Regulamin Ochrony danych Osobowych
obowiązujący w Zespole Szkół Ponadgimnazjalnych w Wodzisławiu Śląskim

Niniejszy regulamin stanowi wyciąg najistotniejszych zapisów zawartych w Polityce Bezpieczeństwa Ochrony Danych Osobowych oraz Instrukcji zarządzania systemami informatycznymi i obowiązuje osoby zatrudnione w Zespole Szkół Ponadgimnazjalnych w Wodzisławiu Śląskim, zwanym dalej „szkołą".

§ 1

Zasady bezpiecznego użytkowania komputerów

1. Należy mieć świadomość, że dane osobowe mogą się znajdować na twardych dyskach komputerów stacjonarnych i komputerów przenośnych.
2. Pracownik zobowiązany jest do zabezpieczenia komputerów przed dostępem osób nieupoważnionych, wglądem w dane osobowe oraz kradzieżą.
3. Pracownik ma obowiązek natychmiast zgłosić zagubienie, utratę lub zniszczenie powierzonego mu komputera.
4. Samowolne zmiany (montaż, demontaż) w wyposażeniu komputera bez zgody dyrektora szkoły są zabronione.

§ 2

Zasady korzystania z oprogramowania

1. Pracownik zobowiązuje się do korzystania wyłącznie z oprogramowania legalnego pochodzenia.
2. Instalowanie jakiegokolwiek oprogramowania na komputerach może być dokonane wyłącznie przez osobę upoważnioną lub za jej zgodą.
3. Użytkownicy nie mają prawa do zmiany parametrów systemu operacyjnego komputera, które mogą być zmienione tylko przez osobę upoważnioną.

§ 3

Zasady korzystania z Internetu

1. Pracownik zobowiązany jest do korzystania z internetu wyłącznie w celach służbowych, chyba że dyrektor szkoły wyrazi zgodę na inne cele.
2. Zabrania się zapisywania na dysk twardy komputera oraz uruchamiania nielegalnych/nielicencjonowanych programów oraz plików pobranych z niewiadomego źródła. Pliki takie powinny być pobierane tylko za każdorazową zgodą Administratora Danych Osobowych lub Administratora Systemów Informatycznych i tylko w uzasadnionych przypadkach.
3. Pracownik ponosi odpowiedzialność za szkody spowodowane przez oprogramowanie instalowane z Internetu.
4. Zabrania się wchodzenia na strony, na których prezentowane są informacje o charakterze przestępczym, hakerskim, pornograficznym, lub innym zakazanym przez prawo (na większości stron tego typu jest zainstalowane szkodliwe oprogramowanie, infekujące w sposób automatyczny system operacyjny komputera szkodliwym oprogramowaniem).
5. Nie należy w opcjach przeglądarki internetowej włączać opcji autouzupełniania formularzy i zapamiętywania haseł.
6. W przypadku korzystania z szyfrowanego połączenia przez przeglądarkę, należy zwracać uwagę na pojawienie się odpowiedniej ikonki (kłódka) oraz adresu www rozpoczynającego się frazą"https:"
7. Należy zachować szczególną ostrożność w przypadku żądania lub prośby podania kodów, PIN-ów, numerów kart płatniczych przez Internet. Szczególnie tyczy się to żądania podania takich informacji przez rzekomy bank.

§ 4

Zasady korzystania z poczty elektronicznej

1. Przesyłanie danych osobowych z użyciem maila poza szkołę, może odbywać się tylko przez osoby do tego upoważnione, z wykorzystaniem szkolnej poczty elektronicznej.
2. W przypadku wysyłania danych osobowych mailem, pliki należy zabezpieczyć hasłem. Hasło musi się składać z minimum 8 znaków: duże i małe litery i cyfry lub znaki specjalne. Hasło należy przesłać odrębnym mailem lub inną metodą, np. telefonicznie lub SMS-em. Rekomendowane jest hasło co najmniej 12 znakowe.
3. Użytkownicy powinni zwracać szczególną uwagę na poprawność adresu odbiorcy dokumentu.
4. Zaleca się, aby użytkownik podczas przesyłania danych osobowych mailem zawarł w treści prośbę o potwierdzenie otrzymania i zapoznania się z informacją przez adresata.
5. Nie należy otwierać załączników (np. plików z rozszerzeniem .exe) w mailach nadesłanych przez nieznanego lub znanego nadawcę.
6. Pracownicy nie powinni rozsyłać za pośrednictwem maila informacji o zagrożeniach dla systemu informatycznego, „łańcuszków szczęścia", itp.
7. Pracownicy powinni okresowo usuwać niepotrzebne maile ze swoich skrzynek pocztowych.
8. Podczas wysyłania maili do wielu adresatów jednocześnie, należy użyć metody „Ukryte do wiadomości – UDW”.

