„Bezpieczne i efektywne korzystanie z technologii informacyjnej”

Internet to nowoczesne medium, które odgrywa ogromną rolę w życiu młodego człowieka i może być przez niego z pożytkiem wykorzystywane. **Codzienne aktywności młodych internautów toczą się równolegle online i offline.** Rozwijanie zainteresowań, rozmowy z rówieśnikami czy odrabianie lekcji to czynności, które z dużą chęcią i swobodą realizowane są w sieci. Pozytywne aspekty technologii informacyjno-komunikacyjnych (TIK) doceniają także dyrektorzy, wyposażając swoje placówki w urządzenia cyfrowe (laptopy i tablety z dostępem do Internetu, rzutniki, tablice interaktywne). W niniejszym szkoleniu przedstawiamy, **dlaczego warto wykorzystywać nowoczesne narzędzia informatyczne w procesie nauczania,** a także pokazujemy, w jaki sposób uczniowie mogą skutecznie i bezpiecznie wyszukiwać w sieci potrzebne informacje. Prezentujemy również definicje pozytywnych treści online oraz kryteria dla stron internetowych, których znajomość pozwoli Państwu polecać dzieciom i ich rodzicom odpowiednie serwisy edukacyjne, a w przypadku młodzieży - ułatwiać tworzenie własnych, bezpiecznych treści w sieci.

Jednak nie można zapominać, że globalna sieć oprócz pozytywnych treści kryje też wiele niebezpieczeństw. **Ważne jest, by nauczyciele kształtowali świadomość uczniów o zagrożeniach internetowych,** a w przypadku zaistnienia niebezpieczeństwa potrafili wskazać im właściwe rozwiązanie. W publikacji tej szczegółowo omawiamy różne formy cyberprzemocy, przedstawiamy ryzykowne zachowania online podejmowane przez nastolatków, a także radzimy, jak postępować w sytuacji uzależnienia od Internetu. Ze względu na wagę tych problemów rekomendujemy szkołom przygotowanie oficjalnych procedur w przypadku cyberprzemocy, nadmiernego korzystania z Internetu oraz reagowania w sytuacji naruszenia bezpieczeństwa infrastruktury szkolnej sieci, które powinny przybrać formę zarządzenia dyrektora lub uchwały rady pedagogicznej. W przypadku procedur dotyczących cyberprzemocy oraz nadmiernego korzystania z Internetu zalecamy przeprowadzenie konsultacji z radą rodziców. Wypracowane procedury powinny być dobrze znane całemu środowisku szkolnemu. W poradniku omawiamy również symptomy nadużywania Internetu oraz wskazujemy punkty kontaktowe udzielające wsparcia i informacji w zakresie trudności będących konsekwencjami ryzykownych zachowań w sieci.

W dzisiejszych czasach nikt już nie ma wątpliwości, że **nowoczesne media, które na dobre zagościły w życiu prywatnym oraz zawodowym, muszą także stanowić integralną część współczesnego szkolnictwa.** Edukacja **medialna** powinna obejmować efektywne, kreatywne i bezpiecznie korzystanie z zasobów Internetu, a sama sieć stać się narzędziem będącym podporą dla nauczania wszelkiego rodzaju przedmiotów szkolnych.

Wprowadzenie Internetu do codziennego życia szkoły zwiększy atrakcyjność i unowocześni zajęcia edukacyjne, ułatwi komunikację pomiędzy kadrą nauczycielską a uczniami i rodzicami, pomoże w prowadzeniu projektów, otworzy szerzej na współpracę międzynarodową oraz zapewni dostęp do nieograniczonych zasobów globalnej sieci. Wykorzystywanie nowych technologii, czyli nowoczesnych narzędzi informatycznych w szkolnictwie takich jak: internetowe platformy edukacyjne, tablice multimedialne, e-podręczniki, narzędzia deweloperskie służące budowaniu stron lub tworzeniu aplikacji itp., może mieć **duży wpływ na rozwijanie u uczniów zdolności twórczych.** Podkreślając też

możliwość kreowania zasobów sieciowych, pokazujemy uczniom, że niekoniecznie trzeba być tylko biernym odbiorcą.

