PRZEDSZKOLE SAMORZĄDOWE NR 26
INTEGRACYJNE
IM. JOANNY STRZAŁKOWSKIEJ-KUCZYŃSKIEJ
w BIAŁYMSTOKU
15-472 Białystok, ul. Ciepła 19
tel./fax 85 6754255, e-mail: psz6@um.bialystok.pl
NIP 5423189823, REGON 200406865

(oznaczenie dyrektora przedszkola)

Zarządzenie Nr 4/2024

Dyrektora Przedszkola Samorządowego Nr 26 Integracyjnego

im. Joanny Strzałkowskiej-Kuczyńskiej w Białymstoku

z dnia 11.03.2024

w sprawie określenia Zasad bezpieczeństwa dla pracowników w Przedszkolu Samorządowym Nr 26 Integracyjnym im. Joanny Strzałkowskiej-Kuczyńskiej w Białymstoku.

Na podstawie art. 68 ust. 1 pkt. 12 ustawy z 14.12.2016 r. - Prawo oświatowe (Dz. U. z 2021 r., poz. 1082) w związku z art. 24 ust. 1 i 2 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L119 s.1 z 2016 r., sprost. Dz. Urz. UE L127 s.2 z 2018 r. , sprost. Dz. Urz. UE L74 s.35 z 2021 r.),

zarządzam, co następuje:

§ 1

1. Ustala się Zasady bezpieczeństwa informacji dla pracowników w **Przedszkolu Samorządowym Nr 26 Integracyjnym im. Joanny Strzałkowskiej-Kuczyńskiej w Białymstoku** w treści stanowiącej załącznik do zarządzenia.

2. Ustanowienie Zasad bezpieczeństwa informacji dla pracowników ma na celu podniesienie poziomu bezpieczeństwa informacji w związku z pracą wykonywaną w **Przedszkolu Samorządowym Nr 26 Integracyjnym im. Joanny Strzałkowskiej-Kuczyńskiej w Białymstoku** poprzez określenie zasad przetwarzania informacji, wprowadzenie procesów ułatwiających zarządzanie i monitorowanie bezpieczeństwa oraz przypisanie odpowiedzialności w sposób zapewniający odpowiedni poziom bezpieczeństwa informacji i oraz zgodnie z obowiązującymi przepisami prawa.

§ 2

Zobowiązuje się wszystkich pracowników **Przedszkola Samorządowego Nr 26 Integracyjnego im. Joanny Strzałkowskiej-Kuczyńskiej w Białymstoku** do przestrzegania **Zasad bezpieczeństwa dla pracowników w Przedszkolu Samorządowym Nr 26 Integracyjnym im. Joanny Strzałkowskiej-Kuczyńskiej w Białymstoku**.

§ 3

Niniejsze zarządzenie wchodzi w życie z dniem podpisania.

DYREKTOR PRZEDSZKOLA
mgr Beata Józefowicz
.....
(podpis dyrektora)

PRZEDSZKOLE SAMORZĄDOWE NR 26
INTEGRACYJNE
IM. JOANNY STRZAŁKOWSKIEJ-KUCZYŃSKIEJ
w BIAŁYMSTOKU
15-472 Białystok, ul. Ciepła 19
tel./fax 85 6754255, e-mail: ps26@um.bialystok.pl
NIP 5423189823, REGON 200406865

Załącznik nr 1
do zarządzenia nr 4/2024
Dyrektora Przedszkola Samorządowego Nr 26 Integracyjnego
im. Joanny Strzałkowskiej-Kuczyńskiej w Białymstoku
z dnia 11.03.2024

Zasady bezpieczeństwa przetwarzania informacji dla pracowników

§ 1

Zakres obowiązywania dokumentu

1. Zasady bezpieczeństwa przetwarzania informacji obowiązują wszystkich pracowników.
2. Zasady bezpieczeństwa przetwarzania informacji dla pracowników nie dotyczą komputerów wykorzystywanych przez uczniów do nauki informatyki lub dostępu do Internetu. Za te komputery odpowiadają wyznaczeni nauczyciele informatyki.
3. Za administrowanie systemem informatycznym odpowiedzialni są informatycy, tj. pracownicy wyznaczeni przez dyrektora placówki lub pracownicy Centrum Usług Informatycznych w Białymstoku, zwani dalej ASI.
4. Każdy pracownik może wykorzystać udostępniony mu system informatyczny, urządzenia oraz dane tylko i wyłącznie w zakresie i na zasadach określonych w niniejszym dokumencie.
5. Nieprzestrzeganie zasad określonych w niniejszym dokumencie może stanowić naruszenie obowiązków pracowniczych, a także skutkować konsekwencjami karnymi.

