AUTORSKA SZKOŁA PODSTAWOWA SMILE.EDU
ul. Wagonowa 2b, 53-609 Wrocław
tel. 577 997 842 , e-mail: aspsmile.edu@gmail.com

# PROCEDURA CYBERBEZPIECZEŃSTWA
# w Autorskiej Szkole Podstawowej Smile.Edutel.

Autorska Szkoła Podstawowa SMILE.EDU 53-609, Wrocław, ul. Wagonowa 2b Dyrektor

**ZATWIERDZONO**
.....
**Dyrektor Autorskiej Szkoły Podstawowej Smile.Edu**
/pieczęć i podpis/
**Data wprowadzenia:** 18 maja 2026 roku

## § 1. Cel procedury

Niniejsza procedura określa zasady zapewnienia cyberbezpieczeństwa w Autorskiej Szkole Podstawowej Smile.Edu we Wrocławiu, w szczególności zasady ochrony systemów informatycznych, danych osobowych, sprzętu komputerowego, dziennika elektronicznego, poczty elektronicznej, dokumentacji cyfrowej oraz bezpieczeństwa uczniów korzystających z Internetu i narzędzi elektronicznych.

Procedura została opracowana w celu zapewnienia, aby szkoła nie ograniczała się wyłącznie do posiadania dokumentów, lecz faktycznie wdrażała, dokumentowała, kontrolowała i aktualizowała działania z zakresu cyberbezpieczeństwa. Jest to szczególnie ważne po zmianach w ustawie o krajowym systemie cyberbezpieczeństwa, ogłoszonych w Dz.U. 2026 poz. 252, które weszły w życie 3 kwietnia 2026 r.

Procedura obejmuje działania organizacyjne, techniczne i wychowawcze, ponieważ cyberbezpieczeństwo w szkole dotyczy nie tylko komputerów i systemów, ale również ochrony małoletnich, przeciwdziałania cyberprzemocy, ochrony wizerunku uczniów, bezpiecznej komunikacji z rodzicami oraz prawidłowego przetwarzania danych osobowych.

## § 2. Podstawa prawna

Procedurę opracowano na podstawie:

1. ustawy z dnia 14 grudnia 2016 r. – Prawo oświatowe, z późn. zm.;
2. ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa, tj. Dz.U. z 2026 r. poz. 20, z późn. zm.;
3. ustawy z dnia 23 stycznia 2026 r. o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw, Dz.U. z 2026 r. poz. 252;
4. rozporządzenia Rady Ministrów z dnia 21 maja 2024 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych, Dz.U. z 2024 r. poz. 773;
5. rozporządzenia Parlamentu Europejskiego i Rady UE 2016/679 z dnia 27 kwietnia 2016 r., czyli RODO;
6. ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych, z późn. zm.;
7. ustawy z dnia 13 maja 2016 r. o przeciwdziałaniu zagrożeniom przestępczością na tle seksualnym i ochronie małoletnich, z późn. zm.;
8. ustawy z dnia 6 czerwca 1997 r. – Kodeks karny, z późn. zm.;
9. ustawy z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną, z późn. zm.;
10. Statutu Autorskiej Szkoły Podstawowej Smile.Edu;
11. Polityki Ochrony Danych Osobowych obowiązującej w szkole;
12. Standardów Ochrony Małoletnich obowiązujących w Autorskiej Szkole Podstawowej Smile.Edu, które przewidują m.in. obowiązek ochrony dzieci przed zagrożeniami w Internecie, ochrony danych osobowych oraz reagowania na sytuacje krzywdzenia dziecka.

## § 3. Zakres procedury

Procedura obowiązuje wszystkich pracowników szkoły, w tym nauczycieli, pracowników administracji, specjalistów, osoby współpracujące ze szkołą na podstawie umów cywilnoprawnych, wolontariuszy, praktykantów, uczniów oraz inne osoby, które korzystają z infrastruktury informatycznej szkoły albo mają dostęp do danych przetwarzanych przez szkołę.

Procedura dotyczy w szczególności:

1. komputerów, laptopów, tabletów, telefonów służbowych, drukarek, skanerów, routerów, urządzeń sieciowych oraz innych urządzeń wykorzystywanych w pracy szkoły;
2. systemów informatycznych, w tym dziennika elektronicznego, poczty elektronicznej, systemów do przechowywania dokumentów, formularzy elektronicznych, platform edukacyjnych i narzędzi komunikacji z rodzicami;
3. danych osobowych uczniów, rodziców, pracowników oraz kandydatów do szkoły;
4. dokumentacji szkolnej prowadzonej w postaci elektronicznej;
5. komunikacji elektronicznej prowadzonej przez szkołę;
6. bezpieczeństwa uczniów w Internecie, w tym przeciwdziałania cyberprzemocy i ochrony wizerunku uczniów.

