

Procedura „Przynieś swoje urządzenie” (BYOD) w Przedszkolu nr 52 „Gołąbki Pocztowe”

1. Cel i zakres zastosowania

1.1. Celem procedury jest określenie zasad korzystania z prywatnych urządzeń elektronicznych (telefonów komórkowych) przez nauczycieli w celach służbowych w Przedszkolu nr 52 „Gołąbki Pocztowe”.

1.2. Procedura ma zapewnić bezpieczeństwo danych przetwarzanych w placówce, ochronę prywatności pracowników oraz zgodność z obowiązującymi przepisami prawa, w tym z RODO.

1.3. Procedura dotyczy wszystkich nauczycieli i pracowników pedagogicznych korzystających z prywatnych urządzeń do wykonywania zdjęć i nagrywania filmów przedstawiających wychowanków podczas zajęć, wydarzeń, wycieczek przedszkolnych.

2. Rodzaje dopuszczonych urządzeń

2.1. Do użytku służbowego dopuszcza się urządzenia spełniające minimalne wymagania techniczne i bezpieczeństwa.

- smartfony z aktualnym systemem Android lub iOS.

2.2. Urządzenie musi być zabezpieczone za pomocą PIN-u, hasła, odcisku palca lub rozpoznawania twarzy.

3. Rejestracja i autoryzacja urządzeń

3.1. Przed rozpoczęciem korzystania z urządzenia do celów służbowych pracownik zgłasza chęć udziału w programie BYOD dyrektorowi przedszkola.

3.2. W zgłoszeniu należy podać: typ urządzenia, numer seryjny, adres MAC (jeśli dotyczy).

3.3. Urządzenie zostaje wpisane do wewnętrznego Rejestru urządzeń BYOD (załącznik nr 1) prowadzonego przez placówkę.

3.4. Korzystanie z niezarejestrowanego urządzenia jest zabronione.

4. Bezpieczeństwo danych i systemów.

4.1. Urządzenie powinno mieć aktywne i aktualne mechanizmy zabezpieczające.

4.2. Pracownik zobowiązany jest chronić dane przed nieuprawnionym dostępem.

4.3. Zabronione jest przechowywanie innych danych osobowych dzieci, rodziców lub pracowników na urządzeniach prywatnych.

5. Dostęp do danych służbowych

5.1. Dostęp do zasobów i danych przedszkola jest możliwy wyłącznie za pośrednictwem zatwierdzonych narzędzi, takich jak: poczta służbowa, platforma edukacyjna „Wrocławska Edukacja”.

5.2. Wykonane zdjęcia i nagrania muszą być przechowywane lokalnie na telefonie. W terminie do 2 dni roboczych pracownik przenosi wykonane materiały na komputer stacjonarny znajdujący się w sali komputerowej przedszkola oraz trwale usuwa materiały z telefonu.

5.3. Zabrania się udostępniania zdjęć, nagrań i innych danych osobowych osobom trzecim, a także przechowywania ich w prywatnych aplikacjach (np. prywatnych chmurach).

5.4. Galeria zdjęć i nagrań zawierających wizerunek wychowanków nie może być udostępniana ani integrowana z aplikacjami takimi jak Facebook, WhatsApp, Messenger, Instagram, TikTok oraz innymi aplikacjami, w tym narzędziami do edycji zdjęć. W przypadku korzystania z takich aplikacji należy ograniczyć uprawnienia dostępu wyłącznie do prywatnych zasobów pracownika.

6. Rozdział danych prywatnych i służbowych

6.1. Dane prywatne i służbowe muszą być wyraźnie rozdzielone.

6.2. Zaleca się korzystanie z oddzielnych folderów lub profili (np. profilu służbowego w telefonie).

6.3. W przypadku konieczności weryfikacji urządzenia pracodawca nie ma prawa dostępu do prywatnych danych pracownika.

6.4. Kontrola urządzenia jest możliwa wyłącznie wtedy, gdy pracownik dobrowolnie i jednoznacznie wyrazi na nią zgodę.

6.5. Dyrektor Przedszkola nr 52 może kontrolować jedynie obszary urządzenia związane z wykonywaniem obowiązków służbowych (np. zawartość folderu ze zdjęciami służbowymi lub aplikację używaną do pracy – „Wrocławska Edukacja”).

6.6. Kontrola musi być ściśle ograniczona do zakresu służbowego i przeprowadzana w sposób nie naruszający prywatności pracownika.

7. Odpowiedzialność pracownika

7.1. Pracownik odpowiada za właściwe i aktualne zabezpieczenie swojego urządzenia.

7.2. Pracownik zobowiązany jest niezwłocznie zgłosić utratę, kradzież lub awarię urządzenia, jeśli sytuacja ta może mieć wpływ na bezpieczeństwo danych przedszkola.

8. Uprawnienia pracodawcy

8.1. Dyrektor lub osoba przez niego upoważniona ma prawo:

- weryfikować zgodność urządzenia z wymaganiami bezpieczeństwa,
- sprawdzać wyłącznie wskazane elementy, takie jak wersja oprogramowania, folder ze zdjęciami wykonanymi na potrzeby przedszkola oraz ustawienia dotyczące synchronizacji danych (np. potwierdzenie braku synchronizacji z prywatnymi chmurami),
- cofnąć zgodę na korzystanie z urządzenia w przypadku naruszenia procedur,
- zażądać niezwłocznego usunięcia danych służbowych z urządzenia.

9. Postępowanie w przypadku utraty lub kradzieży urządzenia

9.1. Pracownik zobowiązany jest natychmiast poinformować dyrektora o utracie lub kradzieży urządzenia.

9.2. Jeśli to możliwe, pracownik powinien zdalnie zablokować dostęp do telefonu.

10. Postępowanie w sytuacjach incydentów naruszenia danych

10.1. Wszelkie podejrzenia naruszenia bezpieczeństwa danych należy niezwłocznie zgłaszać do dyrektora.

10.2. Dyrektor informuje Inspektora Ochrony Danych i podejmuje dalsze działania zgodnie z procedurami wewnętrznej Polityki Ochrony Danych.

11. Zasady odpowiedzialności

11.1. Naruszenie niniejszej procedury może skutkować odpowiedzialnością porządkową zgodnie z przepisami Kodeksu pracy.

11.2. Jeżeli naruszone zostaną przepisy o ochronie danych osobowych, sprawa musi być niezwłocznie zgłoszona do Inspektora Ochrony Danych.

12. Zgodność z prawem i regulacjami

12.1. Procedura została opracowana z uwzględnieniem przepisów:

- Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 (RODO),
- Ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych,
- Kodeksu pracy.

12.2. Procedura podlega corocznej weryfikacji przez dyrektora oraz Inspektora Ochrony Danych.