§ 2

Zasady ogólne

1. Ochronie podlegają wszystkie informacje uzyskane w trakcie wykonywania powierzonych do realizacji obowiązków, w szczególności dane osobowe oraz informacje o stosowanych zabezpieczeniach.
2. Pracownik jest zobowiązany do zachowania w tajemnicy chronionych informacji oraz informacji o zabezpieczeniach.
3. Informacje objęte są ochroną niezależnie od formy ich występowania, tj. elektroniczna lub papierowa, a także od formy ich uporządkowania (rejestry, wykazy spraw, bazy danych) lub nieuporządkowania (notatki, pisma).
4. Pracownik może mieć dostęp jedynie do systemów informatycznych, urządzeń oraz danych, które są mu niezbędne do wykonywania obowiązków pracowniczych.
5. Pracownik ponosi pełną odpowiedzialność za powierzone mu urządzenia informatyczne, dokumenty, a także elektroniczne nośniki danych.

6. W przypadku wykrycia incydentu bezpieczeństwa, pracownik zobowiązany jest do zgłoszenia tego faktu Dyrektorowi Przedszkola.

§ 3

Bezpieczeństwo w pomieszczeniach

1. Informacje chronione można przechowywać tylko w wyznaczonych do tego celu pomieszczeniach, takich jak pomieszczenia dyrekcji, pomieszczenia administracji, pokoje nauczycielskie i składy dokumentów.
2. Z uwagi na specyfikę pomieszczeń, w każdym z nich mogą być inne zabezpieczenia, które pracownik zobowiązany jest stosować. O konieczności ich stosowania pracownika informuje przełożony.
3. Ostatni wychodzący z pomieszczenia pracownik obowiązany jest zamknąć je na klucz.
4. Niedopuszczalne jest pozostawienie bez dozoru osoby nieuprawnionej w pomieszczeniach, w których przetwarzane są dane osobowe.
5. Po zakończonej pracy, dokumenty i nośniki z danymi osobowymi należy przechowywać w zamykanych na klucz szafach lub biurkach.
6. W pomieszczeniach, w których mogą przebywać osoby trzecie, monitory komputerów powinny być ustawione w taki sposób, aby uniemożliwić osobom nieuprawnionym wgląd do przetwarzanych informacji.
7. Odchodząc od komputera pracownik powinien zablokować do niego dostęp.

§ 4

Postępowanie z nośnikami informacji

1. Zabrania się wyrzucania dokumentów lub elektronicznych nośników danych, które nie zostały poddane zniszczeniu lub trwałemu usunięciu danych.
2. Dokumenty papierowe zawierające informacje chronione należy niszczyć w niszczarce, a w przypadku braku jej dostępności, dokument należy porwać na nieduże kawałki, które uniemożliwią odczytanie informacji poprzez ponowne złożenie porwanego dokumentu.
3. Prawidłowe usunięcie pliku na komputerze polega na usunięciu go z folderu oraz opróżnieniu kosza w systemie operacyjnym.
4. W celu trwałego usunięcia danych z elektronicznego nośnika danych (np. pendrive, CD, dysk twardy) należy go przekazać ASI, który usunie jego zawartość oprogramowaniem wielokrotnie nadpisującym nośnik.
5. Wszystkie zbędne kopie informacji powstałe w trakcie ich przetwarzania muszą być zniszczone w ciągu 3 dni od zakończenia ich wykorzystywania.

6. Wzory dokumentów powinny być przechowywane bez danych osobowych, tzn. po uzupełnieniu i zrealizowaniu czynności z dokumentem (np. wydruk, przesłanie), należy usunąć z niego dane osobowe.
7. Drukowane dokumenty powinny być odbierane z urządzeń drukujących i skanujących niezwłocznie po zakończeniu drukowania lub skanowania.
8. Należy regularnie sprawdzać (przynajmniej raz dziennie, po zakończeniu pracy), czy w drukarkach, faksach lub kserokopiarkach nie pozostawiono nieodebranych dokumentów.
9. W przypadku wystąpienia błędu podczas drukowania, należy upewnić się, czy w urządzeniu lub pamięci urządzenia nie pozostały dane.

