Informacje dla nauczycieli, uczniów i rodziców o kształceniu na odległość w szkole, z uwzględnieniem higieny pracy uczniów i nauczycieli oraz zasad bezpieczeństwa w sieci.

W kształceniu na odległość proces nauczania jest pobudzany i kierowany przez nauczyciela w sposób pośredni i ciągły za pomocą różnych mediów pozwalających pokonać dystans. Mediami nauczania mogą być: telefon, laptop, tablet, komputer stacjonarny tj. środki pośredniczące w procesie komunikowania prezentujące treści nauczania.

Nie każde medium nadaje się w jednakowy sposób do pełnienia określonej funkcji kształceniowej w danym procesie nauczania, należy więc dokonać wyboru odpowiedniego do danej sytuacji edukacyjnej środka przekazu z uwagi na wiek odbiorcy lub prezentowane treści. W nauczaniu na odległość musimy brać pod uwagę umiejętności informatyczne nauczycieli ale głównie zdolności percepcyjne uczniów i posiadane przez nich media.

Wymagany sprzęt i narzędzia

Kształcenie na odległość to komunikowanie się za pomocą podstawowych usług Internetu takich jak poczta elektroniczna, lista dyskusyjna, chatt room, FTP (Serwer FTP, zależnie od konfiguracji, może pozwalać na anonimowy, czyli bez podawania hasła uwierzytelniającego, dostęp do jego zasobów. Najczęściej jednak serwer FTP autoryzuje każde połączenie za pomocą loginu i hasła) strony WWW, aplikacje, i inne.

Nauczyciel przygotowuje materiały dydaktyczne, które umieszcza w sieci lub przesyła bezpośrednio swoim uczniom.

Przez sieć:

- daje im wskazówki,
- przekazuje instrukcje,
- kieruje procesem kształcenia, stwarzając warunki do pracy indywidualnej, grupowej i zespołowej.
- Uczniowie komunikują się z nauczycielem lub wchodzą w interakcje z grupą i materiałem kształcenia.

Komunikowanie się przez Internet może przebiegać w dwóch trybach: synchronicznym– komunikowanie w czasie rzeczywistym (on-line) oraz z przesunięciem w czasie, czyli trybie asynchronicznym.

W trybie asynchronicznym wysyłanie komunikatów następuje w różnym czasie. Uczniom daje to możliwość przemyślenia problematyki zajęć i przygotowania odpowiedzi. Asynchroniczny tryb komunikowania jest najlepszy do wszelkiego rodzaju ćwiczeń utrwalających.

W indywidualnych kontaktach nauczyciela i ucznia najlepiej sprawdza się ***poczta elektroniczna,*** daje ona możliwość dostosowania komunikatów do poziomu ucznia zarówno zdolnego, jaki i słabego.

Na równoczesne przesyłanie wiadomości między członkami grupy pozwala ***lista dyskusyjna*****.** Dzięki niej uczniowie porozumiewają się między sobą, a nauczyciel z całą klasą. Mogą wymieniać się doświadczeniami, pomysłami w rozwiązywaniu problemów. Korzystać

z pomocy, gdy napotkają na trudności. Zaktywizowani uczniowie wspólnie dochodzą do właściwych rozwiązań w ten sposób utożsamiają się z grupą.

Dzięki ***usłudze FTP*** uczniowie mogą pobierać materiały dydaktyczne z serwera, na którym zostały umieszczone przez nauczyciela i umieszczać tam swoje prace. Usługa ta pozwala również na ściągnięcie programów komputerowych w celu wykorzystania ich do realizacji zadań.

W kształceniu zdalnym ***strony WWW*** zawierają treści kształcenia, dlatego służą jako podręcznik. Mogą być również wykorzystywane jako tablica informacyjna, na której nauczyciel umieszcza ogłoszenia odnośnie organizacji zajęć. Inne zastosowanie *edukacyjne stron WWW* w kształceniu zdalnym to ***interaktywne bazy danych***. Polega to na tym, że uczniowie zbierają informacje potrzebne do realizacji postawionego zadania i umieszczają je w odpowiednich rekordach przygotowanych przez instruktora bazy danych. Zgromadzony materiał poddawany jest dyskusji przez dopisywanie refleksji i opinii w specjalnie przygotowanych do tego polach.

