Zasady bezpiecznego korzystania z Internetu
w Zespole Szkół Technicznych im. Bohaterów Września 1939 r. w Kolbuszowej

[wersja 2025-04-29]

Informacje ogólne

1. Szkoła zapewnia uczniom oraz personelowi dostęp do Internetu oraz podejmuje działania zabezpieczające uczniów przed dostępem do treści, które mogą stanowić zagrożenie dla ich prawidłowego rozwoju.
2. Szkoła zapewnia personelowi i uczniom możliwość korzystania z Internetu w czasie trwania zajęć.
3. Sieć szkolna jest monitorowana.
4. Ze szkolnej sieci i Internetu można korzystać tylko w celach edukacyjnych i związanych z pracą zawodową.
5. Szkoła dla zapewnienia bezpiecznego dostępu do internetu współpracuje z OSE i NASK.
6. Za zagrożenia związane z użytkowaniem przez małoletnich Internetu i mediów elektronicznych uznaje się: dostęp do treści nielegalnych, szkodliwych i nieodpowiednich, treści nawołujące do przemocy, przestępczości, radykalizacji i ekstremizmu, patostreamy, treści dyskryminacyjne, treści pornograficzne, dostęp do szkodliwych i nieodpowiednich kontaktów online oraz usług online, dostęp do szkodliwych i ryzykownych zachowań.
7. Za zagrożenia związane z bezpieczeństwem sieci uznaje się: złośliwe oprogramowania (malware), ataki z wykorzystaniem złośliwego kodu na stronach internetowych, phishing - wyłudzanie poufnych informacji, spam, ataki DDoS, kradzież tożsamości, naruszenie poufności, integralności lub dostępności danych, zagrożenia wewnętrzne (dywersja), botnety - sieci komputerów przejętych przez przestępców, ingerencja fizyczna w sieć, uszkodzenia, kradzież, wyciek danych, ataki ransomware w celu wyłudzenia okupu za odszyfrowanie lub nieujawnianie wykradzionych danych, cyberszpiegostwo.
8. W przypadku dostępu realizowanego pod nadzorem pracownika Szkoły, ma on obowiązek informowania uczniów o zasadach bezpiecznego korzystania z Internetu. Pracownik Szkoły czuwa także nad bezpieczeństwem korzystania z Internetu przez uczniów podczas zajęć.
9. Pracownicy, nauczyciele i uczniowie są zobowiązani do zgłaszania incydentów związanych z bezpieczeństwem w sieci do szkolnego koordynatora bezpieczeństwa w sieci.
10. W ramach zajęć z wychowawcą lub nauczycielem informatyki przeprowadza się z uczniami warsztaty dotyczące bezpiecznego korzystania z Internetu przynajmniej raz w roku.

Uczeń:

1. Ma prawo korzystać ze szkolnej sieci i Internetu w pracowniach za zgodą i pod opieką nauczyciela prowadzącego zajęcia.
2. Ma obowiązek rozwijać umiejętności cyfrowe, efektywnie korzystać z technologii, rozumieć zasady bezpieczeństwa online i odpowiednio reagować na zagrożenia cyfrowe.
3. Ma obowiązek szanować innych użytkowników Internetu i sieci.
4. Ma obowiązek szanować prawo własności w sieci. Jeśli posługują się materiałami znalezionymi w Internecie, zawsze należy podawaj źródło ich pochodzenia.
5. Ma obowiązek chronić swoją prywatność online i unikać udostępniania informacji osobistych i osobowych.
6. Ma obowiązek chroń dane dostępowe do szkolnego konta pracy grupowej i dziennika elektronicznego.

