Załącznik nr 10

Zasady bezpiecznego korzystania z Internetu i mediów elektronicznych w Szkole Podstawowej im. Zofii Kossak w Pierśćcu.

1. Infrastruktura sieciowa szkoły umożliwia dostęp do Internetu zarówno personelowi jak i uczniom w czasie lekcji i zajęć pozalekcyjnych.
2. Sieć jest monitorowana tak, aby możliwe było zidentyfikowanie sprawców ewentualnych nadużyć.
3. Rozwiązania organizacyjne na terenie szkoły bazują na aktualnych standardach bezpieczeństwa.
4. Wyznaczona jest osoba odpowiedzialna za bezpieczeństwo sieci w szkole. Do jej obowiązków należą:
    a. zabezpieczenie sieci internetowej szkoły przed niebezpiecznymi treściami poprzez instalację i aktualizację odpowiedniego, nowoczesnego oprogramowania;
    b. aktualizowanie oprogramowania w miarę potrzeb, przynajmniej raz w miesiącu;
    c. przynajmniej raz w miesiącu sprawdzanie, czy na komputerach ze swobodnym dostępem podłączonym do Internetu, nie znajdują się niebezpieczne treści. W przypadku znalezienia niebezpiecznych treści, wyznaczony pracownik stara się ustalić, kto korzystał z komputera w czasie ich wprowadzania. Informację o dziecku, które korzystało z komputera w czasie wprowadzania niebezpiecznych treści, wyznaczony pracownik przekazuje dyrektorowi szkoły. Dyrektor organizuje dla dziecka rozmowę z pedagogiem na temat bezpieczeństwa w Internecie. Jeżeli w wyniku przeprowadzonej rozmowy pedagog uzyska informacje, że dziecko jest krzywdzone, podejmuje działania opisane w procedurze interwencji.
5. W szkole istnieje regulamin korzystania z Internetu przez uczniów.
6. W przypadku dostępu do Internetu realizowanego pod nadzorem pracownika szkoły, ma on obowiązek informowania dzieci o zasadach bezpiecznego korzystania z Internetu. Pracownik szkoły czuwa także nad bezpieczeństwem korzystania z Internetu przez dzieci podczas zajęć.
7. W miarę możliwości osoba odpowiedzialna za Internet przeprowadza z dziećmi cykliczne warsztaty dotyczące bezpiecznego korzystania z Internetu.
8. Szkoła zapewnia stały dostęp do materiałów edukacyjnych, dotyczących bezpiecznego korzystania z Internetu.

Regulamin korzystania z Internetu przez uczniów
Szkoły Podstawowej im. Zofii Kossak w Pierśćcu

1. Prawo do korzystania z komputerów znajdujących się w pracowniach informatycznych i bibliotekach przysługuje uczniom oraz nauczycielom. W wyjątkowych sytuacjach innym osobom, jeśli Dyrektor Szkoły wyrazi na to zgodę.
2. Prawo do korzystania z komputerów znajdujących się w poszczególnych salach lekcyjnych przysługuje nauczycielom. W wyjątkowych sytuacjach innym osobom, jeśli Dyrektor Szkoły wyrazi na to zgodę.
3. Korzystanie z komputerów (programów użytkowych i multimedialnych) jest bezpłatne.
4. Uczniowie korzystają z komputera tylko pod opieką nauczyciela.
5. Korzystanie z multimediów, Internetu i programów użytkowych służy wyłącznie celom naukowym, informacyjnym i edukacyjnym.
6. Uczeń może korzystać z Internetu tylko na komputerze z zainstalowanym programem filtrującym treści.
7. Uczeń obsługuje sprzęt komputerowy zgodnie z zaleceniami nauczyciela.
8. Po zakończeniu pracy użytkownik ma obowiązek zostawić komputer wyłączony, chyba że nauczyciel zadecyduje inaczej.
9. Użytkownicy komputera mają prawo do zapisywania swoich plików wyłącznie w wyznaczonym miejscu (nie na pulpicie). Dane tymczasowe, utworzone w trakcie pracy, należy po jej zakończeniu usunąć.
10.Użytkownikowi komputera zabrania się:
a) instalowania oprogramowania oraz dokonywania zmian w konfiguracji oprogramowania zainstalowanego w systemie,
b) usuwania cudzych plików, odinstalowania programów, dekompletowania sprzętu,
c) dotykania elementów z tyłu komputera, kabli zasilających, a także kabli sieciowych.

