KSIĘGA PROCEDUR I REGULAMINÓW
regulujących bezpieczeństwo danych w warunkach zdalnej nauki/pracy
(Dokumentacja ochrony danych osobowych w zdalnym nauczaniu/pracy)

1. Uzasadnienie celowości wprowadzenia zmian w dokumentacji RODO w zdalnym nauczaniu i/lub zdalnej pracy.
2. Instrukcja do pracy z danymi osobowymi w okresie pandemii.
3. Procedura bezpiecznego przetwarzania danych osobowych w zdalnej nauce.
4. Klauzula informacyjna o przetwarzaniu danych osobowych w zdalnym nauczaniu.
5. Karty rejestrów czynności przetwarzania w nauce na odległość.
6. Analiza ryzyka naruszenia ochrony danych w zdalnym nauczaniu.

1. Uzasadnienie celowości wprowadzenia zmian w dokumentacji RODO w zdalnym nauczaniu i/lub zdalnej pracy.

1.1. Wstęp

Prowadzenie procesu dydaktyczno-wychowawczego lub/i wykonywanie pracy zdalnej przez pracowników administracji szkoły nie wiąże się wyłącznie ze zmianą narzędzi, za pomocą których proces jest realizowany/praca jest świadczona, ale zwykle stanowi również zmianę sposobu przetwarzania danych osobowych, co w konsekwencji powinno być poprzedzone analizą ryzyka i kompleksową weryfikacją zgodności przyjętych rozwiązań z RODO, w tym sposobów zapewnienia bezpieczeństwa przetwarzanych danych osobowych.

Wewnętrzne polityki RODO – wcześniej opracowane i wdrożone – nie uwzględniały zmienionego charakteru i kontekstu przetwarzania danych (edukacja zdalna, ocenianie uczniów zdalnie, wykorzystywanie platform edukacyjnych, w tym przesyłania danych do państw trzecich, gdy placówka korzysta np. z Microsoft 365, Microsoft Teams'a)

Wypracowane nowe regulacje wewnętrzne bądź rozszerzenie już istniejących polityk pozwoli na osiągnięcie następujących celów:

1) przetwarzanie danych osobowych pozostanie w zgodności z przepisami prawa, a w szczególności z przestrzeganiem zasad przetwarzania wg RODO, określonych w art. 5 ust. 1;
2) zapewnienie „rozliczalności" na gruncie RODO – art. 5 ust. 2 RODO (ust.2. Administrator jest odpowiedzialny za przestrzeganie przepisów ust. 1 i musi być w stanie wykazać ich przestrzeganie („rozliczalność");
3) wdrożenie ujednoliconych i spójnych reguł bezpieczeństwa;
4) wspieranie nauczycieli i pracowników pracujących zdalnie;
5) przeciwdziałanie odpowiedzialności prawnej;
6) prowadzenie ewaluacji organizacji nauki/pracy zdalnej.

Praca zdalna wymaga wypracowania specyficznych dla niej procedur, o ile rozwiązania jej dotyczące nie zostały przewidziane w politykach obowiązujących wcześniej u administratora.

Dane osobowe muszą by 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 (art. 5 ust. 1. lit. f RODO).

1.2. Przepisy prawa wskazujące konieczność uregulowania

Praca zdalna nie powinna bowiem oznaczać zmniejszonej kontroli nad przetwarzaniem danych osobowych oraz nad zmianami w zbiorach danych, rozliczalnością operacji przetwarzania danych osobowych dokonywanych przez poszczególnych użytkowników czy rezygnacji z uwierzytelniania użytkowników w systemach informatycznych z dookreśleniem tego, do jakich czynności są oni uprawnieni w poszczególnych systemach.

Wykonywanie pracy zdalnej przez pracowników nie wiąże się wyłącznie ze zmianą narzędzi, za pomocą których praca jest świadczona, ale zwykle stanowi również zmianę sposobu przetwarzania danych osobowych, a w konsekwencji powinno być poprzedzone analizą ryzyka i kompleksową weryfikacją zgodności przyjętych rozwiązań z RODO, w tym sposobów zapewnienia bezpieczeństwa przetwarzanych danych osobowych.

Zgodnie z art. 24 ust. 1 RODO to administrator wdraża odpowiednie środki techniczne i organizacyjne, uwzględniając charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie i wadze, aby przetwarzanie odbywało się zgodnie z RODO i aby móc to wykazać, środki te zaś są w razie

potrzeby poddawane przeglądom i uaktualniane oraz – jak wynika to z art. 24 ust. 2 – opisywane w odpowiednich politykach.

Zbliżone obowiązki wprowadza art. 25 ust. 1 RODO, który zobowiązuje do uwzględnienia ochrony danych osobowych w fazie projektowania, przy czym kwalifikowany jako ów projektowany sposób przetwarzania, określany przez pracodawcę może być praca zdalna.

Natomiast art. 32 RODO nakazuje odpowiednio administratorowi i podmiotowi przetwarzającemu odpowiednio zabezpieczyć przetwarzane dane i dokonać szacowania ryzyka naruszenia ich bezpieczeństwa.

Artykuł 24
Obowiązki administratora

1. Uwzględniając charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie i wadze zagrożenia, administrator wdraża odpowiednie środki techniczne i organizacyjne, aby przetwarzanie odbywało się zgodnie z niniejszym rozporządzeniem i aby móc to wykazać. Środki te są w razie potrzeby poddawane przeglądom i uaktualniane.
2. Jeżeli jest to proporcjonalne w stosunku do czynności przetwarzania, środki, o których mowa w ust. 1, obejmują wdrożenie przez administratora odpowiednich polityk ochrony danych.

Artykuł 25
Uwzględnianie ochrony danych w fazie projektowania oraz domyślna ochrona danych

1. Uwzględniając stan wiedzy technicznej, koszt wdrażania oraz charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia wynikające z przetwarzania, administrator – zarówno przy określaniu sposobów przetwarzania, jak i w czasie samego przetwarzania – wdraża odpowiednie środki techniczne i organizacyjne, takie jak pseudonimizacja, zaprojektowane w celu skutecznej realizacji zasad ochrony danych, takich jak minimalizacja danych, oraz w celu nadania przetwarzaniu niezbędnych zabezpieczeń, tak by spełnić wymogi niniejszego rozporządzenia oraz chronić prawa osób, których dane dotyczą.
2. Administrator wdraża odpowiednie środki techniczne i organizacyjne, aby domyślnie przetwarzane były wyłącznie te dane osobowe, które są niezbędne dla osiągnięcia każdego konkretnego celu przetwarzania. Obowiązek ten odnosi się do ilości zbieranych danych osobowych, zakresu ich przetwarzania, okresu ich przechowywania oraz ich dostępności. W szczególności środki te zapewniają, by domyślnie dane osobowe nie były udostępniane bez interwencji danej osoby nieokreślonej liczbie osób fizycznych.

Artykuł 32
Bezpieczeństwo przetwarzania

1. Uwzględniając stan wiedzy technicznej, koszt wdrażania oraz charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia, administrator i podmiot przetwarzający wdrażają odpowiednie środki techniczne i organizacyjne, aby zapewnić stopień bezpieczeństwa odpowiadający temu ryzyku, w tym między innymi w stosownym przypadku:
   a) pseudonimizację i szyfrowanie danych osobowych;
   b) zdolność do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów i usług przetwarzania;
   c) zdolność do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego;
   d) regularne testowanie, mierzenie i ocenianie skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania.

2. Oceniając, czy stopień bezpieczeństwa jest odpowiedni, uwzględnia się w szczególności ryzyko wiążące się z przetwarzaniem, w szczególności wynikające z przypadkowego lub niezgodnego z prawem zniszczenia, utraty, modyfikacji, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych.