   W przypadku utraty kontroli nad swoim kontem pracy grupowej lub dziennika elektronicznego należy to zgłosić szkolnemu administratorowi lub wychowawcy.
7. Należy przestrzegać prawa swojego i innych osób do rozporządzania swoimi danymi oraz swoim wizerunkiem. Nie wolno utrwalać lub zamieszczać w Internecie treści do których nie ma zgody osób których dotyczą.
8. Jeżeli jesteś ofiarą cyberprzemocy, takiej jak nękanie, hejtowanie czy szantaż zgłoś to nauczycielowi, pedagogowi lub wychowawcy.
9. Należy używać w sieci silnych haseł, unikaj klikania w podejrzane linki, rozpoznawać oszustwa online.
10. Należy rozwijać umiejętności krytycznego myślenia i zdrowego podejścia do informacji w Internecie, aby nie ulec fałszywym informacjom, szkodliwym treściom oraz ich nie powielać.
11. W przeglądarkach i wyszukiwarkach z których korzysta mają być włączone domyślnie ustawione filtry bezpiecznego wyszukiwania.
12. Czytaj komunikaty w przeglądarkach, stronach i aplikacjach których używasz, nie wyrażaj zgody na zbieranie danych które nie są wymagane.
13. Komputery na zajęciach i sieć w szkole jest monitorowana.
14. Niedozwolone jest używanie sieci szkolnej i internetu do zakłócania pracy systemów informatycznych lub dostępu do danych. Wszelkie nieprawidłowości w bezpiecznej pracy sieci należy zgłaszać administratorowi sieci.
15. Nie wolno używać nie swoich loginów, kont czy innych poświadczeń w sieci. Pamiętaj aby właściwie kończyć pracę przy komputerze wylogowując się z systemów z których korzystałeś.
16. Zasady korzystania z własnych urządzeń elektronicznych przez uczniów na terenie szkoły reguluje Statut Szkoły.

Rodzicu:

1. Wspólnie ze swoim dzieckiem ucz się zasad bezpieczeństwa w sieci.
2. Stosuj zasadę ograniczonego zaufania w Internecie.
3. Wspólnie przygotujcie swoje komputery, smartfony i inne urządzenia podłączone do internetu na niebezpieczeństwa w sieci.
4. Rozważ wprowadzenie blokady rodzicielskiej szkodliwych treści.
5. Uważaj na uzależnienie od Internetu i komputera.
6. Monitoruj korzystanie przez dziecko z mediów społecznościowych.
7. Własnym przykładem pokaż, że nie jest konieczne korzystanie z mediów społecznościowych.
8. Daj znać swojemu dziecku, że zawsze może przyjść do ciebie w każdej trudnej sytuacji.
9. Nikomu nie podawaj danych dostępowych do dziennika elektronicznego, znajdują się w nim m.in. dane osobowe Twoje oraz Twoich dzieci.

Pracownicy szkoły i nauczyciele:

1. Nauczyciel podczas zajęć czuwa nad bezpieczeństwem korzystania z Internetu, ma on obowiązek informowania małoletnich o zasadach bezpiecznego korzystania z Internetu i reagować na ewentualne zagrożenia w czasie korzystania z sieci.
2. Nauczyciele i pracownicy szkoły mają obowiązek rozwijania swoich umiejętności cyfrowych aby efektywnie korzystać z technologii, rozumieć zasady bezpieczeństwa online i odpowiednio reagować na zagrożenia cyfrowe.
3. Za zgodą dyrektora pracownicy mogą używać własnych urządzeń do łączenia z internetem w szkolnej sieci w celach edukacyjnych i zawodowych. Sposób podłączenia i stopień zabezpieczeń należy skonsultować z administratorem szkolnej sieci.
4. Za zgodą dyrektora z wydzielonej sieci dla gości mogą korzystać inne osoby.
5. Do kontaktu przez Internet z uczniami, rodzicami i współpracownikami używaj szkolnego systemu pracy grupowej i dziennika elektronicznego.
6. Wszelkie nieprawidłowości w pracy sieci należy zgłaszać administratorowi sieci a wszelkie naruszenia bezpieczeństwa sieci szkolnemu koordynatorowi bezpieczeństwa w sieci.
7. Sposoby korzystania ze sprzętu, zabezpieczenia i procedury zawarte są w polityce bezpieczeństwa cyfrowego w szkole.