## § 4. Odpowiedzialność dyrektora szkoły

Dyrektor szkoły odpowiada za organizację cyberbezpieczeństwa w szkole, nadzoruje przestrzeganie niniejszej procedury oraz zapewnia, aby działania w tym zakresie były faktycznie realizowane, dokumentowane i okresowo sprawdzane.

Do zadań dyrektora należy w szczególności:

1. zapewnienie, aby szkoła posiadała aktualną procedurę cyberbezpieczeństwa;
2. wyznaczenie osób odpowiedzialnych za wybrane obszary bezpieczeństwa cyfrowego, jeżeli jest to potrzebne ze względu na organizację pracy szkoły;
3. nadzorowanie nadawania, zmiany i odbierania uprawnień do systemów informatycznych;
4. zapewnienie ochrony danych osobowych zgodnie z RODO;
5. organizowanie szkoleń pracowników z zakresu cyberbezpieczeństwa, ochrony danych osobowych i bezpiecznej komunikacji elektronicznej;
6. nadzorowanie sposobu korzystania z dziennika elektronicznego;
7. zapewnienie reagowania na incydenty cyberbezpieczeństwa;
8. prowadzenie albo nadzorowanie prowadzenia rejestru incydentów;
9. zapewnienie wykonywania przeglądu zasad cyberbezpieczeństwa co najmniej raz w roku;
10. dokumentowanie działań podjętych w zakresie cyberbezpieczeństwa.

W przypadku szkoły niepublicznej prowadzonej przez fundację część obowiązków technicznych może być wykonywana przez organ prowadzący, zewnętrznego informatyka albo firmę IT, jednak dyrektor szkoły powinien posiadać dokumenty potwierdzające, że obowiązki te są faktycznie realizowane.

## § 5. Osoby odpowiedzialne za cyberbezpieczeństwo

W szkole mogą zostać wyznaczone następujące osoby odpowiedzialne za poszczególne obszary:

1. **Dyrektor szkoły** – odpowiada za organizację i nadzór nad systemem cyberbezpieczeństwa.
2. **Administrator systemów informatycznych albo osoba obsługująca IT** – odpowiada za techniczne zabezpieczenia urządzeń, aktualizacje, kopie zapasowe, zabezpieczenia sieci oraz usuwanie usterek.
3. **Osoba odpowiedzialna za dziennik elektroniczny** – odpowiada za nadawanie kont, kontrolę uprawnień, kontakt z operatorem systemu oraz reagowanie na problemy użytkowników.
4. **Inspektor ochrony danych albo osoba odpowiedzialna za RODO** – wspiera dyrektora w sprawach naruszeń ochrony danych osobowych, analizy ryzyka, upoważnień i dokumentacji RODO.
5. **Pedagog, psycholog, wychowawcy klas** – reagują w sytuacjach cyberprzemocy, zagrożeń wobec uczniów, publikowania kompromitujących treści, hejtu, nękania albo przemocy w komunikatorach internetowych.
6. **Nauczyciele informatyki i wychowawcy** – prowadzą działania edukacyjne z zakresu bezpiecznego korzystania z Internetu.

Wyznaczenie osób odpowiedzialnych powinno być potwierdzone pisemnie, np. w zarządzeniu dyrektora, zakresie obowiązków albo upoważnieniu wewnętrznym.

§ 6. Inwentaryzacja sprzętu i systemów ICT

Szkoła prowadzi wykaz sprzętu informatycznego i systemów ICT wykorzystywanych w działalności szkoły. Wykaz ten powinien umożliwiać ustalenie, jakie urządzenia, programy i systemy są używane, kto z nich korzysta, gdzie się znajdują oraz kto odpowiada za ich bezpieczeństwo.

Wykaz obejmuje w szczególności:

1. komputery stacjonarne;
2. laptopy;
3. tablety;
4. drukarki i skanery;
5. routery i urządzenia sieciowe;
6. tablice interaktywne;
7. nośniki danych;
8. systemy wykorzystywane do prowadzenia dokumentacji szkolnej;
9. dziennik elektroniczny;
10. pocztę elektroniczną;
11. formularze elektroniczne;
12. narzędzia do komunikacji z rodzicami;
13. programy wykorzystywane w pracy dydaktycznej i administracyjnej.

Wykaz powinien być aktualizowany po zakupie nowego sprzętu, wycofaniu sprzętu z użytkowania, zmianie osoby odpowiedzialnej albo zmianie sposobu użytkowania danego systemu.

§ 7. Zarządzanie uprawnieniami

Dostęp do systemów informatycznych szkoły otrzymują wyłącznie osoby, którym dostęp jest niezbędny do wykonywania obowiązków służbowych albo korzystania z usług edukacyjnych.