2. Instrukcja do pracy z danymi osobowymi w okresie pandemii w Szkole Podstawowej im. ks. Jana Twardowskiego w Powidzku

I. Postanowienia ogólne

§ 1

1. Niniejszy regulamin określa zasady podejmowania i realizowania pracy zdalnej oraz stacjonarnej w okresie epidemii w Szkole Podstawowej im. ks. Jana Twardowskiego w Powidzku.

2. W regulaminie pod określeniem "pracownik" należy rozumieć zarówno osoby zatrudnione w ramach stosunku pracy, jak i współpracowników, na stale wykonujących zadania w ramach umów cywilnoprawnych wymagające dostępu do zasobów sprzętowych i informacyjnych szkoły.

II. Warunki pracy stacjonarnej w okresie zagrożenia epidemicznego

§ 2

1. Dyrektor szkoły ustala grafik obecności w pracy, którego pracownik jest zobligowany bezwzględnie przestrzegać, ze względu na konieczność zapewnienia swojego oraz współpracowników bezpieczeństwa pracy.
2. Każda wizyta w pracy poza ustanowionym grafikiem musi zostać zgłoszona pracodawcy z co najmniej 2 dniowym wyprzedzeniem i uprzednio zatwierdzona przez pracodawcę.
3. Osoby przeziębione, kaszlące, gorączkujące, czujące duszności, powinny pozostać w domu i w zależności od samopoczucia podjąć pracę zdalną lub skontaktować się z lekarzem.
4. W celu zapewnienia bezpiecznych oraz komfortowych warunków pracy, pracownik powinien niezwłocznie zgłaszać pracodawcy, że źle się czuje, w szczególności, jeżeli objawy go niepokoją, bo są tożsame z tymi świadczącymi o zachorowaniu na COVID-19. W takim wypadku należy przerwać pracę i jak najszybciej opuścić budynek szkoły.
5. W przypadku zaobserwowania niepojących objawów u innego współpracownika lub gościa, należy niezwłocznie zgłosić ten fakt pracodawcy oraz osobom odpowiedzialnym za bezpieczeństwo w biurze.
6. Ze względu na obowiązek zakrywania nosa i ust weryfikacja tożsamości osób wchodzących do szkoły jest utrudniona. W związku z tym każdy pracownik jest zobligowany na żądanie pracownika do okazania dokumentu potwierdzającego tożsamość lub odsłonięcia twarzy, w zależności od instrukcji osoby weryfikującej tożsamość. W trakcie tego procesu należy zachować bezpieczną odległość (min. 2 metry).
7. Na stanowisku pracy należy zachować jak najwyższe standardy higieny. Możliwe często dezynfekować powierzchnie i przedmioty, których się dotyka, dezynfekować dłonie, unikać dotykania twarzy. Dotyczy to także sytuacji, gdy dotykało się tych samych dokumentów, które dotykały inne osoby.
8. Należy korzystać tylko i wyłącznie z wyznaczonego stanowiska pracy. Powinno ono być oddalone od stanowisk pracy innych osób co najmniej o 2 metry. Jednocześnie ustawienie sprzętu komputerowego i dokumentów powinno uwzględniać zapewnienie ich należytej ochrony przed osobami nieuprawnionymi.

9. Należy unikać zatłoczonych miejsc i podejmować działania minimalizujące ryzyko przebywania w takich miejscach bez zachowania zalecanego dystansu. Szczególnie dotyczy to przejść, wind, korytarzy, pomieszczeń socjalnych, toalet.
10. Należy bezwzględnie przestrzegać ograniczeń w zakresie liczby osób przebywających w pomieszczeniu, w szczególności ograniczać liczbę interesantów, tak by było możliwe zachowanie bezpiecznego dystansu pomiędzy wszystkimi osobami przebywającymi w pomieszczeniu.
11. W przypadku konieczności pracy z dokumentami papierowymi, należy stosować wobec zawartych w nich informacji najwyższe standardy ochrony, w szczególności zapewnić, aby nie były udostępniane (pozostawione bez opieki, pozostawione w sposób, który może być dowolnie modyfikowany i dostosowywany umożliwiający zapoznanie się z treścią) osobom postronnym. Te same standardy dotyczą wszelkich kopii dokumentów. Po zakończeniu pracy z dokumentem lub jego kopią, która już nie jest potrzebna i nie wymaga dalszego przechowywania, należy dokument niezwłocznie zniszczyć z wykorzystaniem niszczarki.
12. Wszystkie wydruki, skanowane lub kopiowane dokumenty powinny być niezwłocznie usuwane z urządzeń, w celu uniemożliwienia zapoznania się z nimi osobom postronnym.
13. Jeżeli praca odbywa się w trybie hybrydowym, tzn. częściowo w biurze, częściowo w domu, należy korzystać tylko z zatwierdzonych przez pracodawcę metod udostępniania plików oraz dokumentów, określonych w niniejszym Regulaminie.
14. W przypadku chwilowego opuszczania stanowiska pracy, należy blokować komputer i zabezpieczać dokumenty papierowe.
15. W przypadku opuszczania chwilowego pomieszczenia pracy, należy zamknąć pomieszczenie i zabrać klucz ze sobą.
16. Po otwarciu pomieszczeń i szafek, należy klucze usuwać z zamków, tzn., aby nie pozostawały w zamkach, umożliwiając ich kradzież, skopiowanie lub zamknięcie pomieszczenia przez osobę nieuprawnioną.
17. Jeżeli pomieszczenie jest współdzielone z innymi pracownikami, należy postępować zgodnie z przyjętą w organizacji polityką kluczy.
18. Po zakończeniu pracy należy wyłączyć urządzenia elektroniczne, a także schować wszystkie elektroniczne i papierowe nośniki informacji do szafek zamykanych na klucz. Zbędne nośniki należy zniszczyć. Zasada obowiązuje wszystkich bez wyjątków, ze względu na możliwość wprowadzenia odkażania powierzchni biurowych pod nieobecność pracowników.

III. Warunki pracy zdalnej

§ 3

1. O możliwości podjęcia pracy zdalnej przez pracownika decyduje pracodawca.
2. Pracownik może zgłosić pracodawcy chęć podjęcia pracy zdalnej.
3. Warunki i zasady pracy zdalnej, w tym zakres i harmonogram wykonywanej pracy określa pracodawca, jednakże pracownik może także zaproponować własny harmonogram i zakres pracy, który będzie mógł realizować po uzyskaniu zgody pracodawcy.
4. W przypadku podjęcia pracy zdalnej pracownika obowiązują zasady pracy zdalnej określone w niniejszym Regulaminie.
5. Pracownik podejmując pracę zdalną zapewnia odpowiednie, zgodnie z niniejszym Regulaminem, warunki świadczenia tej pracy.
6. Jeżeli pracownik nie ma możliwości świadczenia pracy zdalnej z zapewnieniem właściwych zabezpieczeń, w szczególności ze względu na siłę wyższą (np. brak prądu lub Internetu), niezwłocznie zgłasza to pracodawcy i postępuje zgodnie z jego instrukcjami.
7. Złamanie zasad określonych w Regulaminie lub niedostosowanie się do postanowień niniejszego Regulaminu może stanowić naruszenie obowiązków pracowniczych. W przypadku osób realizujących zadania w oparciu o umowy cywilnoprawne postępowanie niezgodnie z niniejszym Regulaminem może oznaczać wykonanie zadania niezgodnie z przedmiotem umowy i z wymaganą przez pracodawcę starannością i zawodowym

profesjonalizmem i skutkować rozwiązaniem umowy, a także przewidzianymi w umowie karami umownymi.