§ 5

Ochrona antywirusowa

1. Zaleca się, aby pracownicy skanowali pliki wprowadzane z zewnętrznych nośników programem antywirusowym.
2. Zakazane jest wyłączanie systemu antywirusowego podczas pracy systemu informatycznego przetwarzającego dane osobowe.
3. W przypadku stwierdzenia zainfekowania systemu, Pracownik zobowiązany jest poinformować niezwłocznie o tym fakcie Administratora Systemów Informatycznych lub osobę upoważnioną.

§ 6

Nadawanie upoważnień i uprawnień do przetwarzania danych osobowych

1. Za nadawanie, aktualizację i anulowanie upoważnień odpowiada Administrator Danych Osobowych.
2. Każdy użytkownik systemu przed nadaniem upoważnienia musi zapoznać się z niniejszym regulaminem lub odbyć szkolenie z zasad ochrony danych osobowych oraz podpisać Oświadczenie o poufności.
3. Upoważnienie nadawane jest do zbiorów w wersji papierowej i elektronicznej
4. W przypadku, gdy upoważnienie udzielane jest do zbioru w wersji elektronicznej, nadawany jest użytkownikowi identyfikator w systemie
5. W przypadku anulowania upoważnienia, identyfikator użytkownika jest blokowany w systemie

§ 7

Polityka haseł

1. Hasło dostępu do programu lub do systemu operacyjnego komputera zawierającego dane osobowe składa się co najmniej z 8 znaków (dużych i małych liter oraz z cyfr lub znaków specjalnych).
2. Zmiana hasła do następuje nie rzadziej, niż co 30 dni oraz niezwłocznie w przypadku podejrzenia, że hasło mogło zostać ujawnione.
3. Jeżeli zmiany hasła nie wymusza system, wówczas do zmiany hasła zobowiązany jest użytkownik.
4. Użytkownik systemu w trakcie pracy w aplikacji może zmienić swoje hasło.

5. Hasła nie mogą być powszechnie używanymi słowami. W szczególności nie należy jako haseł wykorzystywać: dat, imion, nazwisk, inicjałów, numerów rejestracyjnych samochodów, numerów telefonów.
6. Użytkownik zobowiązuje się do zachowania hasła w poufności, nawet po utracie przez nie ważności.
7. Zabronione jest zapisywanie haseł w sposób jawny oraz przekazywanie ich innym osobom.

§ 8

Procedura rozpoczęcia, zawieszenia i zakończenia pracy z systemem informatycznym przetwarzającym dane osobowe

1. Użytkownik rozpoczyna pracę z systemem informatycznym z użyciem identyfikatora i hasła.
2. Użytkownik jest zobowiązany do korzystania z komputerów zabezpieczonych oprogramowaniem antywirusowym i zaporą sieciową oraz uniemożliwienia wglądu osobom niepowołanym do danych wyświetlanych na monitorach komputerowych – tzw. polityka czystego ekranu.
3. Przed czasowym opuszczeniem stanowiska pracy, użytkownik zobowiązany jest wywołać blokowany hasłem wygaszacz ekranu lub wylogować się z systemu.
4. Po zakończeniu pracy, użytkownik zobowiązany jest:
   a. wylogować się z systemu informatycznego, a następnie wyłączyć sprzęt komputerowy,
   b. zabezpieczyć stanowisko pracy, w szczególności wszelką dokumentację oraz nośniki magnetyczne i optyczne, na których znajdują się dane osobowe.

§ 9

Postępowanie z elektronicznymi nośnikami zawierającymi dane osobowe

1. Pracownicy nie mogą wynosić na zewnątrz organizacji elektronicznych nośników informacji (takich jak dyski twarde, pendrive'y, CD, DVD) z zapisanymi danymi osobowymi bez zgody dyrektora szkoły.
2. Dane osobowe wynoszone poza organizację muszą być zaszyfrowane.
3. W przypadku uszkodzenia lub zużycia nośnika zawierającego dane osobowe, należy dokonać jego fizycznego zniszczenia lub trwałego usunięcia znajdujących się na nim danych.