Sieć może być również idealnym narzędziem do komunikacji szkolnej między rówieśnikami, nauczycielami i rodzicami. Dzięki telefonom komórkowym i internetowi komunikacja między domem rodzinnym dziecka i szkołą oraz innymi osobami i instytucjami odpowiedzialnymi za edukację z pewnością stała się wygodniejsza i szybsza.

Dlaczego warto korzystać z TIK w szkole:

a) Wspierają nauczanie kompetencji cyfrowych
b) Usprawniają wymianę informacji (np.: dzięki narzędziu Moodle)
c) Umożliwiają organizację zdalnych lekcji oraz wydarzeń edukacyjnych, takich jak np.: Webinaria - czyli tematyczne seminaria online
d) Dają szybki i nieograniczony dostęp do zasobów sieci oraz multimedialnych narzędzi, które nie tylko przybliżą treści, ale również wpierają nauczanie przedmiotów ścisłych oraz nauk przyrodniczych poprzez możliwość zdalnego przeprowadzania eksperymentów edukacyjnych

Korzystanie z TIK jest coraz łatwiejsze dzięki coraz liczniejszym, łatwo dostępnym narzędziom i poradom m.in. na stronach:

www.ore.edu.pl

www.ceo.org.pl

www.fabrykaprzyszlosci.pl

www.edutikacja.oeiizk.waw.pl

www.superbelfrzy.edu.pl

www.edukator.pl

www.etwinning.pl

Na podstawie kilkuletnich badań nad stronami internetowymi adekwatnymi dla dzieci i młodzieży (badania prowadzone przez 20 instytucji z 15 państw Unii Europejskiej w ramach projektu POSCON) określone zostały **definicje pozytywnych treści online,** które mogą być wskazówką zarówno dla producentów treści online, jak i dla nauczycieli, którzy na poniższych wytycznych mogą bazować, polecając odpowiednie serwisy dzieciom i ich rodzicom lub chcących angażować młodzież w samodzielne kreowanie treści internetowych.

Szczegółowe kryteria dotyczące serwisów online, którymi nauczyciel może się, kierować wybierając treści internetowe do celów edukacyjnych oraz polecając serwisy interaktywne dzieciom i ich opiekunom:

a) Odbiorcy treści muszą być jasno określeni i treści właściwie adresowane (język i zawartość dopasowane do rozwoju intelektualnego i emocjonalnego danej grupy wiekowej)
b) Zawartość strony/serwisu, czy też proponowane na stronie usługi muszą być atrakcyjne, użyteczne, rzetelne i niezawodne (np.: znamy autora treści, dane kontaktowe twórców strony, bądź administratora są łatwo dostępne, treści są prawdziwe, sprawdzone

merytorycznie, zawartość strony nie narusza cudzych praw autorskich. Zawartość strony/serwisu, czy też proponowane na stronie usługi muszą być bezpieczne (nie zawierać treści szkodliwych bądź nielegalnych, posiadać łatwy adres - dziecko nie pomyli się i nie trafi na inną stronę)

c) Prywatność dziecka musi być właściwie zapewniona i chroniona (trzeba zwrócić uwagę, jakie dane dziecko musi podać przy rejestrowaniu się i jak te dane są chronione, czy serwis np.: nie zawiera usługi geolokalizacji umożliwiającej szybkie określenie miejsca przebywania dziecka, dla kogo dostępne są dane publikowane przez dziecko np. w portalach społecznościowych. Dobrą procedurą jest również konieczność wyrażenia zezwolenia przez rodziców/opiekunów prawnych na zalogowanie się dziecka do serwisu)
d) Portale społecznościowe muszą posiadać odpowiednie instrukcje dla użytkownika, np.: ułatwiać chroniące użytkownika ustawienie prywatności, być stale moderowane, dawać łatwą możliwość zgłoszenia naruszenia oraz zawierać informacje, jak uchronić się przed cyberprzemocą, bądź gdzie zgłaszać jej przypadki, zaś w przypadku dzieci wymagać podczas rejestracji akceptacji rodzica/opiekuna w momencie logowania się
e) W przypadku stron komercyjnych wymagane jest, by nie mieszać treści z reklamami. Mieć limity zakupowe dla dzieci, metody płatności wymagające akceptacji rodzica, a reklamy niezakłócające korzystania ze strony i właściwie opisane. Na stronach dla dzieci nie powinny pojawiać się reklamy używek.

Zjawisko cyberprzemocy związane jest z istniejącą od zawsze przemocą, w tym przypadku najczęściej rówieśniczą. Nowe technologie dostarczyły kolejnych kanałów zastosowania przewagi fizycznej czy psychicznej. W języku polskim funkcjonuje wiele określeń dotyczących tego zjawiska: cyberdręczenie (*cyberstalking*), agresja elektroniczna, nękanie internetowe, prześladowanie w sieci (*cyberharassment*), mobbing elektroniczny (*cyberbullying*). Od tradycyjnie pojmowanej przemocy, czy to fizycznej czy też psychicznej, cyberprzemoc różni się możliwą skalą skrzywdzenia oraz długością trwania opresji, jakiej podlega dziecko. I w ten właśnie sposób definiuje się cyberprzemoc - jako długotrwałe zjawisko mogące przybrać formę nękania, straszenia, wyzywania czy też poniżania kogoś przy użyciu nowych technologii.

Internet to przestrzeń, w której dla młodych ludzi obecność jest obowiązkowa. Relacje społeczne młodzieży toczą się równolegle w świecie realnym i wirtualnym - dla nich to jedna rzeczywistość. Odrzucenie z grona osób należących do danej grupy, wykluczenie, niezauważanie bądź celowe ignorowanie również może być formą cyberprzemocy. Specyfika sieci powoduje, że dziecko może doświadczać cyberprzemocy stale i - z uwagi na wszechobecny dostęp do Internetu - bez względu na miejsce, w jakim się znajduje.

Problem przemocy przy użyciu nowych technologii może dotknąć każdego, także pracownika szkoły: dyrektora, nauczyciela czy wychowawcę. Warto, żeby szkoła miała wypracowany schemat postępowania również i w takim przypadku. Fałszywe profile, modyfikacje fotografii i informacji tekstowych lub dźwiękowych, zamieszczanych na portalach społecznościowych lub uporczywe nękanie smsami spotkać mogą każdego.

Wiemy w jakiej skali zjawisko to występuje wśród młodzieży , natomiast naiwnością ze strony dorosłych byłoby myślenie, że przypadki tego typu nie zdarzają się również wśród młodszych dzieci. **Dlatego szkoła powinna przeprowadzać lekcje na temat cyberprzemocy na każdym etapie nauki,** żeby każdy z uczniów wiedział, co powinien zrobić w przypadku, kiedy dotknie go cyberprzemoc lub kiedy będzie jej świadkiem. Jasne i

proste procedury, ujęte w dokumentacji szkolnej, pomogą zapobiegać temu zjawisku i zminimalizować jego niepożądane skutki.

Na koniec warto wspomnieć o nowym zjawisku - „wychowywaniu" przez publiczne poniżanie w sieci *(public shaming),* rodem ze średniowiecznego pręgierza. Takie ośmieszenie, poniżenie w formie zamieszczonego w Internecie zdjęcia lub filmu, na którym dziecko publicznie kaja się, przeprasza lub trzyma kartkę z opisaną swoją przewiną stało się nową formą cyberprzemocy, stosowaną przez rodziców lub inne dorosłe osoby bliskie.

Najważniejsza zasada, jaką powinni kierować się dorośli, publikując w sieci informacje o dziecku (zdjęcia, wpisy) to uszanowanie jego godności i podmiotowości.

Do treści szkodliwych, z którymi najmłodsi nie powinni mieć styczności, zalicza się:

a) treści związane z prezentowaniem przemocy (m.in. cyberprzemoc, wulgaryzmy, bójki i „ustawki",okrucieństwo wobec zwierząt)
b) treści nawołujące do przemocy (m.in. treści rasistowskie i ksenofobiczne)
c) treści prezentujące niebezpieczne zachowania (m.in. wyścigi samochodowe, zwiedzanie niebezpiecznych miejsc, jak budowy i ruiny, uprawianie sportów ekstremalnych bez asekuracji i zabezpieczeń)
d) treści promujące zachowania autodestrukcyjne (m.in. treści nawołujące do samookaleczeń, samobójstw, restrykcyjnej diety, zażywania substancji psychoaktywnych)
e) treści prezentujące niewłaściwy obraz rzeczywistości (m.in. treści dyskryminujące, spiskowe, pornograficzne)
f) treści makabryczne (m.in. treści przedstawiające ofiary wojny lub wypadków, przypadki medyczne, bestialstwo wobec zwierząt).

Wymienione powyżej treści nie powinny znajdować się w szerokim, publicznym dostępie. Niestety przepisy prawne (nie tylko polskie) nie zawsze regulują kwestie związane z publikowaniem tego typu materiałów. Często założenie ostrzeżenia, które może pomóc w filtrowaniu treści, zależy od dobrej woli właściciela serwisu oraz od zasad moderacji. Niektóre strony internetowe nie akceptują treści szkodliwych (w części lub w całości), ale ich publikowanie zależy od szybkości i jakości moderacji. Niejednokrotnie treści szkodliwe są publikowane w komentarzach.

Kontakt z niebezpiecznymi treściami może prowadzić do wykrzywienia obrazu rzeczywistości oraz wzbudzić u młodego człowieka poczucie zagrożenia i lęku, a także spowodować różnego rodzaju zaburzenia jego rozwoju.

Odbiorowi każdej informacji w Internecie powinno towarzyszyć ograniczone zaufanie i krytyczne podejście do danego źródła wiedzy.

Ze względu na specyfikę współczesnych mediów, którym zależy na krótkim czasie publikowania informacji, nawet największe serwisy medialne nie są w stanie uchronić się od przedstawiania nieprawdziwej i niesprawdzonej wiadomości.

Nauczyciele powinni wytłumaczyć uczniom, że czytając, a przede wszystkim cytując informację, powinni zwrócić baczną uwagę na to, kto ją publikował. Analizując zalety i

wady danego produktu przed jego zakupem, należy sprawdzić kto jest twórcą opinii. Z pewnością bardziej wiarygodnym źródłem będzie niezależny raport wykonany przez ośrodek konsumenta (niezależnego badacza), niż informacje przedstawiane na stronie internetowej producenta. Należy podkreślić, że firmy promujące produkty lub usługi w kampaniach marketingowych wykorzystują fora internetowe do kształtowania opinii użytkowników. Pracownicy firmy lub osoby specjalnie w tym celu wynajęte prowadzą anonimowy tzw. „marketing szeptany" podszywając się pod zwykłych użytkowników. Dlatego bardzo trudno mieć pewność, że dana opinia jest obiektywna.

Omawiając z młodymi użytkownikami Internetu kwestię podejścia do informacji publikowanych w sieci, radzimy przyjrzeć się, jak prowadzona jest najpopularniejsza encyklopedia internetowa - Wikipedia. Należy zwrócić uwagę uczniów na historię hasła, które ulegało zmianie, było edytowane przez wiele, często anonimowych osób, bądź nie jest weryfikowane przez ekspertów. Zgodnie z filozofią Wikipedii, encyklopedia tworzona jest wspólnym wysiłkiem internetowej społeczności, dlatego często rozwija się nierównomiernie i pewne dziedziny lub hasła są znacznie bardziej rozbudowane niż pozostałe.

Zgodnie z art. 23.2. ustawy o prawie autorskim i prawach pokrewnych zakres własnego użytku osobistego obejmuje korzystanie z pojedynczych egzemplarzy utworów przez osoby pozostające w związku osobistym, na przykład pokrewieństwa, powinowactwa lub stosunku towarzyskiego. Zapis ten miał urealnić prawo do kopiowania na przykład pojedynczych, pożyczonych płyt. Jednak dzisiaj nie oddaje on rzeczywistości, ponieważ często dzieci i młodzież, aktywne na portalach społecznościowych, mają po kilkuset znajomych, są członkami wielotysięcznych grup tematycznych, a to, w gronie „znajomych", umożliwia dystrybucję materiałów na ogromną, nieograniczoną wręcz skalę.