IV. Warunki jakie musi spełniać miejsce świadczenia pracy zdalnej

§ 4

1. Pracownik musi zapewnić właściwe warunki umożliwiające mu skuteczną pracę zdalną z zachowaniem właściwego poziomu bezpieczeństwa informacji.
2. Niedozwolone jest podejmowanie pracy zdalnej w miejscach publicznych, jak kawiarnie, restauracje, galerie handlowe, gdzie osoby postronne mogłyby usłyszeć fragmenty służbowych rozmów lub zapoznać się z fragmentami wykonywanej pracy.
3. Pracując w domu należy zapewnić, aby domownicy nie mieli wglądu w wykonywaną pracę, w szczególności poprzez właściwe ustawienie ekranu komputera oraz smartfona, a także zapewnienie pracy z dokumentami w sposób uniemożliwiający wgląd.
4. Praca zdalna powinna odbywać się zgodnie z harmonogramem ustalonym z pracodawcą, co oznacza, że pracownik jest dostępny i realizuje swoje działania w ustalonych godzinach.
5. Odchodząc od komputera lub kończąc korzystanie z urządzeń IT należy upewnić się, że urządzenie zostało zablokowane.

V. Bezpieczeństwo pracy zdalnej i stacjonarnej

§ 5
Internet

1. Pracownik wykonuje pracę zdalną z wykorzystaniem urządzeń służbowych, tzn. otrzymanych od pracodawcy lub własnych.
2. Jeżeli pracodawca udostępnia pracownikowi modem internetowy lub telefon służbowy z dostępem do Internetu, który może pełnić funkcję HotSpot, pracownik powinien korzystać w pierwszej kolejności z tych urządzeń.
3. W przypadku korzystania z domowej sieci WiFi, należy upewnić się, że została ona skonfigurowana w sposób minimalizujący ryzyko włamania, w szczególności:
   1) korzystanie z internetu powinno wymagać uwierzytelnienia, np. poprzez hasło;
   2) hasło dostępu powinno składać się z co najmniej 8 znaków, w tym z dużych i małych liter oraz cyfr i znaków specjalnych;
   3) jeśli to możliwe, należy zmienić login do panelu administracyjnego routera na własny;
   4) dostęp do panelu administracyjnego routera jest możliwy wyłącznie z urządzeń znajdujących się w sieci domowej.
4. Porad i wsparcia w zakresie konfiguracji sieci domowej, w tym jej zabezpieczenia na potrzeby pracy zdalnej udziela osoba upoważniona przez dyrektora szkoły.

§ 6
Urządzenia służące do pracy zdalnej

1. Zabronione jest udostępnianie urządzeń wykorzystywanych do realizowania pracy zdalnej innym osobom, np. domownikom.
2. Praca zdalna powinna być realizowana z wykorzystaniem służbowego sprzętu, jak komputera stacjonarnego, laptopa, smartfona, tableta, itp.
3. Zgoda na pracę zdalną obejmuje zgodę na korzystanie ze służbowego sprzętu poza siedzibą pracodawcy.
4. Pracownik jest uprawniony także do zabrania komputera stacjonarnego do miejsca wykonywania pracy zdalnej, na czas wykonywania tej pracy.
5. Jeżeli z jakiś względów pracownik nie może wykonywać pracy zdalnej z wykorzystaniem służbowego sprzętu, zgłasza to pracodawcy, który może wydać zgodę na pracę z wykorzystaniem prywatnych urządzeń.

6. Urządzenie służbowe jest wydawane pracownikowi na podstawie umowy użyczenia.
7. Po otrzymaniu zgody na pracę zdalną i uzgodnieniu z pracodawcą z jakich urządzeń będzie korzystał pracownik w celu jej zrealizowania, pracownik niezwłocznie zgłasza ten fakt do sekretariatu w celu przygotowania sprzętu i sporządzenia umowy użyczenia.
8. Sekretariat odnotowuje, które urządzania są wykorzystywane przez pracownika do pracy zdalnej, jeżeli to niezbędne, przeprowadza ich przegląd.
9. Przegląd urządzeń prywatnych jest obowiązkowy.
10. Minimalne wymagania w zakresie bezpieczeństwa:
    1) na urządzeniu jest legalne i aktualne oprogramowanie;
    2) zostały włączone automatyczne aktualizacje;
    3) została włączona zapora systemowa;
    4) został zainstalowany i działa w tle program antywirusowy;
    5) zalogowanie do systemu operacyjnego wymaga uwierzytelnienia, np. poprzez indywidualny login i hasło użytkownika, kod PIN, token;
    6) wyłączono autouzupełnianie i zapamiętywanie hasła w przeglądarce internetowej;
    7) został zainstalowany program umożliwiający zaszyfrowanie i odszyfrowanie danych (np. 7- zip);
    8) zostało ustawione automatyczne blokowanie urządzenia po dłuższym braku aktywności;
    9) jeżeli urządzenie daje taką możliwość, praca jest wykonywana na koncie z ograniczonymi uprawnieniami.
11. Pracodawca może dodatkowo wymagać, aby urządzenie wykorzystywane do pracy zdalnej zawierało inne zabezpieczenia, jak:
    1) zaszyfrowany dysk;
    2) wyłączone porty pamięci zewnętrznych;
    3) oprogramowanie służące monitorowaniu wykonywania pracy przez pracownika, wykorzystywane zgodnie z wymaganiami przepisów prawa pracy.

§ 7
Zabezpieczanie przekazywanych informacji

1. Do pracy zdalnej pracownik powinien wykorzystywać tylko i wyłącznie służbowe programy i systemy udostępnione mu przez pracodawcę.
2. Jeżeli jest niezbędne przesłanie informacji o charakterze poufnym, w szczególności danych osobowych, powinny zostać one zabezpieczone hasłem.
3. Jeżeli informacje poufne będą przekazywane z wykorzystaniem poczty e-mail, powinny zostać udostępnione w załączniku zabezpieczonym hasłem.
4. Zabezpieczeniu powinny podlegać wszelkiego rodzaju dane osobowe, niezależnie od ich charakteru, nawet jeżeli są to jedynie imiona, nazwiska czy adresy e-mail.
5. Hasło powinno zostać przekazane odbiorcy inną drogą komunikacji.
6. Hasło powinno być odpowiednio skomplikowane i niesłownikowe.
7. Dozwolone jest ustalenie stałego hasła na komunikację z jednym odbiorcą.
8. Rekomendowane metody zabezpieczania hasłem:
    1) nadanie hasła do pliku, w którym są dane osobowe;
    2) zabezpieczenie pliku lub plików poprzez kompresję z zabezpieczeniem archiwum wynikowego hasłem.
9. Każda wiadomość powinna być wysyłana z należytą starannością, polegającą w szczególności na sprawdzeniu, czy jest kierowana do odpowiedniego odbiorcy.
10. W przypadku wysyłania informacji do kilku odbiorców, którzy nie znają się wzajemnie i/lub ich adresy e-mail są adresami prywatnymi, należy skorzystać z opcji Ukrytej kopii (UDW/BCC), tzn. adresy wpisać w to pole.
11. Szczegółowe zasady korzystania z poczty e-mail określa odrębny regulamin.
12. Masowe wysyłki wiadomości e-mail należy realizować poprzez specjalne oprogramowanie udostępnione w tym celu przez pracodawcę.

13. Pracownik może także przekazywać pliki z informacjami chronionymi z wykorzystaniem udostępnionych przez pracodawcę serwerów sieciowych lub plików FTP.
14. Wykorzystywanie innych narzędzi do przesyłania i udostępniania plików (We Transfer, Googe Drive, DropBoX) może odbywać się tylko za zgodą pracodawcy, po wcześniejszym zabezpieczeniu hasłem plików.