Szkoła stosuje zasadę minimalnych uprawnień, co oznacza, że użytkownik otrzymuje tylko taki zakres dostępu, jaki jest konieczny do realizacji jego zadań.

Nadanie uprawnień powinno być udokumentowane. W dokumentacji należy wskazać:

1. imię i nazwisko użytkownika;
2. system, do którego nadano dostęp;
3. zakres uprawnień;
4. datę nadania uprawnień;
5. osobę zatwierdzającą dostęp;
6. datę odebrania albo zmiany uprawnień.

Uprawnienia należy niezwłocznie odebrać w przypadku:

1. rozwiązania umowy z pracownikiem;
2. zakończenia współpracy z osobą zewnętrzną;
3. zmiany stanowiska albo zakresu obowiązków;
4. utraty potrzeby korzystania z systemu;
5. podejrzenia naruszenia bezpieczeństwa konta;
6. naruszenia przez użytkownika zasad cyberbezpieczeństwa.

Dyrektor albo osoba przez niego wyznaczona dokonuje przeglądu uprawnień co najmniej raz w roku, a także każdorazowo po zmianach kadrowych.

§ 8. Hasła i konta użytkowników

Każdy użytkownik systemu informatycznego szkoły korzysta z indywidualnego konta. Zabronione jest korzystanie ze wspólnych kont pracowniczych, chyba że z przyczyn technicznych nie można tego uniknąć, a sposób korzystania z takiego konta został zabezpieczony i opisany.

Hasła powinny być tworzone w sposób ograniczający ryzyko ich odgadnięcia. Hasło nie powinno zawierać imienia, nazwiska, daty urodzenia, nazwy szkoły ani prostych ciągów znaków.

Użytkownik nie może:

1. przekazywać hasła innej osobie;
2. zapisywać hasła na kartce przy komputerze;
3. wysyłać hasła przez e-mail lub komunikator;
4. używać tego samego hasła do prywatnych i służbowych systemów;
5. pozostawiać otwartego konta bez nadzoru.

W przypadku podejrzenia, że hasło zostało ujawnione, użytkownik ma obowiązek niezwłocznie

zmienić hasło i poinformować dyrektora albo osobę odpowiedzialną za dany system.

§ 9. Zasady korzystania ze sprzętu szkolnego

Sprzęt szkolny może być wykorzystywany wyłącznie do celów związanych z działalnością szkoły, w szczególności do prowadzenia zajęć, przygotowywania materiałów dydaktycznych, prowadzenia dokumentacji, komunikacji służbowej oraz wykonywania obowiązków administracyjnych.

Pracownik korzystający ze sprzętu szkolnego odpowiada za jego prawidłowe użytkowanie, zabezpieczenie przed zniszczeniem oraz ochronę przed dostępem osób nieuprawnionych.

Zabrania się:

1. instalowania programów bez zgody dyrektora albo osoby odpowiedzialnej za IT;
2. pobierania plików z niepewnych źródeł;
3. korzystania z nielegalnego oprogramowania;
4. obchodzenia zabezpieczeń technicznych;
5. przekazywania sprzętu osobom nieuprawnionym;
6. pozostawiania urządzenia bez nadzoru w miejscu dostępnym dla uczniów albo osób postronnych;
7. przechowywania dokumentacji zawierającej dane osobowe na niezabezpieczonym pulpicie, prywatnym pendrivie albo prywatnym dysku.

Sprzęt szkolny powinien być zabezpieczony hasłem, aktualnym oprogramowaniem antywirusowym oraz aktualizacjami systemowymi, jeżeli pozwalają na to warunki techniczne.

**§ 10. Korzystanie z prywatnych urządzeń**

Korzystanie z prywatnych urządzeń do celów służbowych powinno być ograniczone do niezbędnego minimum. Pracownik nie powinien przechowywać dokumentacji szkolnej ani danych osobowych uczniów na prywatnym komputerze, telefonie, tablecie, prywatnym dysku internetowym albo prywatnej skrzynce e-mail.

Jeżeli z przyczyn organizacyjnych pracownik musi skorzystać z prywatnego urządzenia, powinien zapewnić, aby urządzenie było zabezpieczone hasłem, aktualizowane, chronione przed dostępem osób trzecich i używane w sposób uniemożliwiający ujawnienie danych uczniów.

Zabrania się wykonywania prywatnym telefonem zdjęć dokumentacji ucznia, opinii, orzeczeń, dzienników, list obecności, danych kontaktowych rodziców albo innych dokumentów zawierających dane osobowe, chyba że dyrektor wyraził na to zgodę w szczególnie uzasadnionej sytuacji i określił sposób zabezpieczenia takich danych.