Zasady bezpiecznego korzystania z Internetu:

1. Należy zainstalować program antywirusowy.
2. Nie należy otwierać wiadomości od nieznanych osób.
3. Nie należy klikać w nieznane linki i załączniki w wiadomościach e-mail oraz pobierać plików z niesprawdzonych stron internetowych.
4. Nie należy podawać w sieci danych osobowych ani haseł, wysyłać swoich zdjęć oraz zdjęć rodziny lub znajomych.
5. Przed założeniem konta należy zapoznać się z regulaminem i sprawdzić, czy strona ma zabezpieczenie SSL.
6. Zakładając konto, należy posługiwać się Nickiem, a nie prawdziwym imieniem lub nazwiskiem.
7. Nie wolno naruszać godności i praw innych użytkowników Sieci oraz działać na szkodę innych użytkowników Internetu.
8. Należy szanować prawo własności zdjęć, materiałów, artykułów, itp. w Sieci. Każdorazowo należy podpisywać autora w/w i/lub adres strony internetowej lub skorzystać z narzędzi zawężania wyszukiwania w przeglądarce do takich materiałów, które są

udostępnione do modyfikacji i kopiowania.
9. Nie wolno przesyłać i udostępniać danych naruszających prawo, powszechnie uznanych za obsceniczne lub obraźliwe oraz oszczerstw i treści obrażającej uczucia innych.
10. Zabrania się uprawiania hazardu oraz prowadzenia działalności komercyjnej.
11. Należy zachować ostrożność w spotkaniach z osobami poznanymi w Sieci.
Należy pamiętać, że Cyberbulling – przemoc przy użyciu Internetu – to przestępstwo.

Utworzenia silnego hasła i jego stosowanie

1. Hasła powinny zawierać co najmniej 8 znaków, przy czym co najmniej 2 cyfry oraz dwa znaki specjalne. Hasło nie powinno składać się ze słów powszechnie używanych – są one najprostsze do złamania, nawet jeżeli dodamy do nich liczby lub znaki specjalne.
2. Należy unikać używania znaczących dat, nazw i imion.
3. Tworząc bezpieczne hasło, można korzystać zamiennie z cyfr i znaków specjalnych, np. HasłoDoWifi zamieniamy na H@sł0D0W!f! (zamiast „O" jest „zero").
4. Dobrym sposobem na stworzenie dobrego hasła jest wykorzystanie swojej ulubionej książki, wiersza, tekstu piosenki, itp. Wydające się na skomplikowane i dwunastoznakowe długie hasło OwtzjbSB jest tak naprawdę zapisem pierwszych liter „O większego trudno zucha, jak był Stefek Burczymucha". Tak stworzone hasło jest dużo bezpieczniejsze.
5. Przed podaniem hasła do konta internetowego zalecane jest upewnienie się co do wiarygodności strony WWW, ponieważ zdarzają się strony spreparowane w celu ich wyłudzenia.
6. Dla większego bezpieczeństwa zalecane jest zastosowanie uwierzytelniania dwuskładnikowego.
7. Należy unikać zapisywania haseł na karteczkach, w notatnikach czy innych źródłach, które mogą dostać się w niepowołane ręce lub są ogólnodostępne.
8. Nie należy podawać haseł osobom trzecim.
9. Po zakończonej pracy należy pamiętać, że zamknięcie przeglądarki nie zawsze powoduje wylogowanie się z usług. Przed odejściem od komputera koniecznie należy się wylogować.
10. W przypadku podejrzenia o pozyskanie naszego hasła przez osoby niepowołane, należy natychmiast je zmienić.

Netykieta poczty elektronicznej

1. Należy codziennie sprawdzać pocztę. Nikt nie lubi długo czekać na odpowiedź. Należy sprawić, by komunikacja przebiegała szybko i efektywnie. Jeżeli przez dłuższy czas nie będziemy mieli dostępu do maila, poinformujmy o tym.
2. Nie należy wysyłać dużych załączników, rozsyłać spamu ani łańcuszków szczęścia. Załączniki nie powinny mieć więcej niż 2 MB, aby nie zaśmiecać skrzynki odbiorcy.
Do przekazywania dużych plików lepiej wykorzystać chmurę lub serwisy hostingowe.
Całkowicie niedopuszczalne jest rozsyłanie łańcuszków szczęścia, spamu i nieprzeskanowanych plików, które mogą zawierać wirusy i inne złośliwe oprogramowanie.
3. Spam należy kasować bez czytania treści. Nie należy również otwierać załączników i uruchamiać linków z maili otrzymanych od nieznajomych, od nieznanych osób lub firm.