§ 8
Zasady korzystania z dokumentów w formie papierowej

1. Zgodnie z obowiązującym u pracodawcy zasadami wszystkie dokumenty zawierające informacje poufne, w tym dane osobowe, powinny być przechowywane w szafach zamykanych na klucz w siedzibie pracodawcy.
2. Obowiązuje ogólny zakaz zabierania dokumentów lub ich kopii poza siedzibę pracodawcy.
3. Jeżeli do pracy zdalnej niezbędny jest dostęp do dokumentów papierowych, pracownik zgłasza do pracodawcy prośbę o możliwość ich skopiowania oraz zabrania do domu na czas wykonywania pracy zdalnej.
4. Po otrzymaniu zgody na piśmie lub w formie służbowej wiadomości e-mail, pracownik może sporządzić kopie niezbędnych dokumentów.
5. Zabronione jest zabieranie poza siedzibę pracodawcy oryginałów dokumentów.
6. Po skopiowaniu dokumentów pracownik przygotowuje ich zestawienie, zawierające informacje jakie dokumenty, w jakiej liczbie zostały skopiowane.
7. Informacja jest przekazywana pracodawcy.
8. W czasie przewożenia dokumentów do miejsca realizowania pracy zdalnej, należy zachować szczególną ostrożność, aby ich nie zgubić.
9. Praca z dokumentami nie może być wykonywana w miejscu publicznym (świetlica w szkole, kawiarnia, restauracja, galeria handlowa, itp.).
10. Po zakończeniu pracy, wszystkie dokumenty należy zwrócić pracodawcy, który weryfikuje ich kompletność.

VI. Szczególne sytuacje

§ 9

W przypadku zgubienia lub kradzieży sprzętu, dokumentów lub innych nośników informacji, należy niezwłocznie, w dniu zdarzenia zgłosić zdarzenie do pracodawcy a także inspektora ochrony danych osobowych.

§ 10

Należy niezwłocznie zgłaszać pracodawcy wszelkie podejrzenia naruszeń dla ochrony danych, jak pozostawione bez nadzoru wydruki, niezniszczone dokumenty, pozostawienie kluczy w drzwiach, pozostawienie niezabezpieczonego stanowiska pracy, utrata danych, udostępnienie danych osobie nieuprawnionej, itd. Należy zgłaszać każdą sytuację, która w opinii pracownika odbiega od przyjętej normy i obowiązujących standardów bezpieczeństwa. Do pracodawcy należy ocena ryzyka zdarzenia.

§ 11

Zmiana trybu i sposobu pracy nie zwalania z obowiązku zapewnienia ochrony danych osobowych i nie może wpływać na zmniejszenie lub ograniczenie wcześniej obowiązujących zabezpieczeń.

§ 12

Wszelkiego rodzaju problemy związane z możliwością zapewnienia ochrony danych, należy niezwłocznie zgłaszać, zgodnie z obowiązującą procedurą postępowania przy naruszeniach.

VII. Działania niedozwolone

§ 13

1. Niedozwolone jest:
   1) udostępnianie innym osobom danych służących do uwierzytelnienia do systemów i/lub usług;
   2) przekazywanie informacji chronionych, w szczególności danych osobowych bez zabezpieczenia hasłem, w szczególności w treści wiadomości e-mail;
   3) przekazywanie hasła do zabezpieczonych informacji tą samą drogą komunikacji, którą przekazywany jest zabezpieczony hasłem plik lub pliki;
   4) korzystanie z urządzeń, które nie zostały zatwierdzone przez pracodawcę;
   5) odmówienie przeglądu urządzenia;
   6) niszczenie dokumentów w domu;
   7) udostępnianie służbowego sprzętu lub sprzętu wykorzystywanego do realizowania zadań służbowych innym osobom;
   8) dzielenie się informacjami poufnymi z innymi osobami, w szczególności domownikami;
   9) logowanie się na konto innego użytkownika;
   10) zabranie dokumentów bez pisemnej lub elektronicznej zgody pracodawcy;
   11) zabranie oryginałów dokumentów;
   12) niezwrócenie dokumentów;
   13) niepotwierdzenie z pracodawcą zakresu zwróconych danych,
   14) korzystanie z komunikatorów internetowych nie zatwierdzonych przez pracodawcę/nie posiadających odpowiedniego certyfikatu bezpieczeństwa.

……..……..

3. Procedura bezpiecznego przetwarzania danych osobowych

Procedura bezpiecznego przetwarzania danych osobowych podczas pracy zdalnej w okresie epidemii COVID-19 w Szkole Podstawowej im. ks. Jana Twardowskiego w Powidzku

Celem niniejszej procedury jest zminimalizowanie wysokiego ryzyka naruszenia praw i wolności osób, których dane osobowe są przetwarzane w okresie czasowego ograniczenia funkcjonowania jednostek systemu oświaty w związku z zapobieganiem, przeciwdziałaniem i zwalczaniem COVID-19. Procedura ta została opracowana na podstawie przeprowadzonej wcześniej analizy ryzyka i oceny zagrożeń w świetle przepisów 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 zwane w skrócie „RODO".

§ 1
Postanowienia ogólne

1. Przetwarzanie danych osobowych w ramach pracy zdalnej następuje na podstawie pisemnego polecenia pracy zdalnej wydanego przez pracodawcę.
2. Pracownik, któremu wydano polecenie pracy zdalnej zobowiązany jest w jej trakcie do przetwarzania danych osobowych zgodnie z przepisami powszechnie obowiązującego prawa, w szczególności z przepisami o ochronie danych osobowych oraz innymi przepisami regulujących pracę jednostki systemu oświaty, zwłaszcza z polityką bezpieczeństwa przetwarzania danych osobowych i instrukcją zarządzania systemami informatycznymi.
3. Pracownik zobowiązuje się do przetwarzania udostępnionych mu danych osobowych jedynie w celach służbowych, określonych w umowie o pracę.
4. Zabronione jest wykorzystywanie przez pracownika udostępnionych mu danych osobowych w celach niezwiązanych z wykonywaniem zadań i obowiązków służbowych.

§ 2
Bezpieczeństwo obszaru przetwarzania

1. Pracownik zobowiązuje się zorganizować stanowisko do pracy zdalnej w sposób zapewniający bezpieczne i higieniczne warunki pracy.
2. Pracownik jest odpowiedzialny za właściwe zabezpieczenie danych osobowych przetwarzanych przez niego w ramach pracy zdalnej.
3. Pracownik zobowiązany jest do zachowania poufności informacji, na przykład podczas służbowych rozmów telefonicznych lub wideokonferencji.
4. Pracownik zobowiązany jest do zabezpieczania dostępu do posiadanych danych służbowych przed osobami postronnymi, w tym wspólnie z nim zamieszkującymi oraz przed ich nieuprawnionym zniszczeniem lub modyfikacją.
5. Pracownik zobowiązany jest do uniemożliwienia wglądu osobom postronnym w treści wyświetlane na ekranie sprzętu komputerowego, na przykład poprzez odpowiednie ustawienie ekranu.
6. Pracownik zobowiązany jest do stosowania polityki czystego ekranu, tj. blokowania sprzętu komputerowego w razie oddalenia się od miejsca pracy.
7. Po zakończeniu pracy na sprzęcie elektronicznym należy każdorazowo wylogować się z programów wykorzystywanych do pracy zdalnej oraz z systemu.
8. Pracownik zobowiązuje się do bezpiecznego przechowywania danych osobowych zawartych w dokumentacji w formie papierowej, na przykład w meblach zamykanych na klucz.

§ 3
Bezpieczeństwo domowej sieci

1. Sprzęt komputerowy powinien być podłączony do zabezpieczonej, domowej sieci WiFi. Zabronione jest korzystanie z otwartych sieci WiFi, na przykład WiFi hotelowe, w galeriach handlowych czy hot-spoty w kawiarniach.
2. Dostęp do panelu konfiguracyjnego urządzenia sieciowego oraz dostęp do sieci bezprzewodowej (sieci WiFi) powinien być zabezpieczony silnym hasłem, którym nie jest hasło domyślne, zdefiniowane podczas pierwszej konfiguracji urządzenia.
3. Oprogramowanie urządzenia sieciowego powinno być regularnie aktualizowane.
4. Możliwość konfiguracji sprzętu sieciowego z urządzeniami znajdującymi się poza siecią LAN powinna być wyłączona lub ograniczona tylko do zdefiniowanych adresów IP.
5. Zaleca się zdefiniowanie urządzeń, które mogą uzyskać dostęp do domowej sieci WiFi, na przykład z wykorzystaniem filtracji adresów MAC.