**§ 11. Poczta elektroniczna**

Komunikacja służbowa szkoły powinna odbywać się z wykorzystaniem służbowych adresów e-mail albo systemów wskazanych przez szkołę.

Pracownik szkoły, przesyłając wiadomość e-mail zawierającą dane osobowe, powinien upewnić się, że adres odbiorcy jest prawidłowy, a zakres przekazywanych informacji jest niezbędny do załatwienia sprawy.

W przypadku wysyłania wiadomości do wielu rodziców należy stosować ukrytą kopię, jeżeli ujawnienie adresów e-mail innym odbiorcom nie jest uzasadnione.

Dokumenty zawierające szczególne kategorie danych, informacje o zdrowiu, opinie psychologiczne, orzeczenia, dane dotyczące sytuacji rodzinnej albo dokumentację pomocy psychologiczno-pedagogicznej powinny być przesyłane z zachowaniem podwyższonych środków ostrożności, np. w pliku zabezpieczonym hasłem przekazanym innym kanałem komunikacji.

Pracownik nie otwiera załączników i linków pochodzących z podejrzanych wiadomości, szczególnie gdy wiadomość zawiera presję czasu, prośbę o podanie hasła, informację o rzekomym zablokowaniu konta albo nietypową prośbę o płatność.

**§ 12. Dziennik elektroniczny**

Dziennik elektroniczny jest jednym z podstawowych systemów przetwarzania danych uczniów, dlatego korzystanie z niego wymaga szczególnej staranności.

Każdy użytkownik dziennika elektronicznego korzysta wyłącznie z własnego konta i nie udostępnia loginu ani hasła innej osobie.

Nauczyciel jest zobowiązany do:

1. prawidłowego dokumentowania zajęć;

2. niewprowadzania danych niezgodnych ze stanem faktycznym;
3. ochrony danych uczniów widocznych w systemie;
4. niewyświetlania danych uczniów osobom nieuprawnionym;
5. wylogowania się po zakończeniu pracy;
6. zgłoszenia problemu z dostępem, podejrzenia przejęcia konta albo błędnych uprawnień.

Rodzice i uczniowie korzystający z kont w dzienniku elektronicznym powinni być informowani, że konto jest indywidualne i nie powinno być przekazywane innym osobom.

W przypadku zakończenia pracy nauczyciela w szkole dostęp do dziennika powinien zostać odebrany niezwłocznie, nie później niż w dniu zakończenia współpracy.

## § 13. Bezpieczeństwo Internetu w szkole

Szkoła zapewnia uczniom dostęp do Internetu wyłącznie w celach edukacyjnych i pod nadzorem nauczyciela albo innej osoby prowadzącej zajęcia.

Szkoła podejmuje działania ograniczające dostęp uczniów do treści, które mogą zagrażać ich prawidłowemu rozwojowi, w szczególności treści pornograficznych, przemocowych, hazardowych, nawołujących do nienawiści, samouszkodzeń, używania środków psychoaktywnych albo innych treści nieodpowiednich dla małoletnich.

Nauczyciel, który wykorzystuje Internet podczas zajęć, powinien wcześniej sprawdzić materiały udostępniane uczniom, zwłaszcza filmy, linki, strony internetowe i aplikacje.

Uczniowie nie mogą korzystać ze szkolnej sieci ani sprzętu szkolnego do:

1. obrażania innych osób;
2. publikowania cudzych zdjęć bez zgody;
3. nagrywania nauczycieli i uczniów bez zgody;
4. przesyłania treści wulgarnych, przemocowych albo dyskryminujących;
5. podszywania się pod inne osoby;
6. logowania się na cudze konta;
7. obchodzenia zabezpieczeń sieciowych.

Zasady bezpieczeństwa w Internecie powinny być omawiane z uczniami co najmniej raz w roku szkolnym oraz każdorazowo po ujawnieniu niepokojących zdarzeń.

## § 14. Cyberprzemoc

Cyberprzemocą jest każde zachowanie z użyciem technologii cyfrowych, które narusza godność, bezpieczeństwo, prywatność albo dobro dziecka lub pracownika szkoły.

Za cyberprzemoc uznaje się w szczególności:

1. obrażanie, poniżanie albo wyśmiewanie w Internecie;
2. publikowanie kompromitujących zdjęć, nagrań albo komentarzy;
3. groźby kierowane przez komunikatory, media społecznościowe albo SMS;
4. podszywanie się pod inną osobę;
5. tworzenie fałszywych kont;
6. wykluczanie z grup internetowych w sposób krzywdzący;
7. rozpowszechnianie plotek;
8. nagrywanie i publikowanie wizerunku bez zgody;
9. udostępnianie danych osobowych bez uprawnienia;
10. przesyłanie treści o charakterze seksualnym, przemocowym albo upokarzającym.

W przypadku zgłoszenia cyberprzemocy pracownik szkoły nie bagatelizuje sprawy, nie odsyła dziecka bez pomocy i nie wymaga od ucznia samodzielnego rozwiązania sytuacji. Pracownik przyjmuje zgłoszenie, sporządza notatkę służbową i przekazuje sprawę wychowawcy, pedagogowi, psychologowi albo dyrektorowi.

Szkoła podejmuje działania zgodne ze Standardami Ochrony Małoletnich, w tym rozpoznaje sytuację dziecka, zapewnia wsparcie, kontaktuje się z rodzicami oraz w razie potrzeby zawiadamia właściwe instytucje. Standardy szkoły przewidują obowiązek reagowania na podejrzenie krzywdzenia dziecka i sporządzania dokumentacji interwencji.

## § 15. Ochrona wizerunku uczniów

Wizerunek ucznia podlega ochronie. Zdjęcia, nagrania i materiały przedstawiające uczniów mogą być utrwalane i publikowane wyłącznie zgodnie z przepisami prawa, polityką ochrony danych

osobowych szkoły oraz uzyskanymi zgodami.

Pracownik szkoły nie może publikować zdjęć uczniów na prywatnych profilach społecznościowych, prywatnych komunikatorach ani prywatnych stronach internetowych.

Przed publikacją materiału na stronie internetowej szkoły albo w mediach społecznościowych należy upewnić się, że szkoła posiada odpowiednią zgodę rodzica albo opiekuna prawnego, a publikacja jest zgodna z celem, dla którego zgoda została udzielona.

Jeżeli rodzic cofnął zgodę na publikację wizerunku dziecka, szkoła powinna zaprzestać dalszej publikacji wizerunku tego dziecka, z uwzględnieniem możliwości technicznych usunięcia wcześniej opublikowanych materiałów.

## § 16. Ochrona danych osobowych

Dane osobowe uczniów, rodziców i pracowników mogą być przetwarzane wyłącznie w zakresie niezbędnym do realizacji zadań szkoły.

Pracownik szkoły ma obowiązek chronić dane osobowe przed:

1. dostępem osób nieuprawnionych;
2. przypadkowym ujawnieniem;
3. utratą;
4. zniszczeniem;
5. nieuprawnioną zmianą;
6. przesłaniem do niewłaściwego odbiorcy;
7. publikacją bez podstawy prawnej.

Dokumenty zawierające dane osobowe nie mogą być pozostawiane na biurku, w sali lekcyjnej, przy drukarce, w pokoju nauczycielskim ani w innym miejscu dostępnym dla osób nieuprawnionych.

Dane szczególnie chronione, takie jak informacje o zdrowiu, opinie, orzeczenia, dokumentacja pomocy psychologiczno-pedagogicznej, informacje o sytuacji rodzinnej dziecka albo dokumentacja interwencji, powinny być przetwarzane ze szczególną ostrożnością.

W przypadku podejrzenia naruszenia ochrony danych osobowych szkoła stosuje odrębną Procedurę postępowania w przypadku naruszenia ochrony danych osobowych.

## § 17. Kopie zapasowe

Szkoła zapewnia wykonywanie kopii zapasowych danych, jeżeli dane są przechowywane lokalnie albo w systemach, za które szkoła odpowiada organizacyjnie.

Celem wykonywania kopii zapasowych jest zapewnienie możliwości odtworzenia danych w przypadku awarii, ataku ransomware, przypadkowego usunięcia plików, uszkodzenia urządzenia albo innego zdarzenia powodującego utratę danych.

Kopie zapasowe powinny być:

1. wykonywane regularnie;
2. przechowywane w bezpiecznym miejscu;
3. zabezpieczone przed dostępem osób nieuprawnionych;
4. okresowo sprawdzane pod kątem możliwości odtworzenia;
5. dokumentowane w rejestrze kopii zapasowych.

Jeżeli szkoła korzysta z systemów zewnętrznych, takich jak dziennik elektroniczny albo system pocztowy, dyrektor powinien posiadać informację, kto odpowiada za bezpieczeństwo i kopie zapasowe danych w tych systemach.

## § 18. Aktualizacje i zabezpieczenia techniczne

Szkoła zapewnia, aby urządzenia i systemy wykorzystywane w pracy szkoły były regularnie aktualizowane.

Aktualizacje powinny obejmować:

1. systemy operacyjne;
2. programy antywirusowe;
3. przeglądarki internetowe;
4. oprogramowanie biurowe;
5. programy edukacyjne;
6. systemy zabezpieczeń;
7. urządzenia sieciowe, jeżeli aktualizacje są dostępne.

Nie należy korzystać z oprogramowania, które nie jest już wspierane przez producenta, jeżeli powoduje to istotne ryzyko bezpieczeństwa.