Powinno się stosować zasadę „Nieznane znaczy niebezpieczne”.
4. Pisząc wiadomość, należy zawsze wypełnić pole „temat” wiadomości. Temat powinien być związany z treścią wiadomości.
5. Maile należy wysyłać w formacie tekstowym, bez zbędnych udziwnień w postaci różnych czcionek, kolorów i wklejonych obrazków. Cytować należy tylko najważniejsze fragmenty wiadomości. Pozostałe (wraz ze stopką) można usunąć. Swoją stopkę należy ograniczyć maksymalnie do 3-4 linijek.
6. Przy wysyłaniu jednego emaila do większego grona odbiorców, należy skorzystać z pola BCC (lub UDW – Ukryty do Wiadomości). W końcu nie każdy chciałby, aby jego mail został ujawniony osobom trzecim.
7. Aby zasygnalizować humorystyczne intencje wypowiedzi, można używać „uśmiechów”, tzw. emotikonów, lecz nie należy ich nadużywać.
8. Należy unikać pisania całego tekstu dużymi literami. Po pierwsze jest to mniej czytelne, po drugie może to być odebrane jako krzyk.
9. Należy zwracać uwagę na słownictwo, którego używamy. Słowa i zwroty, które stosujemy, mogą nam się wydawać zupełnie naturalne, ale inni mogą odebrać je jako obraźliwe.
10. Listy powinny być zawsze podpisane prawdziwym nazwiskiem i imieniem ich autora.
11. Przed wysłaniem listu, należy się zastanowić, czy na pewno zawiera treść, którą chcemy przesłać.
12. Należy używać programu antywirusowego na swoim komputerze (aby minimalizować ryzyko przesłania wirusów innym osobom - na przykład w przesłanym załączniku).

Postępowanie w przypadku znalezienia niebezpiecznych treści w komputerze (komputerach) szkolnych.

1. Wyznaczony pracownik szkoły przynajmniej raz na trzy miesiące sprawdza, czy na komputerach z dostępem do Internetu nie znajdują się niebezpieczne treści.
2. W przypadku znalezienie niebezpiecznych treści wyznaczony pracownik niezwłocznie usuwa je i ustala, kto korzystał z komputera w czasie ich wprowadzania.
3. Informacje o dziecku, które korzystało z komputera w czasie wprowadzenia niebezpiecznych treści, wyznaczony pracownik szkoły przekazuje dyrektorowi, psychologowi, pedagogowi szkolnemu, wychowawcy klasy.
4. Pedagog lub psycholog przeprowadza z dzieckiem, o którym mowa w punktach poprzedzających, rozmowę na temat bezpieczeństwa w Internecie.
5. Jeżeli w wyniku rozmowy wychowawca lub pedagog uzyska informacje, że dziecko jest krzywdzone, podejmuje działania opisane w rozdziale II niniejszej *Polityki.*

Gdzie szukać pomocy?

1. Wszelkie zdarzenia związane z naruszeniem bezpieczeństwa cyfrowego w szkole należy zgłosić panu **Michałowi Gawlasowi.**
2. W Internecie istnieją różne zespoły i linie pomocowe w sprawach dotyczących bezpieczeństwa dzieci, również w zakresie bezpieczeństwa w Internecie; dostarczają wiedzy, wskazówek rozwiązania problemu oraz wsparcia psychologicznego.

1) Dla ofiar i świadków cyberprzemocy lub dla osób, które są zaniepokojone jakimś zdarzeniem związanym z bezpieczeństwem cyfrowym są telefony zaufania:
a) 800 12 12 12 - Dziecięcy Telefon Zaufania Rzecznika Praw Dziecka Telefon jest bezpłatny i czynny od poniedziałku do piątku w godzinach od 8.15 do 20.00 (połączenie bezpłatne).
b) 116 111 - Telefon Zaufania dla Dzieci i Młodzieży - www.116111.pl
Bezpłatny i anonimowy telefon dla dzieci i młodzieży prowadzony od 2008 roku przez Fundację Dajemy Dzieciom Siłę.
2) Dyżurnet.pl - to zespół ekspertów Naukowej i Akademickiej Sieci Komputerowej, działający jako punkt kontaktowy do zgłaszania nielegalnych treści w Internecie. Dyżurnet.pl przyjmuje anonimowe zgłoszenia za pomocą:
a) formularza internetowego: https://dyzurnet.pl/formularz/
b) pocztą elektroniczną: dyzurnet@dyzurnet.pl
c) telefonicznie: 801 615 005

Kary dla uczniów, którzy nie przestrzegają postanowień regulaminu

1. Wobec ucznia łamiącego regulamin bezpiecznego korzystania z Internetu mogą być zastosowane kary określone w § 47 Statutu Szkoły.
2. Uczniowi i jego rodzicom przysługuje prawo odwołania w formie pisemnej od kary wymierzonej zgodnie z procedurą opisaną w § 47 oraz § 48 Statutu Szkoły.

Postanowienia końcowe

1. Regulamin obowiązuje wszystkich uczniów korzystających z komputera zarówno podczas planowych zajęć lekcyjnych, jak i poza nimi.
2. W kwestiach niewymienionych w niniejszym regulaminie stosuje się przepisy Statutu Szkoły, wewnętrzne regulaminy pracowni oraz powszechnie obowiązujące przepisy prawa.