Szkoła Podstawowa nr 6
im. Juliusza Słowackiego w Sosnowcu

Ochrona Danych Osobowych
w trakcie nauczania z wykorzystaniem metod
i technik kształcenia na odległość

Dokument opracowano na potrzeby pracy
Szkoły Podstawowej nr 6 im. Juliusza Słowackiego w Sosnowcu

Sosnowiec, 2020 r.

Ochrona Danych Osobowych
w trakcie nauczania z wykorzystaniem metod i technik kształcenia na odległość
w Szkole Podstawowej nr 6 im. Juliusza Słowackiego w Sosnowcu

Postanowienia ogólne

1. W trakcie realizacji nauczania na odległość pracownicy Szkoły Podstawowej nr 6 w Sosnowcu będą przetwarzać dane osobowe zgodnie z Ustawą z dnia 10 maja 2018 r. o ochronie danych osobowych oraz z Rozporządzeniem Ministra Edukacji Narodowej z 20 marca 2020 r. w sprawie szczególnych rozwiązań w okresie czasowego ograniczenia funkcjonowania jednostek systemu oświaty w związku z zapobieganiem, przeciwdziałaniem i zwalczaniem COVID-19.
2. Dyrektor szkoły zobowiązuje wszystkich nauczycieli/ rodziców/ uczniów do wykorzystywania danych osobowych wyłącznie do celów realizacji kształcenia na odległość i tym samym nieudostępniania ich osobom nieupoważnionym, by nie zostały one zniszczone, zmodyfikowane, utracone lub wykorzystane niezgodnie z przeznaczeniem.
3. Nauczyciele zobowiązani są do przetwarzania danych osobowych rodziców oraz uczniów wyłącznie w celach związanych z wykonywaniem swoich obowiązków służbowych.
4. Szkoła może wymagać od ucznia lub reprezentującego go rodzica podania danych do założenia konta w systemie nauczania na odległość, ale tylko w zakresie niezbędnym do tego, aby to konto założyć. Nauczyciele nie powinni przy takiej okazji gromadzić danych nadmiarowych bądź służących do realizacji innych celów.
5. W podstawowym zakresie komunikację z uczniami i rodzicami nauczyciele prowadzą poprzez wdrożone w szkole rozwiązania teleinformatyczne m.in. dziennik elektroniczny Librus.

Nauczyciele i pracownicy szkoły

1. Dyrektor szkoły zobowiązuje wszystkich nauczycieli/pracowników szkoły do przekazania informacji na temat narzędzi, które są przez nich wykorzystywane do prowadzenia nauczania z wykorzystaniem metod i technik kształcenia na odległość. Na tej podstawie zostanie przygotowane zestawienie przedstawiające

wszystkie narzędzia i formy kształcenia na odległość (wszystkie kanały przetwarzania informacji/danych) realizowane w Szkole Podstawowej nr 6.

2. Dyrektor szkoły zobowiązuje wszystkich nauczycieli/pracowników szkoły do przekazywania danych osobowych wyłącznie za pośrednictwem dziennika elektronicznego Librus.
3. Nauczyciele/pracownicy szkoły do wykonywania swoich obowiązków mogą korzystać z własnych komputerów, telefonów, tabletów itd. Warunkiem jest odpowiednie ich zabezpieczenie poprzez zainstalowanie oprogramowania antywirusowego, dokonywania niezbędnych jego aktualizacji oraz zakładanie odrębnych kont w przypadku, gdy z jednego komputera korzysta wiele osób. Nauczyciele/ pracownicy szkoły, przechowując dane na urządzeniach, do których mogą mieć dostęp inne osoby, powinni używać mocnych haseł dostępowych, a przed odejściem od stanowiska pracy urządzenia każdorazowo blokować przed dostępem osób trzecich.
4. Nauczyciele/pracownicy szkoły, którzy nie mają właściwych warunków do pracy na odległość zgłaszają taki fakt dyrektorowi szkoły. Dyrektor, mając na uwadze odpowiednie zabezpieczenie danych osobowych w takich sytuacjach, umożliwi ww. nauczycielom/pracownikom szkoły korzystanie ze sprzętu znajdującego się w szkole.
5. Nauczyciele/pracownicy szkoły wykorzystujący pocztę elektroniczną do kontaktów z rodzicami/ uczniami powinni pamiętać, aby korzystać z niej w sposób rozważny i bezpieczny. Rekomendowane jest, by nauczyciele do korespondencji e-mailowej z uczniami korzystali ze służbowych adresów e-mail (zakładali konta na czas kształcenia na odległość).
6. Nauczyciele/pracownicy szkoły muszą zwrócić szczególną uwagę na zabezpieczenie danych udostępnianych w przesyłanych wiadomościach. Zawsze przed wysłaniem wiadomości powinni upewnić się, czy niezbędne jest wysłanie określonych danych oraz że zamierzają wysyłać je do właściwego adresata. Ponadto powinni sprawdzić, czy w nazwie adresu e-mail adresata nie ma np. przestawionych lub pominiętych znaków tak, aby nie wysłać takiej wiadomości do osób nieupoważnionych. Podczas wysyłania korespondencji zbiorczej powinni korzystać z opcji „UDW", dzięki której odbiorcy wiadomości nie będą widzieć wzajemnie swoich adresów e-mail. Ponadto nie powinni otwierać wiadomości od nieznanych adresatów.
7. Nauczyciele/pracownicy szkoły, którzy przesyłają dane kanałami elektronicznej wymiany danych powinny je szyfrować (np. hasłem przy „pakowaniu" pliku).