§ 4
Procedura bezpiecznego logowania

1. Dostęp do sprzętu lub programu wykorzystywanego do pracy zdalnej powinien być możliwy wyłącznie z wykorzystaniem indywidualnego identyfikatora oraz hasła, na przykład poprzez ustawianie PIN-u lub innej formy uwierzytelnienia.
2. Hasło do sprzętu lub programu wykorzystywanego do pracy zdalnej powinno być odpowiednio długie i złożone. Nie powinno być ono zbudowane za pomocą ciągu znajdujących się obok siebie znaków na klawiaturze lub oparte na prostych skojarzeniach związanych z użytkownikiem, na przykład numer telefonu, data urodzenia, imiona lub nazwiska.
3. Hasło do sprzętu lub programu wykorzystywanego do pracy zdalnej powinno być zmieniane w cyklach 30-dniowych.
4. Zabronione jest udostępnianie osobom trzecim haseł oraz przechowywanie ich w miejscach niegwarantujących ich poufności.
5. Zabronione jest domyślne zapamiętywanie hasła dostępu do konta użytkownika systemu na sprzęcie oraz programów wykorzystywanych w pracy zdalnej, w szczególności dziennika elektronicznego i platform wykorzystywanych w kształceniu na odległość.

§ 5
Bezpieczne korzystanie z programów i platform wykorzystywanych w pracy zdalnej (w tym wideokonferencji)

1. Użycie w pracy zdalnej danego programu/platformy wymaga zgody pracodawcy.
2. W przypadku udostępniania danych osobowych w programach/platformach wykorzystywanych w pracy zdalnej Administrator danych zobowiązany jest do zawarcia umowy powierzenia przetwarzania danych osobowych. Umowa ta ma zapewniać wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, tak aby przetwarzanie spełniało wymogi wskazane w RODO i chroniło prawa osób, których dane dotyczą.
3. Programy/platformy w przypadku, których nie ma możliwości zawarcia umowy powierzenia przetwarzania danych osobowych nie mogą być wykorzystywane do przetwarzania danych osobowych.
4. W pracy zdalnej zalecane jest korzystanie z aplikacji webowych, nie desktopowych.
5. Przed rozpoczęciem korzystania z programu/platformy wykorzystywanej do pracy zdalnej pracownik zobowiązany jest do zapoznania się z ogólnymi warunkami jej użytkowania oraz polityką prywatności.
6. W przypadku korzystania z programów z funkcją wideokonferencji zaleca się wyłączenie opcji nagrywania i przechowywania.
7. Przy podłączaniu się do programu z funkcją telekonferencji zalecane jest korzystanie z kodów dostępu/PIN-ów.

8. Przed rozpoczęciem korzystania z programów z funkcją telekonferencji zalecane jest przeskanowanie ich systemem antywirusowym.
9. W trakcie korzystania z programów lub platform do pracy zdalnej należy ograniczyć ilość podawanych danych osobowych (zasada minimalizacji danych).
10. W przypadku, kiedy pracownikowi został przydzielony służbowy adres e-mail zabronione jest korzystanie przez niego z prywatnego adresu e-mail do celów służbowych.
11. Zabrania się udostępniania dokumentów służbowych/przetwarzania danych osobowych, za pomocą publicznego czatu lub innych komunikatorów.
12. Zabrania się udostępniania w mediach społecznościowych linków do konferencji, prowadzonych zajęć i innych aktywności realizowanych w ramach pracy zdalnej.
13. Zaleca się udostępnianie linków do konferencji, prowadzonych zajęć i innych aktywności realizowanych w ramach pracy zdalnej, na przykład poprzez wskazany przez dziennik elektroniczny.
14. Należy korzystać z opcji „poczekalnia" tak, aby kontrolować uczestników telekonferencji, w celu uniknięcia przypadkowych lub niechcianych osób.

§ 6
Bezpieczne przechowywanie danych

1. Nośniki urządzeń mobilnych wykorzystywane w celach służbowych, w tym komputer, telefon lub tablet powinny być zaszyfrowane, na przykład za pomocą hasła.
2. Zewnętrzne karty pamięci, a także inne nośniki danych, takie jak pendrive lub dysk zewnętrzny, wykorzystywane w celach służbowych powinny być szyfrowane za pomocą hasła.
3. Zabronione jest umieszczanie danych osobowych w publicznych chmurach obliczeniowych, komunikatorach lub innych usługach dostępnych w sieci. W przypadku nauczycieli mogą oni jedynie publikować tam materiały edukacyjne, natomiast nie mogą przetwarzać danych osobowych uczniów i ich rodziców.

§ 7
Ochrona przed cyberatakami

1. Sprzęt wykorzystywany do pracy zdalnej musi być wyposażony w uruchomione i zaktualizowane oprogramowanie antywirusowe.
2. Systemy, w tym system operacyjny wykorzystywany do pracy zdalnej musi być regularnie aktualizowany.
3. Komputer wykorzystywany do pracy zdalnej musi mieć uruchomioną zaporę sieciową.

§ 8
Procedury bezpieczeństwa podczas pracy zdalnej

1. Zabrania się samodzielnej lub z wykorzystaniem wsparcia podmiotów zewnętrznych naprawy sprzętu wykorzystywanego do pracy zdalnej. W celu naprawy uszkodzonego sprzętu należy bezzwłocznie zwrócić go pracodawcy.
2. Zabrania się drukowania dokumentów służbowych w punktach ksero lub z pomocą innych podmiotów czy osób trzecich.
3. Komunikacja z uczniami, rodzicami i innymi klientami jednostki systemu oświaty powinna być prowadzona przede wszystkim za pośrednictwem wdrożonych rozwiązań teleinformatycznych, na przykład poprzez dziennik elektroniczny.
4. Pracownik zobowiązany jest do weryfikowania nadawców wiadomości e-mailowych oraz w przypadku wątpliwości do nieotwierania załączników oraz hiperłączy znajdujących się w tekście.
5. Podczas wysyłania korespondencji zbiorczej należy korzystać z opcji „kopia ukryta" (pole UDW – Ukryci Do Wiadomości lub BCC – Blind Carbon Copy), dzięki której odbiorcy wiadomości nie zobaczą wzajemnie swoich adresów e-mail.

6. Pracownik zobowiązany jest do szyfrowania wiadomości e-mailowych zawierających dane osobowe i przekazywania hasła zawsze inną formą, na przykład telefonicznie.
7. Zabronione jest przesyłanie służbowych wiadomości e-mail na prywatne konta e-mailowe.
8. Zabrania się włączać opcję autouzupełniania formularzy w opcjach przeglądarki internetowej.
9. W przypadku korzystania z szyfrowanego połączenia przez przeglądarkę, należy zwracać uwagę na pojawienie się odpowiedniej ikonki „kłódka". W tej sytuacji należy „kliknąć" na ikonę kłódki i sprawdzić, czy właścicielem certyfikatu jest wiarygodny właściciel.

§ 9

Dodatkowe zalecenia do pracy zdalnej na prywatnym sprzęcie komputerowym

1. Zalecane jest stworzenie oddzielnego konta użytkownika systemu w pracy na prywatnym sprzęcie, wykorzystywanym do pracy zdalnej. Konto użytkownika powinno posiadać ograniczone uprawnienia i być chronione silnym hasłem oraz nie udostępniane osobom trzecim.
2. Za legalność oprogramowania, w tym programu antywirusowego odpowiada właściciel sprzętu.
3. Po zakończeniu okresu pracy poza miejscem jej stałego wykonywania pracownik jest zobowiązany bezzwłocznie przekazać pracodawcy wszystkie dane zapisane na prywatnym sprzęcie (dokumenty służbowe tworzone i przechowywane w pamięci komputera, pliki oraz inne posiadane informacje) związane z wykonywanymi zadaniami służbowymi, a następnie usunąć je w sposób trwały.

