zgodę uzyskał,
- sprzęt IT nie będzie podłączany do publicznych (w szczególności niezabezpieczonych) sieci WI-FI,
- w przypadku konieczności połączenia z siecią internetową, sprzęt IT będzie podłączony do prywatnych, zabezpieczonych hasłem sieci WI-FI, a gdy tylko jest to możliwe, sprzęt IT będzie podłączony przez VPN (wirtualna sieć prywatna szyfrująca dane przesyłane przez sieć internetową),
- sprzęt IT nie będzie pozostawiany bez nadzoru, w szczególności w pojazdach prywatnych, środkach komunikacji publicznej, na konferencjach itd.,

- na czas wynoszenia sprzętu IT, znajdować się na nim mogą wyłącznie te dane osobowe i dokumenty, które są niezbędne do wykonania tych konkretnych obowiązków lub poleceń Administratora, w wykonaniu których użytkownik wynosi sprzęt IT,
- w przypadku każdej przerwy w korzystaniu ze sprzętu IT niewymagającej wyłączenia sprzętu IT, użytkownik stosuje blokady ekranu lub wylogowuje się w taki sposób, aby nie było możliwe skorzystanie ze sprzętu przez inną osobę,
- korzysta ze sprzętu IT w sposób uniemożliwiający osobom trzecim podejrzenie zawartości sprzętu IT i danych osobowych,
- podejmuje wszelkie inne środki mające na celu zabezpieczenie sprzętu IT i przetwarzanych danych osobowych, które w danej sytuacji powinny zostać podjęte.

Jednocześnie zobowiązuję Panią/Pana do korzystania z powierzonego sprzętu jedynie w celach wynikających z łączącej Panią/Pana umowy z Administratorem oraz niniejszej zgody, w miejscach i w okresie wskazanych powyżej, a także wyłącznie, gdy jest to niezbędne do wykonywania obowiązków lub poleceń wskazanych powyżej.
Zgoda wygasa z chwilą ustania Pana/Pani zatrudnienia lub współpracy (bez względu na podstawę prawną zatrudnienia lub współpracy) lub odwołania zgody.

.....
(data i podpis Dyrektora)

OŚWIADCZENIE

W związku z udzieloną mi powyższą zgodą **oświadczam**, że zobowiązuję się do korzystania z niej jedynie celach wynikających z łączącej mnie umowy z Administratorem oraz z niniejszej zgody, w miejscach i w okresie wskazanych w udzielonej zgodzie, a także wyłącznie, gdy jest to niezbędne do wykonywania obowiązków lub poleceń Administratora wskazanych w treści zgody.
Zobowiązuję się do korzystania ze wynoszonego sprzętu IT zgodnie z przepisami prawa i zasadami ochrony danych osobowych wprowadzonymi przez Administratora.
Ponadto **zobowiązuję się** do dysponowania w odniesieniu do wynoszonego sprzętu IT, którego dotyczy udzielona mi zgoda, odpowiednimi środkami organizacyjnymi gwarantującymi przetwarzanie danych osobowych zgodnie z przepisami prawa i zasadami ochrony danych osobowych wprowadzonymi przez Administratora. Oświadczam, że będę przetwarzać dane osobowe wyłącznie w sposób chroniący prawa osób, których dane dotyczą.

.....
(data i podpis danej osoby)

Załącznik Nr 24

do Zarządzenia Nr .....
Dyrektora Zespołu Szkół Zawodowych w Rawiczu

Rejestr wydania sprzętu IT do używania poza siedzibą pracodawcy - wzór

Lp.	Imię i nazwisko	Stanowisko	Nr udzielonej zgody	Rodzaj sprzętu IT	Data udzielenia zgody

Załącznik Nr 25

do Zarządzenia Nr .....
Dyrektora Zespołu Szkół Zawodowych w Rawiczu

Regulamin korzystania z kont w usłudze G Suite przez uczniów Zespołu Szkół Zawodowych im. Stefana Bobrowskiego w Rawiczu