Zabezpieczenie sprzętu:

1. Sprzęt komputerowy jest zlokalizowany w pomieszczeniach zamykanych. W pomieszczeniach mogą przebywać wyłącznie upoważnieni pracownicy, a osoby postronne tylko pod nadzorem upoważnionego pracownika.

2. Okablowanie sieciowe zostało zaprojektowane w ten sposób, że dostęp do linii teletransmisyjnych jest możliwy tylko z pomieszczeń zamykanych.

3. Poszczególne części sieci (administracja, sieć bezprzewodowa, internet dla gości, pracownie...) są odseparowane fizycznie lub programowo;

4. Sieć bezprzewodowa została zaprojektowana tak aby dostęp do niej miały tylko pracownicy i osoby upoważnione, oraz jest odseparowana od innych części sieci;

5. Bieżąca konserwacja sprzętu wykorzystywanego w szkole jest przeprowadzana przez pracowników szkoły. Natomiast poważne naprawy sprzętu który służy między innymi w dostępie do danych osobowych wykonywane przez personel zewnętrzny realizowane są na terenie szkoły po zawarciu z podmiotem wykonującym naprawę umowy o powierzenie przetwarzania danych osobowych, określającej kary umowne za naruszenie bezpieczeństwa danych.

6. Dopuszcza się konserwowanie i naprawę sprzętu poza siedzibą administratora danych jedynie po trwałym usunięciu danych osobowych. Zużyty sprzęt służący do przetwarzania danych osobowych może być zbywany dopiero po trwałym usunięciu danych, a urządzenia uszkodzone mogą być przekazywane w celu utylizacji (jeśli trwałe usunięcie danych wymagałoby nadmiernych nakładów ze strony administratora) właściwym podmiotom, z którymi także zawiera się umowy powierzenia przetwarzania danych.

7. Administratorem systemów informatycznych oraz sieci w szkole i w pracowniach są osoby wyznaczone przez dyrektora szkoły.

8. Administratorzy systemów informatycznych i sieci w celu zapewnienia bezpieczeństwa współpracują z wyznaczonym przez dyrektora koordynatorem bezpieczeństwa sieci.

9. Wszystkie awarie, działania konserwacyjne i naprawy systemu informatycznego są zgłaszane do Administratora systemów informatycznych lub sieci.

10. Administrator systemów informatycznych dobiera elektroniczne środki ochrony przed atakami z sieci stosownie do pojawiania się nowych zagrożeń (malware, wirusy, robaki, trojany, inne możliwości przełamywania zabezpieczeń), a także stosownie do rozbudowy systemu informatycznego w szkole. Jednocześnie należy zwracać uwagę, czy rozwijający się system zabezpieczeń sam nie wywołuje nowych zagrożeń.

11. Poszczególnym osobom upoważnionym do przetwarzania danych osobowych przydziela się sprzęt lub konta opatrzone niepowtarzalnym identyfikatorem, umożliwiające dostęp do danych, zgodnie z zakresem upoważnienia do ich przetwarzania. Administrator systemu informatycznego na polecenie dyrektora przydziela pracownikowi upoważnionemu do przetwarzania danych sprzęt lub konto w systemie informatycznym. W razie potrzeby, po uzyskaniu uprzedniej akceptacji dyrektora, administrator systemu informatycznego może przydzielić konto opatrzone identyfikatorem osobie upoważnionej do przetwarzania danych osobowych, nieposiadającej statusu pracownika.

12. Administrator sieci wykorzystuje centralną zaporę sieciową w celu separacji lokalnej sieci od sieci publicznej.

13. Operacje za pośrednictwem rachunku bankowego administratora danych może wykonywać wyłącznie upoważniony pracownik działu księgowości po uwierzytelnieniu się zgodnie z procedurami określonymi przez bank obsługujący rachunek.