Osoba odpowiedzialna za IT albo dyrektor dokumentuje podstawowe działania dotyczące aktualizacji i zabezpieczeń, przynajmniej w formie notatki, protokołu przeglądu albo wpisu w rejestrze działań technicznych.

### § 19. Praca zdalna i dostęp poza szkołą

Jeżeli pracownik wykonuje zadania służbowe poza szkołą, powinien zapewnić, aby dane uczniów i dokumentacja szkolna były chronione w takim samym stopniu jak na terenie szkoły.

Pracownik wykonujący pracę zdalną nie może:

1. pozostawiać dokumentów szkolnych w miejscu dostępnym dla domowników albo osób trzecich;
2. korzystać z publicznych komputerów do logowania się do systemów szkolnych;
3. zapisywać haseł w przeglądarce na cudzych urządzeniach;
4. przesyłać dokumentów szkolnych przez prywatne komunikatory;
5. drukować dokumentacji szkolnej poza szkołą bez uzasadnionej potrzeby;
6. omawiać spraw uczniów w miejscach publicznych.

Jeżeli pracownik zgubi urządzenie, na którym znajdowały się dane szkolne, ma obowiązek niezwłocznie poinformować dyrektora.

### § 20. Formularze elektroniczne i narzędzia online

Szkoła może korzystać z formularzy elektronicznych, platform edukacyjnych i narzędzi online, jeżeli ich wykorzystanie jest uzasadnione działalnością szkoły i zgodne z zasadami ochrony danych osobowych.

Przed użyciem nowego narzędzia należy sprawdzić:

1. jakie dane będą zbierane;
2. kto będzie administratorem danych;
3. gdzie dane będą przechowywane;
4. czy narzędzie jest adekwatne do celu;
5. czy nie zbiera nadmiernych danych;
6. czy rodzice i uczniowie otrzymali wymaganą informację o przetwarzaniu danych.

Nie należy zbierać przez formularze elektroniczne danych szczególnie wrażliwych, jeżeli nie jest to konieczne i nie zostały zapewnione odpowiednie środki bezpieczeństwa.

### § 21. Incydenty cyberbezpieczeństwa

Incydentem cyberbezpieczeństwa jest każde zdarzenie, które narusza lub może naruszyć bezpieczeństwo systemów informatycznych, danych, kont użytkowników, urządzeń albo komunikacji elektronicznej szkoły.

Za incydent uznaje się w szczególności:

1. włamanie na konto w dzienniku elektronicznym;
2. przejęcie skrzynki e-mail;
3. wysłanie danych osobowych do niewłaściwego adresata;
4. utratę laptopa, pendrive'a albo dokumentacji cyfrowej;
5. zainfekowanie komputera wirusem;
6. zaszyfrowanie danych przez ransomware;
7. ujawnienie hasła;
8. podejrzenie korzystania z konta przez osobę nieuprawnioną;
9. cyberprzemoc wobec ucznia;
10. publikację wizerunku ucznia bez zgody;
11. usunięcie albo zmianę danych bez uprawnienia;
12. brak dostępu do systemu z powodu awarii albo ataku;
13. podejrzane wiadomości phishingowe skierowane do pracowników szkoły.

Każdy pracownik, który zauważy incydent albo podejrzewa jego wystąpienie, ma obowiązek niezwłocznie zgłosić sprawę dyrektorowi.

### § 22. Postępowanie w przypadku incydentu

Po otrzymaniu informacji o incydencie dyrektor albo osoba przez niego wyznaczona podejmuje

działania w następującej kolejności:

1. przyjmuje zgłoszenie i ustala, kto zgłasza incydent;
2. zabezpiecza podstawowe informacje o zdarzeniu;
3. ustala, jakiego systemu, urządzenia albo danych dotyczy incydent;
4. podejmuje działania ograniczające skutki incydentu;
5. w razie potrzeby odłącza urządzenie od sieci;
6. zabezpiecza dowody, np. zrzuty ekranu, wiadomości, daty, adresy e-mail, nazwy kont;
7. ustala, czy doszło do naruszenia ochrony danych osobowych;
8. ustala, czy sprawa dotyczy bezpieczeństwa dziecka;
9. podejmuje decyzję o powiadomieniu rodziców, organu prowadzącego, UODO, Policji, CSIRT NASK albo innych instytucji;
10. dokumentuje zdarzenie w rejestrze incydentów;
11. podejmuje działania naprawcze;
12. analizuje, jak zapobiec podobnym zdarzeniom w przyszłości.

Jeżeli incydent dotyczy danych osobowych, dyrektor stosuje również procedurę naruszeń ochrony danych osobowych i ocenia, czy zachodzi obowiązek zgłoszenia naruszenia do Prezesa UODO.

Jeżeli incydent dotyczy krzywdzenia dziecka albo cyberprzemocy, szkoła stosuje również Standardy Ochrony Małoletnich i procedury interwencyjne obowiązujące w szkole.

Jeżeli incydent ma charakter poważny i może powodować istotne skutki dla działania szkoły, danych albo użytkowników, szkoła analizuje obowiązek zgłoszenia incydentu do właściwego CSIRT. Zgodnie z materiałem przekazanym do opracowania, incydenty poważne powinny być zgłaszane do właściwego CSIRT, najczęściej CSIRT NASK, nie później niż w ciągu 72 godzin od wykrycia.

## § 23. Rejestr incydentów cyberbezpieczeństwa

Szkoła prowadzi rejestr incydentów cyberbezpieczeństwa. Rejestr może być prowadzony w formie papierowej albo elektronicznej, pod warunkiem zapewnienia poufności i integralności zapisów.
Rejestr powinien zawierać:

1. numer incydentu;
2. datę i godzinę zgłoszenia;
3. osobę zgłaszającą;
4. opis zdarzenia;
5. system, urządzenie albo dane, których dotyczy incydent;
6. osoby, których dotyczy zdarzenie;
7. ocenę skutków incydentu;
8. informację, czy doszło do naruszenia danych osobowych;
9. podjęte działania zabezpieczające;
10. decyzję o ewentualnym zgłoszeniu do instytucji zewnętrznych;
11. działania naprawcze;
12. datę zakończenia sprawy;
13. podpis osoby odpowiedzialnej.

Rejestr incydentów jest dokumentem wewnętrznym szkoły i nie powinien być udostępniany osobom nieuprawnionym.

## § 24. Zgłaszanie poważnych incydentów

Jeżeli incydent może spowodować poważne zakłócenie działania szkoły, utratę danych, istotne skutki dla uczniów, rodziców albo pracowników, dyrektor dokonuje oceny, czy incydent należy zgłosić do właściwego zespołu CSIRT.
Przy ocenie powagi incydentu należy brać pod uwagę:

1. liczbę osób, których dotyczy incydent;
2. rodzaj danych objętych incydentem;
3. czas trwania zakłócenia;
4. możliwość odtworzenia danych;
5. wpływ na bezpieczeństwo uczniów;
6. wpływ na prowadzenie zajęć i dokumentacji szkolnej;
7. ryzyko szkody dla osób, których dane dotyczą;
8. możliwość dalszego rozprzestrzeniania się zagrożenia.

Dyrektor dokumentuje decyzję o zgłoszeniu albo braku zgłoszenia incydentu.

### § 25. Analiza ryzyka

Szkoła dokonuje analizy ryzyka w zakresie cyberbezpieczeństwa i ochrony danych osobowych. Analiza ryzyka ma na celu ustalenie, jakie zagrożenia mogą wystąpić w szkole, jakie mogą mieć skutki i jakie działania należy podjąć, aby ograniczyć ryzyko.

Analiza ryzyka powinna obejmować w szczególności:

1. ryzyko utraty danych;
2. ryzyko nieuprawnionego dostępu do dziennika elektronicznego;
3. ryzyko przejęcia konta e-mail;
4. ryzyko cyberprzemocy wobec uczniów;
5. ryzyko publikacji wizerunku ucznia bez zgody;
6. ryzyko korzystania z prywatnych urządzeń;
7. ryzyko braku kopii zapasowych;
8. ryzyko stosowania słabych haseł;
9. ryzyko braku aktualizacji;
10. ryzyko przesłania danych do niewłaściwego odbiorcy;
11. ryzyko nieodebrania uprawnień byłemu pracownikowi.

Wyniki analizy ryzyka powinny prowadzić do konkretnych działań, np. szkolenia pracowników, zmiany haseł, aktualizacji sprzętu, ograniczenia dostępu, poprawy dokumentacji albo zmiany sposobu komunikacji.

### § 26. Przegląd systemu cyberbezpieczeństwa

Dyrektor szkoły zapewnia przegląd systemu cyberbezpieczeństwa co najmniej raz w roku.

Przegląd powinien obejmować:

1. aktualność procedury cyberbezpieczeństwa;
2. aktualność wykazu sprzętu i systemów;
3. aktualność uprawnień użytkowników;
4. realizację szkoleń;
5. rejestr incydentów;
6. działania naprawcze po incydentach;
7. skuteczność kopii zapasowych;
8. bezpieczeństwo dziennika elektronicznego;
9. bezpieczeństwo poczty elektronicznej;
10. zabezpieczenie urządzeń;
11. ryzyka związane z cyberprzemocą;
12. zgodność z dokumentacją RODO i Standardami Ochrony Małoletnich.

