# Zasady ogólne ochrony danych osobowych dziecka

1. Jednostka oświatowa uznając prawo dziecka do prywatności zapewnia zgodne z przepisami standardy ochrony danych osobowych i wizerunku dziecka.
2. Dane osobowe dzieci gromadzone są na podstawie przepisów obowiązującego prawa w celu realizacji zadań powierzonych jednostce. Dane gromadzone na podstawie przepisów prawa są przez jednostkę przetwarzane w zakresie i czasie, jaki jest w wskazany przepisach.
3. Dane są gromadzone także na podstawie zgody rodziców w celu prezentacji i promocji zespołu oraz docenienia osiągnięć uczniów. Wyrażoną zgodę można wycofać w każdej chwili.
4. Rodzice dzieci zostają poinformowani o celu gromadzenia danych, podstawie prawnej, ich odbiorcach i okresie przechowywania.
5. Rodzice zostają również poinformowani jeśli jakiekolwiek dane będą przekazywane do państw trzecich (tzn. inne, niż państwa Europejskiego Obszaru Gospodarczego) lub gdy dane podlegały będą zautomatyzowanemu podejmowaniu decyzji.
6. Obowiązkowo przekazywane są także informacje na temat przysługujących praw w związku z przetwarzaniem danych, tj:
7. prawa do dostępu do danych oraz ich kopii,
8. prawa do poprawiania i aktualizowania danych,
9. prawa do usunięcia danych lub ograniczenia ich przetwarzania,
10. prawo do przenoszenia danych,
11. złożenia skargi do Urzędu Ochrony Danych Osobowych.
12. Wizerunek ucznia jest przetwarzany w celu:
	* 1. Zapewnienia bezpieczeństwa poprzez rejestrację monitoringiem wizyjnym -
		na podstawie przepisów obowiązującego prawa.
		2. Prezentacji działań szkoły i osiągnięć ucznia na terenie zespołu oraz na stronach internetowych i mediach społecznościowych należących do jednostki – na podstawie zgody wyrażonej przez rodziców ucznia.

# Zasady przetwarzania danych w ramach monitoringu wizyjnego

1. Monitoring wizyjny obejmuje korytarze szkolne, bibliotekę, otoczenie zewnętrzne budynku, wejście do szkoły.
2. Monitoring nie obejmuje klas lekcyjnych, szatni, toalet oraz innych miejsc, gdzie mogłaby zostać naruszona intymność ucznia.
3. Wprowadzono procedurę regulującą kwestie bezpieczeństwa i zasady przetwarzania danych pochodzących z nagrań.
4. Nagrania te są udostępniane wyłącznie osobom, których dotyczą z zachowaniem poufności danych innych osób, które się na nim znalazły.

# Zasady przetwarzania wizerunku w celu promocji działań jednostki

* 1. Zgoda rodziców/opiekunów prawnych na wykorzystanie wizerunku ich dziecka jest tylko wtedy wiążąca, jeśli dzieci i rodzice/opiekunowie prawni zostali poinformowani o sposobie wykorzystania zdjęć/nagrań i ryzyku wiążącym się z publikacją wizerunku.
	2. Zgodę można wycofać w dowolnym momencie oraz a wraz z jej wycofaniem wnioskować o usunięcie danych przetwarzanych na jej podstawie.
	3. Zdjęcia i nagrania przetwarzane są do wycofania zgody na ich przetwarzanie.
	4. Materiały zawierające wizerunek są każdorazowo przed wykorzystaniem analizowane pod względem moralnym, etycznym oraz pod względem bezpieczeństwa, aby zapobiec udostępnianiu materiałów krzywdzących, ośmieszających lub zawierających dane, których ujawnienie stanowiłoby zagrożenie dla praw i wolności osoby, której dane dotyczą.
	5. W przypadku niewyrażenia zgody na przetwarzanie wizerunku dziecka osoba wykonująca zdjęcia lub film zostanie o tym poinformowana i zobowiązana do respektowania tej decyzji. Jej realizacja nie może być w żaden sposób wykluczająca dla ucznia.

# Bezpieczeństwo danych

1. Wszystkie dane przetwarzane przez jednostkę są na bieżąco analizowane pod względem ich niezbędności dla administratora.
2. Personel przechodzi regularne szkolenia z zasad ochrony danych osobowych.
3. Przeprowadzana jest analiza ryzyka oraz – w razie potrzeby – ocena skutków przetwarzania danych.
4. Zawarto umowy powierzenia przetwarzania danych aby zachować założone standardy bezpieczeństwa również w przypadku powierzania przetwarzania danych podmiotom zewnętrznym.
5. Stosowane są zabezpieczenia fizyczne, techniczne i organizacyjne dla obszarów, w których dane osobowe są przetwarzane.
6. Każde podejrzenie niewłaściwego wykorzystywania danych, naruszenia poufności, integralności lub dostępności danych są niezwłocznie zgłaszane dyrektorowi oraz poddawane analizie ryzyka przy wsparciu inspektora ochrony danych.