§ 10

Bezpieczne przetwarzanie danych osobowych zawartych w dokumentacji papierowej podczas pracy zdalnej

1. Dokumentacja papierowa zawierająca dane osobowe udostępniana jest pracownikowi w zakresie niezbędnym do realizacji obowiązków służbowych w zakresie pracy zdalnej, za zgodą pracodawcy.
2. Pracodawca zapewnia ewidencjonowanie wydanych pracownikom dokumentów zawierających dane osobowe.
3. Pracownik zobowiązany jest przechowywać udostępnione dokumenty papierowe przez okres niezbędny do wykonania określonego zadania podczas pracy zdalnej (zasada ograniczenia przetwarzania). Po tym czasie zobowiązany jest niezwłocznie zwrócić je pracodawcy.
4. Podczas przenoszenia dokumentów pracownik zobowiązany jest do odpowiedniego ich zabezpieczenia i przenoszenia dokumentów w taki sposób, aby były niewidoczne dla osób trzecich, na przykład w zabezpieczonej teczce.
5. Pracownik zobowiązany jest do bezpiecznego niszczenia dokumentów papierowych, na przykład za pomocą niszczarki do dokumentów. Jeżeli pracownik nie posiada niszczarki dokumentów, powinien dokumenty zabezpieczyć, a po zakończeniu pracy zdalnej niezwłocznie zniszczyć je w siedzibie pracodawcy.
6. Zabrania się pracownikowi wyrzucania papierowych dokumentów służbowych do domowego kosza na śmieci.

§ 11

Naruszenie ochrony danych osobowych podczas pracy zdalnej

1. Pracownik, który stwierdzi lub podejrzewa naruszenie ochrony danych osobowych w systemie informatycznym lub w systemie tradycyjnym, zobowiązany jest do niezwłocznego pisemnego poinformowania o tym administratora danych.
2. W przypadku powzięcia informacji o naruszeniu ochrony danych osobowych Administrator danych prowadzi postępowanie wyjaśniające w toku, którego:

1) ustala zakres i przyczyny naruszenia ochrony danych osobowych oraz jego ewentualne skutki;
2) informuje i konsultuje tok postępowania z Inspektorem Ochrony Danych;
3) podejmuje działania prewencyjne zmierzające do eliminacji podobnych incydentów w przyszłości lub zmniejszenia strat w momencie ich zaistnienia.

3. W przypadku naruszenia ochrony danych osobowych skutkującego ryzykiem naruszenia praw lub wolności osób fizycznych, administrator bez zbędnej zwłoki – w miarę możliwości, nie później niż w terminie 72 godzin po stwierdzeniu naruszenia – zgłasza je organowi nadzorczemu – Urząd Ochrony Danych Osobowych oraz w pewnych przypadkach powiadamia osoby, których dane dotyczą.
4. Jeżeli przyczyną naruszenia zasad ochrony danych osobowych było zaniedbanie ze strony pracownika, administrator może wyciągnąć konsekwencje dyscyplinarne wynikające z regulaminu pracy.
5. Zabrania się świadomego lub nieumyślnego wywoływania naruszeń przez osoby upoważnione do przetwarzania danych.

.....

4. Klauzula informacyjna RODO w związku ze zdalnym nauczaniem

Klauzula informacyjna RODO w związku ze zdalnym nauczaniem

W związku z przetwarzaniem danych osobowych wynikającego z realizacji zdalnego nauczania Dyrektor Szkoły Podstawowej, działając w imieniu Administratora danych informuje, że:

1. Administratorem Państwa danych osobowy oraz danych dziecka jest Szkoła Podstawowa im. ks. Jana Twardowskiego w Powidzku z siedzibą w Powidzko 49, 55-140 Żmigród, tel. 71 385 6693, e-mail sppowidzko_49@op.pl
2. W szkole powołany jest Inspektor ochrony danych osobowych. Kontakt z inspektorem jest możliwy pod adresem e-mail: sppowidzko_49@op.pl lub listownie na adres pocztowy placówki.
3. Dane osobowe przetwarzane są w celu realizacji zadania w interesie publicznym, którym jest organizacja i prowadzenie nauczania zdalnego na podstawie art. 6 ust. 1 lit. c oraz Rozporządzenie Ministra Edukacji Narodowej z dnia 11 marca 2020 r. w sprawie czasowego ograniczenia funkcjonowania jednostek systemu oświaty w związku z zapobieganiem, przeciwdziałaniem i zwalczaniem COVID-19 (Dz. U. poz. 1389 ze zm.). Przepisy prawa nie określają jakie dane mają być przetwarzane w związku z realizacją tego zadania, dlatego minimalny zakres danych do realizacji tego celu przetwarzania określa Administrator i pozostaje on w zgodzie z danymi osobowymi, które szkoła przetwarza w stacjonarnym procesie kształcenia.
4. Administrator przewiduje przetwarzanie wizerunków uczniów. Wizerunek ucznia będzie przetwarzany jedynie w związku z uczestnictwem w wideo konferencjach, w tym na lekcjach prowadzonych z użyciem platformy MS Teams.
5. Zdalne nauczanie jest realizowane poprzez:
   - dziennik elektroniczny dostarczany przez: Librus Spółka z ograniczoną odpowiedzialnością sp. k. ul. Korfantego 193, 40-153 Katowice,
   - platformę e-podręczniki – platformę edukacyjną Ministerstwa Edukacji Narodowej,
   - platformę MS Teams,
   - platformę WSiPnet
   - dostawcę usług e-mail: Google, wp, onet, interia
6. Administratorem danych przetwarzanych w narzędziach, systemach, aplikacjach służących do kształcenia na odległość jest dostawca danego rozwiązania. Należy dokładnie zapoznać się z regulaminami i Politykami prywatności dostawców usług i rozwiązań służących do zdalnego nauczania, z których korzystają uczniowie i nauczyciele.
7. Dane osobowe dzieci, rodziców i opiekunów prawnych będą przetwarzane przez okres przetwarzania (okres trwania obowiązku nauki zdalnej). Następnie niezbędna dokumentacja jest dołączana do dokumentacji ucznia, przechowywane zgodnie z zapisami jrwa dla dokumentacji pedagogicznej.
8. Posiada Pan/Pani prawo do: żądania od administratora dostępu do danych osobowych, prawo do ich sprostowania, usunięcia, na zasadach określonych w art. 15-17 RODO lub ograniczenia przetwarzania, w przypadkach określonych w art. 18.
9. Przysługuje Państwu prawo wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych (ul. Stawki 2, 00-193 Warszawa).
10. Dane osobowe kandydatów do pracy nie są przekazywane osobom trzecim.
11. Dane osobowe przetwarzane w procesie zdalnej nauki nie są przetwarzane z sposób zautomatyzowany i nie podlegają profilowaniu.
12. Dane osobowe nie są profilowane ani przetwarzane automatycznie
13. Podanie danych osobowych jest wymogiem ustawowym i jest obowiązkowe ze względu na realizacje ustawowego obowiązku nauk/obowiązku szkolnego.
14. Nie przewidujemy transferu danych do Państw trzecich. Jednocześnie informujemy, że nie przekazujemy danych poza teren Europejskiego Obszaru Gospodarczego. Jednak zastrzegamy, że przepływy danych serwisu Facebook, Google, MS Teams mają charakter ponadnarodowy. Serwis ten może przekazywać Państwa dane poza teren Europejskiego

Obszaru Gospodarczego. Jednocześnie wskazujemy, iż Facebook, Google, MS Teams posiada certyfikat EU-US-PrivacyShield dołączony do umowy pomiędzy USA a Komisją Europejską. Komisja Europejska stwierdziła odpowiedni poziom ochrony danych w przypadku przedsiębiorstw posiadających certyfikat PrivacyShield.