§ 10

Postępowanie z danymi osobowymi w wersji papierowej

1. W szkole w wersji papierowej prowadzi się i gromadzi następującą dokumentację zawierającą dane osobowe uczniów:
   a. arkusze ocen,
   b. księgi uczniów,
   c. zezwolenia dyrektora szkoły na:
      - indywidualny program lub tok nauki,
      - spełnianie przez ucznia obowiązku szkolnego lub obowiązku nauki poza szkołą,
   d. zaświadczenia o przebiegu nauczania ucznia,
   e. dokumentację organizacji pomocy psychologiczno – pedagogicznej,
   f. protokoły z konferencji Rady Pedagogicznej,
   g. dokumentację związaną z rekrutacją do klas pierwszych,
   h. dokumentację wycieczek szkolnych,
   i. dokumentację spotkań z rodzicami,
   j. dokumentację zebrań zespołów przedmiotowych, wychowawczych i zespołu ds. integracji,
   k. dokumentację związaną z pomocą materialną, np. programem „wyprawka szkolna",
   l. dokumentację związaną ze stypendiami za osiągnięcia w nauce.

2. Miejscem tworzenia, uzupełniania i przechowywania dokumentacji zawierającej dane osobowe są pomieszczenia szkolne: sekretariat, gabinet dyrektora, gabinet wicedyrektorów, pokój nauczycielski, pomieszczenie kierownika gospodarczego, księgowość, gabinet pomocy psychologiczno-pedagogicznej, biblioteka.
3. Osoby upoważnione do przetwarzania dokumentacji zobowiązane są do zachowania tajemnicy służbowej.
4. Za bezpieczeństwo dokumentów i wydruków zawierających dane osobowe odpowiedzialny jest Administrator Danych Osobowych oraz osoby przez niego upoważnione.
5. Dokumenty i wydruki zawierające dane osobowe przechowuje się w pomieszczeniach zabezpieczonych fizycznie przed dostępem osób nieupoważnionych.
6. Dokumentację, o której mowa w punkcie 1 archiwizuje się zgodnie z Instrukcją archiwizacji.
7. Pracownicy zobowiązani są do stosowania „polityki czystego biurka". Polega ona na zabezpieczeniu dokumentów przed kradzieżą lub wglądem osób nieupoważnionych np. w zamykanych na klucz szafach, biurkach i pomieszczeniach.
8. Osobom prowadzącym dokumentację w szczególności zabrania się:
   - drukowania dokumentacji wymienionej w punkcie 1 poza miejscem pracy,
   - kopiowania, skanowania i fotografowania dokumentacji wymienionej w punkcie 1,
   - wynoszenia poza teren szkoły dokumentacji wymienionej w punkcie 1,
   - pozostawiania dokumentów lub kopii dokumentów zawierających dane osobowe w miejscach, do - których dostęp mogą mieć osoby nieupoważnione do przetwarzania danych osobowych (np. w drukarkach, kserokopiarkach),
   - przekazywania informacji zawierających dane osobowe osobom nieupoważnionym.
9. W przypadku, gdy dokumenty zawierające dane osobowe nie są objęte obowiązkiem archiwizowania lub obowiązek ten ustał, osoby prowadzące dokumentację zobowiązane są do skutecznego zniszczenia tych dokumentów w niszczarce dostępnej w sekretariacie szkoły lub bibliotece szkolnej.
10. Osoby prowadzące dokumentację zobowiązane są do niezwłocznego poinformowania Administratora Danych Osobowych o podejrzeniu dostępu i przetwarzania dokumentacji przez osoby nieupoważnione.
11. W celu zabezpieczenia danych osobowych w dokumentacji diagnozującej postępy w nauce (kartkówkach, sprawdzianach i innych pracach pisemnych ucznia) zaleca się ich pseudonimizację.
12. W przypadku, gdy dokumentacja wymieniona w punkcie 11 zawiera dane osobowe należy dochować wszelkiej staranności w zabezpieczeniu tych prac przed kradzieżą, zniszczeniem i wglądem przez osoby do tego nieupoważnione, na przykład poprzez przechowywanie w zamykanych na klucz szafach, biurkach, pomieszczeniach.
13. O wszelkich przypadkach zagubienia lub zniszczenia dokumentacji należy niezwłocznie powiadomić Administratora Danych Osobowych.

§ 11

Zapewnienie poufności danych osobowych

1. Pracownik zobowiązany jest do zachowania w tajemnicy danych osobowych, do których ma lub będzie miał dostęp w związku z wykonywaniem zadań służbowych lub obowiązków pracowniczych lub zadań zleconych przez Pracodawcę.
2. Pracownik zobowiązany jest do niewykorzystywania danych osobowych w celach pozasłużbowych bądź niezgodnych ze zleceniem, o ile nie są one jawne.
3. Pracownik zobowiązany jest do zachowania w tajemnicy sposobów zabezpieczenia danych osobowych, o ile nie są one jawne.