Główną drogą zmierzającą do poprawy poszanowania praw autorskich przez młodych użytkowników sieci są kompleksowe akcje uświadamiające. Podczas zajęć w szkole poświęconych tematowi poszanowania cudzej twórczości należy zapoznawać uczniów z zapisania prawa autorskiego uświadamiać konsekwencje karne związane z tego rodzaju wykroczeniami oraz uwrażliwiać też na straty jakie ponoszą twórcy.

W kontekście szkół niezwykle istotne jest, aby rodzice zdali sobie sprawę z powagi sytuacji związanej z kopiowaniem, przepisywaniem oraz nielegalnym ściąganiem plików. Dorośli powinni mieć świadomość, jak istotne jest, aby młodzi ludzie uczyli się indywidualnej pracy oraz, że pozorna oszczędność w budżecie domowym związana ze ściąganiem nielegalnych plików jest obarczona odpowiedzialnością karną.

Placówki szkolne, coraz lepiej wyposażone w infrastrukturę sieciową i aplikacyjną, podlegają w tym samym stopniu co inne instytucje i przedsiębiorstwa typowym zagrożeniom w cyberprzestrzeni. Jednocześnie pełnią one ważną misję edukacyjną w stosunku do dzieci i młodzieży w zakresie bezpiecznego korzystania z Internetu, zatem powinny być chronione.

Kadra placówki szkolnej powinna zatem zadbać, aby infrastruktura TIK spełniała standardy bezpieczeństwa, a korzystanie z niej odbywało się Zgodnie z opracowanymi w placówce regulaminami.

Zasady bezpiecznego zachowania w sieci:

NALEŻY

a) regularnie zmieniać hasła do urządzeń, aplikacji i serwisów internetowych; hasła powinny być odpowiednio długie i zawierać małe, duże litery, cyfry oraz znaki specjalnie
b) jeśli to możliwe używać haseł dwuskładnikowych (np. urządzenia generujące hasła jednorazowe czy sms w telefonie)
c) korzystać z szyfrowanych połączeń z witrynami internetowymi (zamknięta kłódeczka w pasku adresowym przeglądarki), szczególnie przy podawaniu wrażliwych danych - można sprawdzić dane witryny po kliknięciu w kłódeczkę
d) zwracać uwagę na zagrożenia nie tylko przy korzystaniu z poczty elektronicznej czy surfowaniu po stronach WWW - wirusy czy phishing zdarza się także na portalach społecznościowych czy internetowych grach komputerowych.
e) czytać regulaminy usług internetowych, z których korzystamy
   mieć włączone systemy antywirusowe czy filtrujące oraz zapory sieciowe, które pomogą nam dbać o bezpieczeństwo.
   NIE NALEŻY
   a) otwierać załączników e-maili oraz klikać na adresy internetowe (linki) zawarte w e-mailach pochodzących z nieznanych źródeł - załączniki mogą zawierać szkodliwe programy a linki prowadzić do zarażonych stron internetowych
   b) podawać identyfikatorów lub haseł na nie zaufanych stronach internetowych dokonywać ważnych operacji w internecie poprzez publiczne, otwarte sieci WiFi
   c) ściągać na urządzenia mobilne aplikacji, które nie pochodzą z oficjalnych sklepów - np. Google, Apple, ponieważ mogą mieć ukryte funkcje narażające nasze bezpieczeństwo lub prywatność.

   Jeśli zdarzy się incydent, ważna jest odpowiednia reakcja!
   Jeśli komputer przestaje sprawnie działać, na przykład jest wolny, zawiesza się, nie zawsze oznacza to awarię - należy sprawdzić czy nie jest zawirusowany, czy ma działający program antywirusowy lub jaka jest data ostatniej aktualizacji. Należy również przeskanować programem antywirusowym całą zawartość urządzenia
   Jeśli placówka szkolna padnie ofiarą oszustw w Internecie, należy zgłosić przestępstwo na Policję. Wówczas urządzenie komputerowe (jego zawartość) jest dowodem w sprawie i powinno być zabezpieczone do ewentualnej analizy.