5. Rejestr czynności przetwarzania w nauczaniu zdalnym

Na administratorze danych zgodnie z wymaganiami RODO ciąży szereg obowiązków zapewnienia właściwego przetwarzania danych osobowych przy pracy zdalnej. Powinien wprowadzić odpowiednie zasady ochrony danych osobowych przy wykonywaniu pracy zdalnej w miejscu zamieszkania pracownika, w tym określić zabezpieczenia na podstawie wcześniej dokonanej analizy ryzyka.

Brak realizacji powyższych działań może skutkować **odpowiedzialnością karną lub finansową** pracodawców realizujących przetwarzanie danych osobowych w trybie pracy zdalnej, określoną w przepisach o ochronie danych.

Dobrze prowadzony rejestr czynności przetwarzania pozwala:

1) zorientować się i panować nad tym, jakie dane i dlaczego przetwarzane są w organizacji, niezależnie od tego kto jest ich administratorem;
2) skupić w jednym dokumencie przegląd wszystkich czynności na danych osobowych;
3) łatwo przypisać osoby odpowiedzialne za poszczególne obszary (tzw. właścicieli procesów);
4) łatwo zgromadzić dane do przygotowania klauzul informacyjnych i zapewnić ich jednolitość;
5) o wiele sprawniej i dokładniej przeprowadzić analizę ryzyka oraz ocenę skutków dla ochrony danych (DPIA).

Rejestr czynności przetwarzania danych osobowych w zbiorze „Uczniowie" – nauczanie zdalne		Nr karty **34**
art. 30 ust. 1 lit. a	imię i nazwisko/nazwa oraz dane kontaktowe administratora	Szkoła Podstawowa im. ks. Jana Twardowskiego w Powidzku, Powidzko 49, 55-140 Żmigród tel. 71 385 6693 e-mail: ela_rychlicka@interia.pl
	imię i nazwisko Inspektora Ochrony Danych, kontakt	Magdalena Pęczk, tel. 71 385 6693 e-mail: sppowidzko_349@op.pl
art. 30 ust. 1 lit. b	cele przetwarzania	realizacja obowiązku obowiązku szkolnego w sytuacji ograniczenia funkcjonowania jednostek systemu oświaty w formie stacjonarnej
art. 30 ust. 1 lit. c	kategoria osób	uczniowie szkoły, nauczyciele
	opis kategorii danych osobowych	dane zwykłe: imię i nazwisko, adres poczty elektronicznej dane szczególnej kategorii przetwarzania: wizerunek, głos
art. 30 ust. 1 lit. d	kategorie odbiorców, którym dane osobowe zostały lub zostaną ujawnione	Administratorzy: a) dziennik elektroniczny dostarczany przez: nazwa dostawcy (Librus Spółka z ograniczoną odpowiedzialnością sp. k. ul. Korfantego 193, 40-153 Katowice), b) platforma e-podręczniki – platforma edukacyjna Ministerstwa Edukacji Narodowej, c) platforma WSiPnet,
	kategorie odbiorców w państwach trzecich lub w organizacjach międzynarodowych	Administratorzy: d) platforma MS Teams e) dostawcę usług e-mail: Google, wp, onet, interia

art. 30 ust. 1 lit. f	planowane terminy usunięcia poszczególnych kategorii danych	Po zakończeniu nauki w wariancie B lub C
art. 30 ust. 1 lit. d	ogólny opis technicznych i organizacyjnych środków bezpieczeństwa, o których mowa w art. 32 ust. 1.	1. Serwery jak i stacje robocze są zabezpieczane oprogramowaniem antywirusowym oraz zaporą typu firewall. 2. Przenośne nośniki danych oraz inne urządzenia po konserwacji lub naprawie poza siedzibą jednostki, przed rozpoczęciem pracy w systemie informatycznym jednostki są sprawdzane za pomocą aktualnego oprogramowania antywirusowego. 3. Możliwość instalacji i dezinstalacji mają użytkownicy wyłącznie z uprawnieniami administratora. 4. W jednostce sporządzane są kopie zapasowe wg. harmonogramu zatwierdzonego przez administratora. Częstotliwość sporządzania kopii zapasowych zapewnia możliwości ciągłości działania w razie wystąpienia utraty danych w systemie informatycznym. 5. Miejsce przechowywania kopii zapasowych jest zabezpieczone przed dostępem osób nieuprawnionych, zaś nośniki, na których zostały wykonane kopie, zabezpieczone są przez działaniem szkodliwych czynników (np. zalanie, pożar, działanie silnego pola elektromagnetycznego). 6. Sieć wewnętrzna administratora zabezpieczona jest w sposób uniemożliwiający włącznie urządzeń innych niż te autoryzowane przez administratora. 7. Sieć wewnętrzna na styku z siecią publiczną Internet jest zabezpieczona aplikacją/urządzeniem typu firewall. 8. Usługi sieciowe, które nie są wykorzystywane lub uznane za niebezpieczne są zablokowane lub wyłączane. 9. Systemy operacyjne i wykorzystywane aplikacje są aktualizowane do najnowszych, bezpiecznych i stabilnych wersji. 10. Urządzenia sieciowe chronione są hasłem. 11. Dostęp do systemu informatycznego jednostki mają wyłącznie osoby uprawnione przez administratora. 12. Dostęp do systemu odbywa za pomocą unikalnego loginu nadawanego wyłącznie jednemu użytkownikowi. 13. System operacyjny, po okresie bezczynności o czasie jej trwania nie dłuższym niż 5 minut przechodzi w stan nieaktywny blokując dostęp do urządzenia. Powrót do stanu aktywności wymaga podania hasła. 14. W jednostce wprowadzono blokadę portów USB. 15. Naprawy oraz konserwacje sprzętu służącego do przetwarzania danych osobowych obywają się wyłącznie na podstawie zawartych umów, w których precyzyjnie określono zadania, odpowiedzialności oraz zawarto zobowiązanie podmiotu realizującego usługę do zachowania poufności. 16. Umowy zawarte na naprawę, konserwację sprzętu, dostęp do sieci Internet zawierają określenie maksymalnego czasu na naprawę sprzętu oraz przywrócenie dostępu do sieci, które pozwoli jednostce dostępność do danych bez uszczerbku dla podmiotów danych. 17. Przenośne nośniki danych są ewidencjonowane przez administratora i mogą być wynoszone poza teren

		jednostki wyłącznie po otrzymaniu na to zgody od administratora oraz wyłącznie w formie zaszyfrowanej. 18. Instalacja okablowania poprowadzona jest w sposób uniemożliwiający dostęp osobom nieuprawnionym oraz uniemożliwiającym uszkodzenie okablowania. 19. W jednostce prowadzona jest kompletne i aktualna dokumentacja połączeń fizycznych i logicznych w celu zmniejszenia prawdopodobieństwa błędu. 20. W jednostce wdrożono system poczty elektronicznej, który zapewnia ochronę przed szkodliwym oprogramowanie rozpowszechnianym za pomocą poczty elektronicznej, ochronę antywirusową, ochronę antyspamową, możliwość użycia dostępnych technik kryptograficznych do ochrony poufności i integralności wiadomości poczty elektronicznej. 21. Dane osobowe są przetwarzane wyłącznie przez osoby upoważnione przez administratora. 22. Pracownicy przetwarzający dane sensytywne w kadrach oraz w zakresie gospodarowania zakładowym funduszem świadczeń socjalnych posiadają odrębne wydane przez administratora upoważnienia. 23. Osoby upoważnione do przetwarzania danych osobowych składają oświadczenie o zachowaniu poufności. 24. Przed dopuszczeniem do pełnienia obowiązków służbowych, pracownicy przechodzą obowiązkowe szkolenie z zakresu ochrony danych osobowych. 25. Pracownicy przetwarzający dane osobowe podlegają obowiązkowym, okresowym szkoleniom z zakresu ochrony danych osobowych. 26. W jednostce opracowano i wdrożono wewnętrzne procedury ochrony danych osobowych zawarte w Polityce bezpieczeństwa. 27. Dokumenty zawierające dane osobowe mogą być przechowywane wyłącznie w zamykanych na klucz szafach. 28. W jednostce wyznaczono inspektora ochrony danych, który prowadzi stałe konsultacje dla osób przetwarzających dane osobowe z upoważnienia administratora.