Zabezpieczenia we własnym zakresie:

Dla bezpieczeństwa informacji oraz sieci każda osoba upoważniona do przetwarzania danych lub użytkownik zobowiązany jest do:

1. Ustawiania ekranów komputerowych tak, by osoby niepowołane nie mogły oglądać ich zawartości.

2. Nie pozostawiania bez kontroli dokumentów, nośników danych i sprzętu w miejscach publicznych oraz w samochodach.

3. Dbania o prawidłową eksploatację powierzonego sprzętu.

4. Pilnego strzeżenia danych, pamięci przenośnych i komputerów przenośnych.

5. Trwałego kasowania po wykorzystaniu danych na dyskach przenośnych.

6. Niezapisywania hasła wymaganego do uwierzytelnienia się w systemie na papierze lub innym nośniku niezabezpieczonym.

7. Powstrzymywania się przez osoby upoważnione do przetwarzania danych osobowych od samodzielnej ingerencji w oprogramowanie i konfigurację powierzonego sprzętu obniżające poziom bezpieczeństwa.

8. Przestrzegania przez osoby upoważnione do przetwarzania danych osobowych swoich uprawnień w systemie, tj. właściwego korzystania z baz danych, używania tylko własnego identyfikatora i hasła oraz stosowania się do zaleceń inspektora ochrony danych osobowych.

9. Opuszczania stanowiska pracy dopiero po wylogowaniu z systemu/zasobu/konta pracy grupowej/dziennika elektronicznego, aktywacji blokady ekranu lub po zablokowaniu stacji roboczej w inny sposób.

10. Kopiowania tylko jednostkowych danych (pojedynczych plików). Obowiązuje zakaz robienia kopii całych zbiorów danych lub takich ich części, które nie są konieczne do wykonywania obowiązków przez pracownika. Jednostkowe dane mogą być kopiowane na nośniki magnetyczne, optyczne i inne po ich zaszyfrowaniu lub przechowywane w

zamkniętych na klucz szafach. Po ustaniu przydatności tych kopii dane należy trwale skasować lub fizycznie zniszczyć nośniki, na których są przechowywane.

11. Zabrania się przesyłania danych osobowych pocztą elektroniczną bez zastosowania szyfrowania.

12. Nie wynoszenia na jakichkolwiek nośnikach całych zbiorów danych oraz szerokich z nich wypisów, nawet w postaci zaszyfrowanej.

13. Należytego dokonywania kopii roboczych danych, na których się właśnie pracuje, tak często, aby zapobiec ich utracie.

Przed atakami z sieci wewnętrznej i zewnętrznej komputery chronione są środkami dobranymi przez administratora systemów informatycznych. Ważne jest, by użytkownicy zwracali uwagę na to, czy urządzenie, na którym pracują, domaga się aktualizacji tych zabezpieczeń. O wszystkich takich przypadkach należy poinformować administratora systemów informatycznych.

Komputery przenośne i praca na odległość:

1. Urządzenia przenośne oraz nośniki danych wynoszone z siedziby szkoły nie powinny być pozostawiane bez nadzoru w miejscach publicznych. Należy się upewnić czy nie ma na nich danych osobowych w postaci nie zaszyfrowanej.

2. Nie należy pozostawiać bez kontroli dokumentów, nośników danych i sprzętu w hotelach i innych miejscach publicznych ani też w samochodach.

3. Informacje przechowywane na urządzeniach przenośnych lub komputerowych nośnikach danych należy chronić przed uszkodzeniami fizycznymi lub utratą.

4. W domu niedozwolone jest udostępnianie domownikom szkolnego sprzętu. Użytkownik powinien zachować w tajemnicy wobec domowników identyfikator i hasło, których podanie jest konieczne do rozpoczęcia pracy na komputerze przenośnym lub w systemie pracy grupowej.

5. W przypadku korzystania do pracy ze własnego sprzętu należy upewnić się że nikt inny nie ma do niego dostępu, upewnić się że stan i aktualność zabezpieczeń jest na odpowiednim poziomie.

6. W zakresie nieuregulowanym w polityce bezpieczeństwa stosuje się do pracy z wykorzystaniem komputerów przenośnych postanowienia instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych.