Polityka bezpieczeństwa internetowego
Państwowej Szkoły Muzycznej I i II stopnia
Im. Karola i Antoniego Szafranków w Rybniku

I. Postanowienia wstępne:

1. **„Polityka Bezpieczeństwa Internetowego”** jest zbiorem działań, które podejmuje szkoła w celu zapewnienia bezpieczeństwa uczniom podczas korzystania przez nich z nowych technologii informatycznych w szkole, jak i poza szkołą, oraz ma na celu zapobieganie cyberprzemocy wśród uczniów.
2. Jeżeli w dokumencie jest mowa o:
   a) *Administratorze bezpieczeństwa informacji* – rozumie się przez to osobę, której dyrektor szkoły powierzył opiekę nad infrastrukturą informatyczną działającą na terenie szkoły.
   b) *Infrastrukturze Informatycznej* – jest zbiorem urządzeń tj. komputerów wraz z oprogramowaniem, routerów, modemów oraz siecią zarówno wewnętrzną jak i ogólnodostępną dla użytkowników szkolnego wi-fi.
   c) *Systemie informatycznym* – rozumie się przez to zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych.
   d) *Szkole* – rozumie się przez to Państwową Szkołę I i II stopnia im. Karola i Antoniego Szafranków w Rybniku.
   e) *Użytkowniku* – rozumie się przez to uczniów, nauczycieli oraz rodziców i osoby postronne korzystające na terenie szkoły z dostępnej infrastruktury informatycznej.
   f) *Cyberprzemocy (agresji elektronicznej)* – rozumie się przez to stosowanie przemocy przez: prześladowanie, zastraszanie, nękanie, wyśmiewanie innych osób przy użyciu internetu oraz form komunikacji elektronicznej takiej jak SMS, fora dyskusyjne, media społecznościowe, strony internetowe, pojęcie cyberprzemocy obejmuje zarówno działania werbalne jak i niewerbalne (*graficzne, dźwiękowe*).
   g) *Szkole ogólnokształcącej* – rozumiemy przez to Szkołę podstawową bądź ponadpodstawową do której uczęszcza uczeń oprócz Państwowej Szkoły I i II stopnia im. Karola i Antoniego Szafranków w Rybniku.
3. „Polityka Bezpieczeństwa Internetowego” określa zbiór podejmowanych działań na terenie szkoły, których celem jest:
   a) Kształtowanie odpowiedzialnej i odpowiedniej społecznie postawy w zakresie korzystania z nowoczesnych technologii komunikacyjnych.

b) Poprawie świadomości oraz zwiększenia wrażliwości społeczności szkoły na temat zagrożeń jakie występują podczas korzystania ze współczesnych technologii informacyjnych.
c) Zadbanie o bezpieczeństwo uczniów podczas korzystania ze stanowisk komputerowych dostępnych na terenie szkoły.

II. **Zadania do realizacji**

Lp.	**Zadanie**	**Sposób realizacji**	**Odpowiedzialni**
1	Zapewnienie bezpieczeństwa uczniom podczas korzystania ze szkolnych stanowisk komputerowych oraz szkolnej infrastruktury informatycznej.	1. Instalacja oprogramowania uniemożliwiającego dostęp do niepożądanych treści i portali w szkolnym systemie informatycznym. 2. Wyposażenie stanowisk w oprogramowanie antywirusowe. 3. Zabezpieczenie ruchu infrastruktury informatycznej w celu wyeliminowania dostępności treści nieodpowiednich poprzez instalację filtrów.	Administrator bezpieczeństwa informacji
2	Edukacja uczniów oraz rodziców i opiekunów.	1. Zapoznanie uczniów i rodziców oraz opiekunów z zasadami bezpiecznego korzystania technologii informacyjnych: – ochrona danych osobowych, w tym regulacje prawne wynikające z Konstytucji RP oraz Ustawy o ochronie danych. – Cyberprzemoc jako przestępstwo przeciw prawu, rodzaje zachowań kwalifikowanych jako cyberprzemoc. – Ochrona własnego wizerunku i wizerunku innych osób. – Pojęcie pozornej anonimowości w sieci – Prawa autorskie i ich ochrona. – Co to jest kradzież własności intelektualnej i dzieł chronionych prawami autorskimi.	Kierownicy sekcji, Nauczyciele, Opiekun młodzieży

		– Na czym polega kradzież tożsamości. – Jakie zagrożenia można napotkać podczas korzystania z form komunikacji elektronicznej. – pojęcie „złośliwego oprogramowania” 2. Informowanie uczniów rodziców oraz opiekunów o sposobach radzenia sobie z przejawami cyberprzemocy, rozpoznawaniu oraz postępowaniu w przypadku jej wystąpienia. 3. Przygotowanie wytycznych mających na celu poprawę bezpieczeństwa uczniów podczas wystąpienia konieczności pracy zdalnej z użyciem technologii informacyjnych, które mogą mieć również zastosowanie w codziennym korzystaniu z nowych technologii.	
3	Reakcja na zjawisko Cyberprzemocy.	1. Podejmowanie interwencji w przypadkach ujawnienia lub podejrzenia cyberprzemocy, za porozumienie i we wsparciu szkoły ogólnokształcącej do której uczęszcza uczeń. 2. Przekazanie informacji uczniom oraz rodzicom o potrzebie poinformowania pedagoga lub wychowawcy w szkole ogólnokształcącej o zastosowaniu wobec ucznia cyberprzemocy.	Nauczyciel przedmiotu głównego w porozumieniu z dyrekcją szkoły.
4	Zadania dla Rady Pedagogicznej	1. Zapoznanie Rady pedagogicznej z Polityką Bezpieczeństwa Internetowego, w formie zdalnej bądź podczas zebrania. 2. Przedstawienie profilaktyki przeciwdziałaniu cyberprzemocy, bezpieczeństwa w sieci oraz sposobów bezpiecznej świadomej pracy zdalnej w sytuacji kiedy jest ona konieczna.	Dyrektor Nauczyciele

		3. Uświadomienie rodzicom potrzeby kontroli dostępu do internetu oraz innych nośników elektronicznych używanych przez uczniów.	Nauczyciele

III. **Postanowienia końcowe:**

1. Każdy pracownik szkoły jest zobowiązany do przestrzegania „Polityki Bezpieczeństwa Internetowego” Szkoły.
2. Niezastosowanie się do procedur wynikających z niniejszego dokumentu i naruszenie procedur bezpieczeństwa internetowego dla uczniów jest traktowane jako naruszenie obowiązków służbowych i może skutkować konsekwencjami prawnymi.

Data przedstawienia Radzie Pedagogicznej 26 marzec 2020 w trybie elektronicznym.

Romana Kuczera
Dyrektor szkoły

Opracował: mgr Paweł Szklarski