§ 1 Postanowienia ogólne

1. Niniejszy regulamin określa w szczególności:
a) zasady przyznania konta w usłudze G Suite dla Szkół i Uczelni,
b) zasady korzystania z konta w usłudze G Suite dla Szkół i Uczelni przez uczniów,
c) zakres i uprawnienia dyrektora, dotyczące kont w usłudze G Suite dla Szkół i Uczelni,
d) postanowienia końcowe.
2. Usługa G Suite dla Szkół i Uczelni to zintegrowane rozwiązanie do komunikacji i współpracy, w ramach którego Google oferuje hostowane usługi poczty e-mail, kalendarza, czatu, dysku i innych działających w oparciu o tzw. chmurę.
3. Administratorem danych osobowych jest Zespół Szkół Zawodowych im. Stefana Bobrowskiego w Rawiczu.
4. Użytkowanie przez niepełnoletnich uczniów konta w oparciu o rozwiązania G Suite dla Szkół i Uczelni wiąże się z akceptacją Warunków korzystania z usługi Google oraz Polityki prywatności Google.
5. Konta w usłudze G Suite dla Szkół i Uczelni tworzone są w domenie zszrawicz.pl

§ 2 Zasady przyznania uczniowi konta w usłudze GSuite dla Szkół i Uczelni

1. Konta w usłudze GSuite dla Szkół i Uczelni tworzone będą według wzorca: imię.nazwisko(bez polskich znaków)@zszrawicz.pl
2. W przypadku powtórzenia się nazwy użytkownika, na jej końcu dodawana będzie kolejna liczba naturalna.
3. Każdy uczeń ZSZ w Rawiczu otrzymuje dostęp do konta w usłudze GSuite dla Szkół i Uczelni na czas edukacji w szkole.
4. Utworzenie oraz użytkowanie konta w usłudze GSuite dla Szkół i Uczelni przez ucznia wiąże się z:
a) wyrażeniem zgody jego rodziców (prawnych opiekunów) lub pełnoletniego ucznia na założenie i używanie konta w usłudze GSuite dla Szkół i Uczelni - załącznik nr 1 lub załącznik 2
b) akceptacją przez ucznia postanowień niniejszego regulaminu - załącznik nr 1.

5. Osobę zarządzającą kontami uczniów, zwaną dalej szkolnym administratorem usługi GSuite dla Szkół i Uczelni, wyznacza dyrektor szkoły. Administrator przekazuje użytkownikom szczegóły dotyczące pierwszego logowania oraz hasła startowe .

§ 3 Zasady korzystania z usługi GSuite dla Szkół i Uczelni

1. Konto w usłudze G Suite dla Szkół i Uczelni może być wykorzystywane przez ucznia między innymi w celu:
   a) realizacji wymagań podstawy programowej,
   b) zakładania kont i logowania w serwisach edukacyjnych,
   c) korzystania z usług elektronicznych służących pogłębianiu wiedzy i umiejętności w zakresie technologii informacyjno-komunikacyjnych,
   d) komunikacji z innymi uczniami i nauczycielami szkoły.
2. Użytkownik zobowiązuje się do wykorzystywania konta zgodnie z obowiązującymi przepisami prawa, normami społecznymi i obyczajowymi, postanowieniami niniejszego Regulaminu oraz zasadami netykiety, a w szczególności do:
   a) działania w sposób nie naruszający praw innych użytkowników (takich jak prawo do ochrony prywatności i wizerunku),
   b) nierozsyłania z konta niechcianej przez innych użytkowników korespondencji (spamu),
   c) nieużywania konta usługi do nielegalnego udostępniania plików,
   d) nieprzenoszenia na osoby trzecie prawa do korzystania z konta.
3. Dostęp do konta możliwy jest za pomocą:
   a) przeglądarki internetowej lub https://www.google.pl,
   b) programów pocztowych do obsługi poczty elektronicznej.
4. W razie utraty możliwości logowania się do usług Google Suitę należy bezzwłocznie powiadomić o tym szkolnego administratora lub wychowawcę klasy.
5. Konta utworzone w usłudze GSuite dla Szkół i Uczelni oraz powiązane z nimi dane (w tym dokumenty, materiały itp.) będą usuwane w następujących przypadkach:
   a) w przypadku nauczyciela i pracownika administracji: ustanie stosunku pracy ze szkołą,
   b) w przypadku ucznia: po zakończeniu edukacji w szkole.
6. Użytkownik zobowiązuje się do wykorzystywania konta zgodnie z obowiązującymi przepisami prawa, normami społecznymi i obyczajowymi, postanowieniami niniejszego Regulaminu oraz zasadami netykiety, a w szczególności do:
   a) działania w sposób nienaruszający praw innych użytkowników (takich jak prawo do ochrony prywatności i wizerunku),
   b) nierozsyłania z konta niechcianej przez innych użytkowników korespondencji (spamu),
   c) nieużywania konta usługi do nielegalnego udostępniania plików,
   d) nieprzenoszenia na osoby trzecie prawa do korzystania z konta.