§ 5

Zasady dostępu do środowiska teleinformatycznego

1. Dostęp do zasobów środowiska teleinformatycznego udzielany jest pracownikowi przez ASI na wniosek lub z upoważnienia dyrektora placówki.
2. Obowiązuje zakaz udostępniania swoich kont innym osobom.
3. Hasło nie może być powszechnie używanymi pojedynczymi słowami. W szczególności nie należy jako hasła wykorzystywać: dat, imion, nazwisk, inicjałów, numerów rejestracyjnych samochodów, numerów telefonów, itp.
4. Hasło nie może być ujawnione nawet po utracie przez nie ważności. W przypadku, gdy zachodzi podejrzenie ujawnienia hasła, należy je niezwłocznie zmienić.
5. Przełożony osoby posiadającej nadane uprawnienia w systemie nie ma prawa żądać hasła dostępu do jego konta.
6. W przypadku przekazywania informacji zabezpieczonej ochroną kryptograficzną, hasło do zaszyfrowanej informacji należy przekazać odbiorcy innym kanałem wymiany informacji, np. poprzez telefon, sms, lub osobiście.

§ 6

Zasady korzystania z systemów teleinformatycznych

1. Pracownik ma zakaz samodzielnego instalowania oprogramowania oraz dokonywania samodzielnych zmian w konfiguracji sprzętowej urządzeń informatycznych.
2. Zabronione jest przynoszenie i podłączanie przez pracownika własnych urządzeń do systemu informatycznego, w tym do sprzętu komputerowego lub sieci.
3. Zabronione jest podejmowanie prób omijania lub przełamywania istniejących zabezpieczeń.

§ 7

Zasady korzystania z Internetu

1. Należy ograniczyć korzystanie z Internetu do niezbędnego minimum, unikając korzystania ze stron internetowych nieznanego pochodzenia.
2. Pracownicy nie mogą za pomocą komputerów należących do placówki pobierać, instalować lub przesyłać oprogramowania oraz innych „utworów" w rozumieniu ustawy z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych, chronionych prawem autorskim (utwory muzyczne, filmy, gry komputerowe, itp.), z wyłączeniem realizacji obowiązków służbowych.
3. Pracownik pobierający jakiekolwiek dane na stanowisku komputerowym, jest odpowiedzialny za sprawdzenie ich pod kątem możliwości występowania wirusów.
4. Służbowa poczta elektroniczna jest udostępniana pracownikom wyłącznie do wypełniania obowiązków pracowniczych i nie służy do prowadzenia prywatnej korespondencji.
5. Pracownikom nie wolno używać do realizacji obowiązków służbowych poczty elektronicznej innej niż wskazana przez przełożonego.
6. W ramach korzystania z poczty elektronicznej pracownikowi zabrania się:
   1) automatycznego przeadresowywania i przesyłania służbowej poczty elektronicznej na serwery nie należące do placówki;
   2) otwierania załączników pochodzących z nieznanych źródeł lub z plikami samorozpakowującymi się bądź wykonywalnymi typu: .bat, .com, .exe oraz nielegalnych plików multimedialnych i graficznych;
7. W przypadku potrzeby przesłania pocztą elektroniczną danych osobowych kilku lub więcej osób, dane należy umieścić w zaszyfrowanym załączniku wiadomości.

§ 8

Kopie bezpieczeństwa

1. Za wykonywanie kopii bezpieczeństwa danych zgromadzonych na serwerach odpowiada ASI.
2. Kopie bezpieczeństwa plików zgromadzonych na komputerze pracownik wykonuje we własnym zakresie.
3. Kopie oprogramowania wraz z danymi w bazie danych zainstalowanych na komputerze pracownika, wykonuje ten pracownik zgodnie z procedurą wykonywania kopii bezpieczeństwa dostarczoną przez ASI.

§ 9

Przetwarzanie danych poza placówką

1. Wynoszenie danych osobowych poza teren placówki wymaga uzyskania zgody Dyrektora.
2. Wynoszenie elektronicznego nośnika informacji zawierającego dane osobowe poza teren placówki wymaga jego zaszyfrowania. W celu zaszyfrowania elektronicznego nośnika informacji należy go przekazać ASI.

3. Urządzenia oraz elektroniczne nośniki zawierające dane chronione, a w szczególności komputery przenośne, powinny być zawsze transportowane jako bagaż podręczny i nie należy ich zostawiać bez dozoru w miejscach takich, jak przechowalnie bagażu, kabiny samochodów lub w innych miejscach podatnych na zagrożenie utraty.
4. Zabrania się pozostawiania bez nadzoru osoby upoważnionej, urządzeń przenośnych w środkach transportu publicznego oraz w innych miejscach, w których pracownik nie ma możliwości zapewnienia bezpieczeństwa tym urządzeniom oraz danych na nich zawartych.
5. W przypadku kradzieży urządzenia przenośnego, pracownik niezwłocznie zgłasza kradzież Policji oraz powiadamia Dyrektora.

DYREKTOR PRZEDSZKOLA
mgr Beata Jóźwowicz