Zasady bezpiecznego korzystania z Internetu oraz mediów i urządzeń elektronicznych

Zasady korzystania z urządzeń elektronicznych i Internetu na terenie szkoły dla uczniów

1. Prawo do korzystania z komputerów i innych urządzeń elektronicznych znajdujących się na terenie szkoły przysługuje uczniom oraz nauczycielom. W wyjątkowych sytuacjach innym osobom, jeśli Dyrektor Szkoły wyrazi na to zgodę.
2. Prawo do korzystania z komputerów/laptopów znajdujących się w poszczególnych salach lekcyjnych przysługuje nauczycielom. W wyjątkowych sytuacjach innym osobom, jeśli Dyrektor Szkoły wyrazi na to zgodę.
3. Uczniowie korzystają z komputerów i innych urządzeń elektronicznych tylko pod opieką nauczyciela.
4. Zasady korzystania z telefonów komórkowych określa Statut Szkoły § 25 p.2.5
5. Korzystanie z komputerów i urządzeń elektronicznych oraz zainstalowanych na nich programów użytkowych, multimedialnych jest bezpłatne i służy wyłącznie celom naukowym, informacyjnym oraz edukacyjnym.
6. Uczeń może korzystać z Internetu tylko na urządzeniu, na którym są filtrowane treści (OSE).
7. Uczeń obsługuje szkolny sprzęt elektroniczny zgodnie z zaleceniami nauczyciela.
8. Po skończeniu pracy użytkownik ma obowiązek zostawić komputer/laptop/tablet wyłączony, chyba że nauczyciel zadecyduje inaczej.
9. Użytkownicy komputera/laptopa 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. Należy zrobić kopię zapasową ważnych dokumentów w miejscu innym niż oryginał, najlepiej wykorzystując do tego celu chmurę danych.
11. Użytkownikowi komputera/laptopa/tabletu zabrania się:
    1) Instalowania oprogramowania oraz dokonywania zmian w konfiguracji sieci oraz oprogramowania zainstalowanego w systemie,
    2) usuwania cudzych plików, odinstalowania programów, dekompletowania sprzętu,
    3) dotykania elementów z tyłu komputera, kabli zasilających, a także kabli sieciowych.

Zasady postępowania w sytuacjach awaryjnych stanowiących zagrożenie dla życia lub zdrowia uczniów

1. W razie wypadku (np. zapalenia się urządzenia) należy natychmiast odsunąć się od sprzętu i powiadomić nauczyciela. Nauczyciel w miarę możliwości powinien wyłączyć urządzenie stanowiące zagrożenie oraz sporządzić protokół wypadku.
2. W przypadku zauważenia iskrzenia, wydobywającego się z komputera dymu, wyczucia zapachu tlącej się izolacji lub spostrzeżenia innych objawów mogących spowodować pożar, uczeń natychmiast powiadomić nauczyciela, który powinien wyłączyć zasilanie główne.
3. W sytuacjach awaryjnych uczniowie powinni natychmiast przerwać wszystkie prace ze sprzętem elektronicznym, zachować spokój oraz ściśle wykonywać wszystkie polecenia nauczyciela.

Zasady bezpiecznego korzystania z Internetu:

1. Należy zainstalować oprogramowanie chroniące przed rozprzestrzenianiem się wirusów.
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 i mediów elektronicznych.
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 *Cyberbullying* – przemoc z użyciem urządzeń elektronicznych, najczęściej telefonu bądź komputera – to przestępstwo.

Polityka haseł i jej 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, ponieważ 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 załącznikówi 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 różnychczcionek, kolorów i wklejonych obrazków. Cytować należy tylko najważniejsze fragmentywiadomości. 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 polaBCC (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).