Powinni przy tym pamiętać, by haseł do plików nie przekazywać tym samym kanałem. Jeśli zaszyfrowany plik wysyłany jest pocztą elektroniczną, hasło powinni wysłać SMS-em/ przekazać w rozmowie telefonicznej/ poprzez dziennik elektroniczny itd.

8. Nauczyciele/pracownicy szkoły, którzy przechowują dane na urządzeniach przenośnych (np. pamięć USB), powinni bezwzględnie je szyfrować i chronić hasłem, by zapewnić odpowiednie bezpieczeństwo danych osobowych, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową ich utratą, zniszczeniem lub uszkodzeniem.
9. Nauczyciele korzystający z programów lub aplikacji mobilnych powinni korzystać z możliwych do zastosowania w nich mechanizmów ochrony prywatności użytkowników. Jeśli użycie jakiegoś programu wymaga logowania, nauczyciele powinni zadbać o silne hasło dostępu, a dodatkowo chronić je przed utratą czy dostępem osób nieuprawnionych.
10. Nauczyciele na ogólnie dostępnych portalach lub stronach internetowych mogą jedynie publikować materiały edukacyjne, natomiast nie mogą przetwarzać danych osobowych uczniów lub rodziców.
11. Nauczyciele muszą zachowywać podstawowe zasady bezpieczeństwa przy zdalnym łączeniu się z dziennikiem elektronicznym ze swojego urządzenia w domu.
12. Nauczyciele w celu sprawdzania i monitorowania obecności uczniów w zajęciach prowadzonych na odległość powinni zachować proporcjonalność i minimalizację danych. Dla przykładu nie powinni w tym celu korzystać z narzędzi zbierających dane biometryczne, w tym wykorzystujące systemy wykrywania twarzy.
13. Rodzice mają prawo wiedzieć, jak szkoła jako administrator będzie przetwarzała dane osobowe ich dzieci w trakcie kształcenia na odległość.
14. W trakcie kształcenia na odległość nauczyciele/rodzice/uczniowie powinni wdrażać dobre praktyki pomagające zachować bezpieczeństwo danych podczas lekcji online (Załącznik 1).

Załącznik 1

Dobre praktyki pomagające zachować bezpieczeństwo danych podczas lekcji online

20 zasad bezpieczeństwa, o których powinni pamiętać zarówno szkolni administratorzy, jak i nauczyciele oraz uczniowie, przygotowując się do lekcji online, aby chronić swoje dane

1. Na bieżąco aktualizuj systemy operacyjne.
2. Systematycznie aktualizuj programy antywirusowe, antymalware i antyspyware.
3. Regularnie skanuj stacje robocze programami antywirusowymi, antymalware i antyspyware.
4. Pobieraj oprogramowanie wyłącznie ze stron producentów.
5. Nie otwieraj załączników z nieznanych źródeł dostarczanych poprzez korespondencję elektroniczną.
6. Nie zapamiętuj haseł w aplikacjach webowych.
7. Nie zapisuj haseł na kartkach.
8. Nie używaj tych samych haseł w różnych systemach informatycznych.
9. Zabezpieczaj serwery plików czy inne zasoby sieciowe.
10. Zabezpieczaj sieci bezprzewodowe – Access Point.
11. Dostosuj złożoność haseł odpowiednio do zagrożeń.
12. Unikaj wchodzenia na nieznane czy przypadkowe strony internetowe.
13. Nie loguj się do systemów informatycznych w przypadkowych miejscach z niezaufanych urządzeń lub publicznych niezabezpieczonych sieci Wi-Fi.
14. Wykonuj regularne kopie zapasowe.
15. Korzystaj ze sprawdzonego oprogramowania do szyfrowania e-maili lub nośników danych.
16. Szyfruj dane przesyłane pocztą elektroniczną.
17. Szyfruj dyski twarde w komputerach przenośnych.
18. Przy pracy zdalnej korzystaj z szyfrowanego połączenia VPN.
19. Odchodząc od komputera, blokuj stację komputerową.
20. Nie umieszczaj w komputerze przypadkowo znalezionych nośników USB. Może znajdować się na nich złośliwe oprogramowanie.

Źródło:www.uodo.gov.pl