§ 4 Zakres i uprawnienia dyrektora dotyczące kont w usłudze GSuite dla Szkół i Uczelni

1. Z uwagi na konieczność zapewnienia ochrony interesu i bezpieczeństwa szkoły dyrektor zastrzega sobie prawo kontroli i wglądu we wszystkie działania związane z użytkowaniem przez uczniów kont w usłudze GSuite dla Szkół i Uczelni.
2. Kontrola odbywa się z poszanowaniem prawa do prywatności i ochrony danych.
3. Dyrektor ma prawo również kontroli przestrzegania zasad korzystania z kont określonych w niniejszym Regulaminie.

§ 5 Postanowienia końcowe

1. Szkoła zastrzega sobie prawo do:
   1) zmian postanowień niniejszego Regulaminu,
   2) usuwania kont uczniów, którzy przestają być uczniami szkoły w terminie do dwóch miesięcy od zakończenia zajęć edukacyjnych,
   3) zablokowania kont uczniów w przypadkach wykorzystania ich w sposób niezgodny z przeznaczeniem lub sprzeczny z szeroko rozumianym interesem szkoły, w szczególności może to dotyczyć:
      a) zachowań naruszających zasady wymienione w niniejszym Regulaminie,

b) zachowań naruszających inne zasady i regulaminy użytkowania sieci komputerowych szkoły,
c) naruszania ogólnie przyjętych zasady współistnienia użytkowników sieci Internet

Załącznik Nr 26

do Zarządzenia Nr .....
Dyrektora Zespołu Szkół Zawodowych w Rawiczu

ZGODA RODZICA LUB PRAWNEGO OPIEKUNA NA KORZYSTANIE Z KONTA GSUITE

Wyrażam zgodę na założenie mojemu dziecku: (imię i nazwisko)
uczniowi klasy ..... konta GSuite dla Szkół i Uczelni oraz na zarządzanie tym
kontem przez Zespół Szkół Zawodowych im. Stefana Bobrowskiego w Rawiczu.
Jednocześnie potwierdzam, iż zapoznałam/em się z informacjami dla rodzica lub opiekuna na temat
GSuite dla Szkół i Uczelni zamieszczonymi na stronie szkoły.
Uczeń korzystający z ww. konta akceptuje postanowienia zawarte w Regulaminie korzystania z kont w usłudze GSuite dla Szkół i Uczelni przez uczniów Zespołu Szkół Zawodowych im. St. Bobrowskiego w Rawiczu,

czytelny podpis rodzica lub prawnego opiekuna

ZGODA PEŁNOLETNIEGO UCZNIA NA KORZYSTANIE Z KONTA GSUITE

(imię i nazwisko)..... z klasy.....

Wyrażam zgodę na założenie konta GSuite dla Szkół i Uczelni oraz na zarządzanie tym kontem przez Zespół Szkół Zawodowych im. Stefana Bobrowskiego w Rawiczu.
Jednocześnie potwierdzam, iż zapoznałam/em się z informacjami na temat GSuite dla Szkół i Uczelni zamieszczonymi na stronie szkoły.
Korzystając z ww. konta akceptuje postanowienia zawarte w Regulaminie korzystania z kont w usłudze GSuite dla Szkół i Uczelni przez uczniów Zespołu Szkół Zawodowych im. St. Bobrowskiego w Rawiczu.

czytelny podpis ucznia