WebQuest – rodzaj metody projektów zorientowanej na uczniowskie badania w oparciu o instrukcję umieszczoną na stronie internetowej. Celem WebQuestu jest rozwinięcie u uczniów umiejętności problemowego, krytycznego i twórczego myślenia oraz współpracy w zespole. Projekt w oparciu o pracę z komputerem determinuje aktywne działanie, pozwalając porzucić postawę biernego odbiorcy.

WebQuest wykorzystuje zainteresowanie uczniów komputerem i Internetem, pozwala skierować je w odpowiednim kierunku i wykorzystać w procesie nauczania. Uczy przemyślanego i konstruktywnego korzystania z zasobów Internetu. Pokazuje, że wirtualna sieć może być narzędziem pracy, a nie wyłącznie rozrywki. Odpowiednio dobrany przez nauczyciela materiał źródłowy pozwala uczniom bardziej skupić się na krytycznej analizie i użyciu informacji niż na ich szukaniu w przepastnym Internecie. WebQuest może być realizowany jako ćwiczenie grupowe, w którym każda grupa realizuje inną część projektu, wykonując inne zadania. Podział na grupy ma funkcję motywującą, gdyż wiąże się zazwyczaj z wcieleniem w jakąś rolę. Pobudza to zainteresowanie uczniów danym zagadnieniem. Produktem finalnym może być plakat, praca pisemna, prezentacja multimedialna, wystąpienie publiczne itp.

Struktura WebQuestu zawiera następujące części (podstrony):

1. Wprowadzenie – ogólny, motywujący opis projektu,
2. Zadanie – polecenia dla poszczególnych grup, opis produktu, który należy stworzyć,
3. Proces – opis kroków, jakie należy wykonać, aby rozwiązać zadania,
4. Źródła (zasoby) – lista linków do zasobów dostępnych w sieci, potrzebnych do rozwiązania poszczególnych zadań,
5. Ewaluacja (kryteria ocen) – punktacja i sposób oceny wykonania zadań,
6. Konkluzja (podsumowanie) – podsumowanie projektu, czasem zawierające prezentację gotowych materiałów będących efektem pracy uczniów.

Komunikacja w trybie synchronicznym wymaga jedności czasu, przy zachowaniu dystansu fizycznego osób komunikujących się. Synchroniczny sposób komunikowania wymaga ustalenia czasu i miejsca spotkania w sieci. Miejscem tym jest najczęściej ***chat room*****.** Wykorzystywany jest, kiedy przy rozwiązaniu problemu ważna jest natychmiastowa odpowiedź. Od

uczestników, chatu wymagana jest koncentracja umysłowa i wewnętrzna dyscyplina oraz biegłość w obsłudze klawiatury. Ważne jest, aby wszyscy uczestnicy mieli możliwość dyskusji i nie byli ignorowani przez innych. Synchroniczny sposób komunikowania w kształceniu zdalnym przypomina dyskusję stosowaną w nauczaniu tradycyjnym.

Problemy w edukacji zdalnejIzolacja osoby uczącej się od nauczyciela i innych członków grupy.

Brak komfortu psychicznego w sytuacji braku umiejętności informatycznych. Wymogi posiadania umiejętności samodzielnego uczenia się. Konieczność wykazania przez uczącą się osobę wysokiego stopnia samodyscypliny.

Zasady bezpiecznej pracy przy komputerze

Bezpieczeństwo i higiena pracy przy komputerze, ekranie telefonu itp. pozwala zniwelować skutki wpatrywania się w monitor przez kilka godzin, co może bardzo obciążać wzrok. W przypadku siedzącej pracy przed komputerem ważny jest odpowiedni dobór mebli. Kluczowe jest, aby krzesło miało regulowaną wysokość, fotel biurowy powinien mieć także regulowane odchylenie oparcia. Odległość twarzy od monitora powinna wynosić około 40-70 cm.

Jeśli trudno jest się oderwać od komputera można pobrać darmową aplikacje dostępną w sieci np. Anti-EyeStatin lub EyeCareReminder, które pomagają zaplanować czas spędzony przed monitorem, przypomną o przerwie i zaproponują ćwiczenie oczu.

Podstawowe zasady użytkowania komputera, telefonu, tabletu, itp.

Należy:

- Przed przystąpieniem do pracy rozgrzać nadgarstki, palce, przedramiona,
- W pozycji siedzącej zachować naturalne krzywizny kręgosłupa i nie garbić się,
- Podpierać plecy w okolicy lędźwiowej,
- Opierać przedramiona na podłokietnikach,
- Pamiętać o tym, ze górna krawędź monitora znajdowała się na wysokości oczu lub niżej,
- Co godzinę przerywać pracę lub zabawę i odpocząć – wykonać ćwiczenia relaksacyjne lub chociaż zmienić pozycję ciała,
- Wietrzyć pomieszczenia,
- Stosować ćwiczenia relaksacyjne oczu,
- Używać okularów korekcyjnych jeśli mamy wady wzroku,

Nie należy:

- Używać sprzętu elektronicznego w skręcie tułowia,
- Ściskać kurczowo myszki, telefonu,
- Uderzać mocno w klawisze,
- Spędzać długiego czasu używając sprzętu elektronicznego.

Zasady bezpieczeństwa w sieci

Zrozumienie zagrożeń cyberbezpieczeństwa i stosowanie skutecznych sposobów zabezpieczania się przed tymi zagrożeniami to wiedza niezbędna każdemu użytkownikowi komputera, smartphona czy też usług internetowych.

Do najpopularniejszych zagrożeń w cyberprzestrzeni, z którymi mogą się Państwo spotkać, należą:

- ataki z użyciem szkodliwego oprogramowania (*malware*, wirusy, robaki, itp.),
- kradzieże tożsamości,
- kradzieże (wyłudzenia), modyfikacje bądź niszczenie danych,
- blokowanie dostępu do usług,
- spam (niechciane lub niepotrzebne wiadomości elektroniczne),
- ataki socjotechniczne (np. *phishing*, czyli wyłudzanie poufnych informacji przez podszywanie się pod godną zaufania osobę lub instytucję).

Sposoby zabezpieczenia się przed zagrożeniami:

- Zainstaluj i używaj oprogramowania antywirusowego i spyware. Najlepiej stosuj ochronę w czasie rzeczywistym.
- Aktualizuj oprogramowanie oraz bazy danych wirusów (dowiedz się czy twój program do ochrony przed wirusami posiada taką funkcję i robi to automatycznie).
- Nie otwieraj plików nieznanego pochodzenia.
- Nie korzystaj ze stron banków, poczty elektronicznej czy portali społecznościowych, które nie mają ważnego certyfikatu, posiadają połączenie szyfrowane, chyba że masz stuprocentową pewność z innego źródła, że strona taka jest bezpieczna.
- Nie używaj niesprawdzonych programów zabezpieczających czy też do publikowania własnych plików w Internecie (mogą one np. podłączać niechciane linijki kodu do źródła strony).
- Co jakiś czas skanuj komputer i sprawdzaj procesy sieciowe – jeśli się na tym nie znasz poproś o sprawdzenie kogoś, kto się zna. Czasami złośliwe oprogramowanie nawiązujące własne połączenia z Internetem, wysyłające twoje hasła i inne prywatne dane do sieci może się zainstalować na komputerze mimo dobrej ochrony – należy je wykryć i zlikwidować.
- Sprawdzaj pliki pobrane z Internetu za pomocą skanera.
- Staraj się nie odwiedzać zbyt często stron, które oferują niesamowite atrakcje (darmowe filmiki, muzykę, albo łatwy zarobek przy rozsyłaniu spamu) – często na takich stronach znajdują się ukryte wirusy, trojany i inne zagrożenia.
- Nie zostawiaj danych osobowych w niesprawdzonych serwisach i na stronach, jeżeli nie masz absolutnej pewności, że nie są one widoczne dla osób trzecich.
- Nie wysyłaj w e-mailach żadnych poufnych danych w formie otwartego tekstu.
- Aktualizuj system operacyjny i aplikacje bez zbędnej zwłoki.
- Pamiętaj o uruchomieniu firewalla.
- Wykonuj kopie zapasowe ważnych danych.
- Pamiętaj, że żaden bank czy Urząd nie wysyła e-maili do swoich klientów/interesantów z prośbą o podanie hasła lub loginu w celu ich weryfikacji.