6. Analiza ryzyk dla bezpieczeństwa danych i praw osób przetwarzanych w procesie zdalnego przetwarzania w Szkole Podstawowej im. ks. Jana Twardowskiego w Powidzku

Objaśnienia:

1. Prawdopodobieństwo szacowane w skali 1 – 5, skutki szacowane w skali 1 – 5.
2. Reakcja na ryzyko: **T** – tolerowanie; **P** – przeniesienie; **D** - działanie; **W** – wycofanie
3. Istotność ryzyka:
   1) niska o wartości 4 i mniejszej;
   2) średnia o wartości powyżej 4 i mniejszej lub równej 9;
   3) wysoka o wartości powyżej 9 i mniejszej lub równej 16;
   4) katastrofalne – o wartości powyżej 16

Lp.	**Zagrożenie**	**Opis ryzyka**	**Zabezpieczenia**	**Prawdopodobieństwo** (w skali od 1-5)	**Skutek** (w skali od 1-5)	**Istotność ryzyka** (P x S)	**Reakcja na ryzyko**
1	**Zagrożenie ciągłości działania**	1. Awarie/uszkodzenia urządzeń w infrastrukturze szkoły wykorzystywanych w procesie zdalnego nauczania (obejmuje także awarie komputerów przenośnych należących do szkoły)	**1. Procedury:** 1) Regulamin ODO dla pracowników, w którym określono procedury bezpieczeństwa przy przetwarzaniu danych osobowych, w tym w procesie zdalnego nauczania: a) zasady korzystania z internetu, b) zasady korzystania z poczty elektronicznej, c) zasady użytkowania komputerów przenośnych, d) zasady wynoszenia nośników elektronicznych poza jednostkę, e) zasady zabezpieczania dokumentacji papierowej, f) procedura niszczenia danych na nośnikach elektronicznych,	3	2	6	T
		2. Ataki cybernetyczne na infrastrukturę szkoły.		2	3	6	T

		3. Awarie/uszkodzenia urządzeń prywatnych wykorzystywanych w procesie zdalnego nauczania należących do uczniów i nauczycieli.	g) Polityka naprawy sprzętu IT w serwisach zewnętrznych, h) Polityka dotycząca zasad gospodarki kluczami; i) Procedura zabezpieczenia systemów informatycznych. 2) Osoby zatrudnione przy przetwarzaniu danych są świadome odpowiedzialności prawnej i karnej- podpisanie oświadczenia o poufności; 3) Szkolenie pracowników, w tym w formie e-learningu; 4) Przeniesienie infrastruktury szkolnej do chmury obliczeniowej - wykorzystanie rozwiązań chmurowych od dostawców gwarantujących odpowiednie warunki techniczne i organizacyjne bezpiecznej pracy zdalnej i ochronę danych osobowych 5) Sporządzanie umów powierzenia z firmami zajmującymi się hostingiem serwera, naprawą komputerów, brakowaniem dokumentacji w składnicy akt. **1. Zabezpieczenia:** 1) Zabezpieczenie dostępu do pomieszczeń – drzwi zamykane na klucz; 2) Zabezpieczenie dokumentacji w pomieszczeniach – zamykane niemetalowe szafy; 3) Monitoring wizyjny w obrębie obiektu i otoczenia; 4) Zahasłowane wygaszacze ekranu aktywowane w przypadku nieaktywności użytkownika;	3	2	6	PD
		4. Awaria sieci uniemożliwiająca dostęp do infrastruktury szkolnej podczas pracy zdalnej lub znacznie spowalniające pracę zdalną.		3	3	9	T
		5. Brak kopii zapasowych lub nieaktualne kopie zapasowe, przechowywanie kopii zapasowych w tych samych pomieszczeniach co pozostała część infrastruktury szkolnej; problemy z przywróceniem funkcjonowania w przypadku awarii lub cyberataku		3	3	9	T
2	**Zagrożenie dla bezpieczeństwa danych**	6. Brak aktualizacji systemu operacyjnego dla urządzeń użytkowników	1. **Procedury:** 1) Regulamin ODO dla pracowników, w którym określono procedury bezpieczeństwa przy przetwarzaniu danych osobowych, w tym: zasady korzystania z internetu, zasady korzystania z poczty elektronicznej; 2) Wykluczenie ze zdalnego nauczania urządzeń z systemami operacyjnymi bez wsparcia producenta lub po zakończeniu wsparcia;	3	2	6	T
		7. Brak aktualizacji systemu operacyjnego w infrastrukturze serwerowej		2	3	**6**	T

		8. Brak lub nieaktualne oprogramowanie wspomagające zapewnienie bezpieczeństwa we wszystkich urządzeniach w procesie zdalnego nauczania (oprogramowanie antywirusowe, antymalware, antyspyware)	3) Osoby zatrudnione przy przetwarzaniu danych są świadome odpowiedzialności prawnej i karne j- podpisanie oświadczenia o poufności; 4) Szkolenie pracowników, w tym w formie e-learningu; 5) Stosowana jest Procedura audytu oraz uwzględniono kontrole przestrzegania zasad przetwarzania danych w planie kontroli wewnętrznej. **2. Zabezpieczenia:** 1) System antywirusowy i antyspamowy instalowany na każdej jednostce stosowanej w przetwarzaniu danych;	3	2	**6**	T
		9. Instalacja szkodliwego oprogramowania/działanie szkodliwego oprogramowania		3	3	**9**	T
		10. Ataki socjotechniczne: phishing, spearphishing, cybersquatting		2	2	**4**	T
		11. Niedostateczne bezpieczeństwo uwierzytelniania w systemie zdalnego nauczania, m.in. proste hasła, powtarzające się hasła, hasła zapisywane na kartkach lub zapamiętywane w aplikacjach webowych, brak możliwości stosowania wieloskładnikowego uwierzytelnienia (2FA/MFA)		4	2	**8**	PD
		12. Korzystanie z publicznych lub niezabezpieczonych połączeń internetowych dla użytkowników pracujących zdalnie		2	3	**6**	W

3	**Zagrożenie dla bezpieczeństwa danych i praw osób, których dane dotyczą**	13. Upublicznienie danych w przestrzeni publicznej, dostęp przez Internet, przesłanie lub wydawanie danych osobowych osobie nieupoważnionej	**1. Procedury:** 1) Regulamin ODO dla pracowników, w którym określono procedury bezpieczeństwa przy przetwarzaniu danych osobowych, w tym: zasady korzystania z internetu, zasady korzystania z poczty elektronicznej; **2. Zabezpieczenia** 1) Firewall sprzętowy i programowy; 2) Aktualizacje systemu operacyjnego.	4	3	**12**	T

7. Mapa istotności ryzyka

SKUTEK					
bardzo wysoki **5**					
poważny **4**					
średni **3**		**2; 7; 12**	**4; 5; 9**	**13**	
niski **2**		**10**	**1; 3; 6; 8**	**11**	
nieznaczny **1**					
	1 rzadkie	**2** małe	**3** możliwe	**4** prawdopodobne	**5** prawie pewne

PRAWDOPODOBIEŃSTWO