4. Zabrania się przekazywania bezpośrednio lub przez telefon danych osobowych osobom nieupoważnionym.

§ 12

Skrócona instrukcja postępowania w przypadku naruszenia ochrony danych osobowych

1. Użytkownik zobowiązany jest do powiadomienia Administratora Danych Osobowych w przypadku stwierdzenia lub podejrzenia naruszenia ochrony danych osobowych.
2. Sytuacje, które użytkownik powinien zgłosić Administratorowi Danych Osobowych:
   - ślady na drzwiach, oknach i szafach wskazujące na próbę włamania,
   - niszczenie dokumentacji w sposób umożliwiający odtworzenie danych osobowych,
   - zauważenie na terenie szkoły obecności osób zachowujących się podejrzanie,
   - otwarte drzwi do pozostawionych bez nadzoru pomieszczeń, szaf, gdzie przechowywane są dane osobowe,
   - ustawienie monitorów pozwalające na wgląd osób postronnych w dane osobowe,
   - wynoszenie danych osobowych w wersji papierowej i elektronicznej na zewnątrz organizacji bez upoważnienia ADO,
   - udostępnienie danych osobowych osobom nieupoważnionym w formie papierowej, elektronicznej lub ustnej,
   - telefoniczne próby wyłudzenia danych osobowych,
   - kradzież komputerów lub CD/DVD, twardych dysków, Pen-drive z danymi osobowymi
   - maile zachęcające do ujawnienia identyfikatora i/lub hasła,
   - pojawienie się wirusa komputerowego lub niestandardowe zachowanie komputerów,
   - hasła do systemów umiejscowione w miejscach narażonych na wgląd nieupoważnionych osób.

§ 13

Postępowanie dyscyplinarne

1. Przypadki, nieuzasadnionego zaniechania obowiązków wynikających z niniejszego dokumentu potraktowane będą jako ciężkie naruszenie obowiązków pracowniczych. Wobec osoby, która w przypadku naruszenia zabezpieczeń systemu informatycznego lub uzasadnionego domniemania takiego naruszenia nie podjęła działania określonego w niniejszym dokumencie, a w szczególności nie powiadomiła odpowiedniej osoby zgodnie z określonymi zasadami, a także, gdy nie zrealizowała stosownego działania dokumentującego ten przypadek, można wszcząć postępowanie dyscyplinarne.
2. Kara dyscyplinarna, orzeczona wobec osoby uchylającej się od powiadomienia nie wyklucza odpowiedzialności karnej tej osoby zgodnie z Ustawą z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz.U. z 2018, poz. 1000) oraz możliwości wniesienia wobec niej sprawy z powództwa cywilnego przez pracodawcę o zrekompensowanie poniesionych strat.

§ 14

Praktyczne zasady ochrony danych w Zespole Szkół Ponadgimnazjalnych

1. Zakazuje się przekazywania informacji o danych osobowych uczniów osobom nieupoważnionym, np. w sytuacjach towarzyskich, pozazawodowych lub, gdy nie można zweryfikować tożsamości osoby upoważnionej do dostępu do tych informacji. Dotyczy to szczególnie udzielania informacji telefonicznej.
2. Zakazuje się wynoszenia dokumentów zawierających dane osobowe poza szkołę w formie papierowej oraz na nośnikach (np. pen drive), bez zgody dyrektora szkoły lub braku podstawy prawnej.
3. W szczególnych przypadkach za zgodą dyrektora szkoły dozwolone jest wynoszenie danych osobowych poza szkołę na zaszyfrowanych pendrive, jeżeli są one zabezpieczone co najmniej 8

znakowym hasłem, zawierającym duże litery, małe litery, cyfry

4. W szczególnych przypadkach za zgodą dyrektora dozwolone jest wynoszenie danych osobowych poza szkołę na komputerze przenośnym, gdy przechowywane są na zaszyfrowanej partycji twardego dysku, lub gdy pliki z danymi są zahasłowane co najmniej 8 znakowym hasłem, zawierającym duże litery, małe litery, cyfry.
5. Zabrania się przechowywania danych osobowych na komputerach prywatnych i domowych pracowników a w szczególności plików z danymi uczniów
6. Po zakończeniu pracy należy zabezpieczyć (zamykać na klucz w szafach) dokumenty zawierające dane osobowe.
7. Pliki z danymi osobowymi uczniów i pracowników nie powinny być trwale zapisywane na twardych dyskach komputerów, jeżeli komputery nie zapewniają indywidualnego logowania się wszystkich użytkowników. Pliki te powinny być usunięte (skasowane) po ich wykorzystaniu, np. do wydruku.
8. Zobowiązuje się Administratora Systemów Informatycznych do comiesięcznej kontroli stanowisk, na których pracownicy dydaktyczni przetwarzają dane osobowe uczniów, w celu wyeliminowania ich nieuzasadnionego przechowywania.

……

Podpis