Netykieta grup dyskusyjnych

1. Nie należy zapominać, że po drugiej stronie też jest człowiek. Nie powinno się pisać tego,czego chciałoby się powiedzieć osobiście, prosto w oczy, w pokoju pełnym ludzi.
2. Przed zadaniem jakiegokolwiek pytania należy odszukać zbiór najczęściej zadawanych pytań (FAQ). Większość grup posiada taki zbiór pytań i odpowiedzi. Jeśli niczego takiego tam nie ma, należy sprawdzić, czy ktoś w ostatnim czasie nie zadał podobnego pytania.
3. Należy stosować się do reguł pisania obowiązujących w danej grupie, np. do zasad dotyczących znaków diakrytycznych – użytkownicy niektórych kanałów IRC nie życzą sobie używania polskich liter, natomiast na forach internetowych pisanie bez polskich znaków diakrytycznych bywa źle widziane; sprawy te regulowane są czasem przez lokalną netykietę lub FAQ.
4. Włączając się do grupy dyskusyjnej, należy przeczytać uważnie, co zostało powiedziane dotychczas, zanim wyśle się swoją pierwszą wypowiedź.
5. Nie należy pisać zbyt długich wiadomości, a swoim postom należy nadawać krótkie tytuły, które będą dobrze odzwierciedlały ich treść.
6. Należy się zastanowić, do kogo chce się skierować swoją wypowiedź i postarać się dotrzeć do ludzi, których może zainteresować to, co mamy do powiedzenia, a nie, koniecznie, dojak największej liczby odbiorców.
7. Należy zwracać się w kulturalny sposób do innych internautów i korzystać ze zwrotów grzecznościowych, np. „Ty”, „Ci”, „Tobie”.
8. Nie należy pisać dużymi literami. Wyglądają na KRZYK.
9. Odpowiedź należy kierować bezpośrednio do pytającego, a nie do wszystkich uczestników dyskusji. Pytający może później podsumować wszystkie odpowiedzi i podać je do wiadomości grupy. Zaoszczędzi to innym użytkownikom czytania wielu podobnychmaili.
10. Wypowiedź należy wysłać tylko raz.
11. Nie należy nagabywać osób (uparcie łączyć się z), które sobie tego nie życzą.
12. Nie należy zwracać innym uwagi na literówki i błędy językowe i samemu ich unikać.

13. Grupa dyskusyjna nie powinna być źródłem wiadomości przy odrabianiu lekcji. Powinnosię szukać tego typu informacji na własną rękę.
14. Grupa dyskusyjna nie służy do celów reklamowych.
15. Korzystając z grup dyskusyjnych nie należy floodować (wielokrotnie wysłać tą samąwiadomość lub wiele różnych wiadomości w bardzo krótkich odstępach czasu).

Netykieta dla prowadzącego bloga

1. Zakładając własnego bloga, należy pamiętać, aby kolorystyka była przyjemna dla oczu innych osób, powinno się unikać jaskrawych kolorów i nie przesadzać z gifami.
2. Na pierwszej stronie witryny nie warto umieszczać bardzo dużych plików. Spowodujeto długie ładowanie strony.
3. Należy szanować prywatność innych osób i nie opisywać kogoś lub umieszczać jegowizerunku bez jego wiedzy i zgody.
4. Nie powinno się powtarzać wielokrotnie tych samych wpisów lub wpisów mówiącycho tym samym, ale w inny sposób.
5. Nie wolno kopiować i wklejać cudzych tekstów bez podawania przypisu czy źródła.
6. Należy pamiętać o usuwaniu złośliwych komentarzy i spamu.

Gdzie szukać pomocy

1. Wszelkie zdarzenia związane z naruszeniem bezpieczeństwa cyfrowego w szkole należy zgłosić wychowawcy lub pedagogowi szkolnemu.
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). Jeśli ktoś zadzwoni tam w godzinach

nocnych i zostawi informację o sobie i swój numer - konsultanci oddzwonią do takiej osoby.

b) 116 111 - Telefon Zaufania dla Dzieci i Młodzieży - www.116111.pl Bezpłatna i anonimowy telefon dla dzieci i młodzieży prowadzony od 2008roku 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

3. Online można sprawdzić również chronić użytkowników poczty elektronicznej i ułatwić instytucjom sprawdzenie poprawności konfiguracji mechanizmów zapewniających jej bezpieczeństwo. Służy do tego strona https://bezpiecznapoczta.cert.pl/
4. W celu ochrony poufnych danych osobowych za pomocą SMS'ów należy skorzystać ze strony https://cert.pl/baza-wiedzy/falszywe-smsy/ lub przesłać informację o potencjalnym zagrożeniu wiadomością SMS na numer 8080
5. Zgłaszanie incydentów dotyczących szeroko rozumianego cyberbezpieczeństwa można przesyłać za pomocą strony: https://incydent.cert.pl/#!/lang=pl

Kary dla uczniów, którzy nie przestrzegają postanowień regulaminu

1. Wobec ucznia łamiącego regulamin bezpiecznego korzystania z Internetu mogą byćzastosowane kary określone w § 29 p.2 Statutu szkoły.
2. Uczniowi i jego rodzicom przysługuje prawo odwołania w formie pisemnej od karywymierzonej zgodnie z procedurą opisaną w §29 p.6 Statutu szkoły.

Postanowienia końcowe

1. Regulamin obowiązuje wszystkich uczniów korzystających z komputera zarówno podczasplanowych 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.