Z przeglądu sporządza się protokół, który zawiera ustalenia, wnioski i zalecenia do realizacji. Materiał przekazany przez szkołę wskazuje, że po zmianach w KSC system bezpieczeństwa powinien być przeglądany co najmniej raz w roku oraz dokumentowany.

### § 27. Szkolenia pracowników

Szkoła organizuje szkolenia pracowników z zakresu cyberbezpieczeństwa i ochrony danych osobowych nie rzadziej niż raz w roku szkolnym oraz każdorazowo wtedy, gdy pojawią się nowe istotne zagrożenia albo zmiany w procedurach.

Szkolenie powinno obejmować co najmniej:

1. zasady bezpiecznego korzystania z poczty elektronicznej;
2. rozpoznawanie phishingu;
3. ochronę haseł;
4. korzystanie z dziennika elektronicznego;
5. ochronę danych osobowych uczniów;
6. zasady przesyłania dokumentów;
7. reagowanie na incydenty;
8. cyberprzemoc i ochronę małoletnich;
9. ochronę wizerunku uczniów;
10. korzystanie z prywatnych urządzeń;

11.zasady pracy zdalnej.

Udział pracownika w szkoleniu powinien być potwierdzony podpisem na liście obecności albo innym dowodem zapoznania się z materiałami.

## § 28. Edukacja uczniów i rodziców

Szkoła prowadzi działania edukacyjne skierowane do uczniów i rodziców w zakresie bezpiecznego korzystania z Internetu, cyberprzemocy, ochrony danych, ochrony wizerunku oraz odpowiedzialności za zachowanie w sieci.

Wychowawcy klas omawiają z uczniami zasady bezpiecznego korzystania z Internetu co najmniej raz w roku szkolnym. Tematyka ta może być realizowana podczas godzin wychowawczych, zajęć informatyki, spotkań z pedagogiem, psychologiem albo innych działań profilaktycznych.

Rodzice są informowani o zasadach cyberbezpieczeństwa podczas zebrań, przez dziennik elektroniczny albo przez materiały udostępniane przez szkołę.

Działania te są spójne ze Standardami Ochrony Małoletnich, które przewidują edukację dzieci i rodziców w zakresie zagrożeń, bezpiecznych relacji, korzystania z Internetu i ochrony wizerunku.

## § 29. Dokumentowanie działań

Szkoła dokumentuje działania podejmowane w zakresie cyberbezpieczeństwa. Dokumentacja może obejmować:

1. procedurę cyberbezpieczeństwa;
2. zarządzenie dyrektora o wprowadzeniu procedury;
3. wykaz sprzętu i systemów ICT;
4. rejestr osób z dostępem do systemów;
5. rejestr nadania i odebrania uprawnień;
6. rejestr incydentów cyberbezpieczeństwa;
7. rejestr naruszeń ochrony danych osobowych;
8. protokoły przeglądu systemu cyberbezpieczeństwa;
9. analizę ryzyka;
10. listy obecności ze szkoleń;
11. oświadczenia pracowników o zapoznaniu się z procedurą;
12. notatki służbowe dotyczące incydentów;
13. potwierdzenia działań naprawczych;
14. dokumentację zgłoszeń do instytucji zewnętrznych, jeżeli takie zgłoszenia były dokonywane.

Dokumentowanie działań jest istotne, ponieważ nowe przepisy i praktyka kontroli wymagają wykazania realnego wdrożenia zasad bezpieczeństwa, a nie tylko posiadania dokumentów.

## § 30. Postanowienia końcowe

Procedura wchodzi w życie z dniem zatwierdzenia przez dyrektora szkoły.

Z procedurą zapoznaje się wszystkich pracowników szkoły. Potwierdzeniem zapoznania się z procedurą jest podpis pracownika na liście albo oświadczeniu.

Procedura jest przechowywana w dokumentacji wewnętrznej szkoły. Wersja informacyjna zasad bezpieczeństwa cyfrowego może zostać udostępniona rodzicom i uczniom na stronie internetowej szkoły, w dzienniku elektronicznym albo na tablicy informacyjnej.

Procedura podlega przeglądowi co najmniej raz w roku szkolnym oraz każdorazowo w przypadku zmiany przepisów prawa, zmiany systemów informatycznych, wystąpienia poważnego incydentu albo zaleceń organów właściwych do spraw cyberbezpieczeństwa.

Załączniki do procedury

1. Wykaz sprzętu i systemów ICT.
2. Rejestr osób posiadających dostęp do systemów informatycznych.
3. Wzór zgłoszenia incydentu cyberbezpieczeństwa.
4. Rejestr incydentów cyberbezpieczeństwa.
5. Protokół rocznego przeglądu cyberbezpieczeństwa.
6. Oświadczenie pracownika o zapoznaniu się z procedurą.
7. Lista kontrolna cyberbezpieczeństwa dla dyrektora szkoły.