

STANDARDY OCHRONY MAŁOLETNICH DLA

***TECHNIKUM MECHANICZNEGO NR 17
BRANŻOWEJ SZKOŁY I STOPNIA NR 17***

**W ZESPOLE SZKÓŁ MECHANICZNYCH NR 3
IM. GEN. WŁADYSŁAWA SIKORSKIEGO
W KRAKOWIE**

(WERSJA SKRÓCONA DLA UCZNIÓW)



Standardy ochrony małoletnich przed krzywdzeniem
obowiązujące
w Zespole Szkół Mechanicznych nr 3 im. gen. Władysława Sikorskiego
w Krakowie
(wersja skrócona dla uczniów)

Placówka posiada dokument Polityki ochrony dzieci, który uwzględnia:

procedury zgłaszania podejrzeń oraz podejmowania interwencji w sytuacji krzywdzenia dziecka lub zagrożenia jego bezpieczeństwa ze strony osób obcych, członków rodziny, personelu placówki oraz rówieśników;

zasady ochrony danych osobowych małoletniego, w tym wizerunku, określające sposób przechowywania i udostępniania informacji o nim;

zasady dostępu uczniów niepełnoletnich do Internetu oraz ich ochrony przed szkodliwymi treściami w Internecie;

zasady bezpiecznych relacji personel placówki – dziecko oraz relacji małoletni- rówieśnicy, określające zachowania pożądane i niedozwolone w kontakcie z niepełnoletnim uczniem;

zasady bezpiecznej rekrutacji personelu do pracy w szkole

zasady monitoringu stosowania Standardów

Preambuła

Naczelną zasadą przyjętą w Zespole Szkół Mechanicznych nr 3 im. Gen. Władysława Sikorskiego w Krakowie jest działanie pracowników dla dobra i bezpieczeństwa małoletnich. Mając na uwadze, że niepełnoletni uczeń wymaga szczególnej opieki i troski, w tym właściwej ochrony przed krzywdzeniem, został opracowany i wdrożony niniejszy dokument. Pracownicy placówki realizując te cele traktują ucznia podmiotowo i działają w ramach obowiązującego prawa i przepisów oraz posiadanych kompetencji.

Rozpoznawanie czynników ryzyka krzywdzenia dzieci i reagowanie na nie

Rekrutacja pracowników Szkoły oraz współpraca z Partnerami odbywa się zgodnie z zasadami bezpieczeństwa.

Pracownicy szkoły posiadają niezbędną wiedzę i w ramach wykonywanych obowiązków zwracają uwagę na czynniki ryzyka i symptomy krzywdzenia dzieci.

Pracownicy znają i stosują przyjęte w placówce zasady bezpiecznych relacji personel- małoletni i uczeń- uczeń.

ZASADY BEZPIECZNYCH RELACJI PRACOWNIK- UCZEŃ

Podstawową zasadą wszystkich czynności podejmowanych przez personel jest działanie dla dobra ucznia i w jego interesie. Personel traktuje ucznia z szacunkiem oraz uwzględnia jego godność i potrzeby.

Zasady bezpiecznych relacji personelu z uczniami obowiązują wszystkich pracowników, partnerów szkoły oraz stażystów i wolontariuszy.

Pracownik ZSM nr 3 w kontakcie z uczniami:

zachowuje cierpliwość, odnosi się do ucznia z szacunkiem i jest otwarty na jego problemy, nie zawstydzia ucznia, nie lekceważy, nie upokarza i nie obraża, nie krzyczy, chyba że wymaga tego zachowanie zasad bezpieczeństwa, nie ujawnia drażliwych informacji o uczniu osobom do tego nieuprawnionym, dotyczy to również ujawniania jego wizerunku.

Decyzje dotyczące ucznia powinny uwzględniać jego oczekiwania, ale również brać pod uwagę bezpieczeństwo pozostałych uczniów.

Pracownikowi ZSM nr 3 nie wolno w obecności uczniów niestosownie żartować, używać wulgaryzmów, wykonywać obraźliwych gestów, wypowiadać treści o zabarwieniu seksualnym, wykorzystywać przewagi fizycznej ani stosować gróźb.

Pracownik ZSM nr 3 zobowiązany jest do równego traktowania uczniów, niezależnie od ich płci, orientacji seksualnej, wyznania, pochodzenia etnicznego czy też niepełnosprawności.

Pracownikowi ZSM nr 3 bezwzględnie zabrania się:

nawiązywania relacji seksualnych z uczniem,

składania uczniowi propozycji o charakterze seksualnym i pornograficznym, w tym również udostępniania takich treści,

proponowanie uczniom alkoholu, wyrobów tytoniowych i innych używek (narkotyków, tzw. dopalaczy).

skracania dystansu w relacjach interpersonalnych niosących ryzyko naruszenia bezpieczeństwa małoletniego.

W uzasadnionych przypadkach dopuszczalny jest kontakt fizyczny pracownika z uczniem. Do sytuacji takich należy zaliczyć np. udzielenie pomocy przedmedycznej w przypadku urazu, zasłabnięcia itp.; interwencja w przypadku niebezpiecznych zachowań.

Jeśli pracownik musi spotkać się z uczniem poza godzinami pracy ZSM nr 3, wymagane jest poinformowanie o tym fakcie dyrektora, a opiekun musi wyrazić na taki kontakt zgodę.

W przypadku, gdy pracownika łączą z uczniem lub jego opiekunem relacje rodzinne lub towarzyskie, zobowiązany on jest do zachowania pełnej poufności, w szczególności do utrzymania w tajemnicy spraw dotyczących innych uczniów, opiekunów i pracowników.

RELACJE MIĘDZY UCZNIAMI

Na terenie Zespołu Szkół Mechanicznych nr 3 w Krakowie w relacjach między uczniami obowiązuje zasada równości w swoich prawach. Każdy uczeń bez względu na płeć, pochodzenie, wyznanie, poglądy polityczne, status socjoekonomiczny, stan rodzinny czy orientację seksualną jest równy w swoich prawach. Zachowania uczniów wobec siebie nie mogą naruszać obowiązujących przepisów prawnych.

Relacje między każdym uczniem (niepełnoletnim oraz pełnoletnim) mają opierać się na wzajemnym szacunku. Każdy uczeń ma prawo do wyrażania własnego zdania, o ile nie krzywdzi ono innych oraz nie jest wymierzone w osobę lub grupę innych osób, a zatem z poszanowaniem ich godności oraz wolności, bez znamion dyskryminacji. Podejmowane działania nie mogą naruszać nietykalności cielesnej, powodować szkody na zdrowiu fizycznym lub psychicznym ucznia, wywoływać cierpienia lub krzywdy.

Zachowania dozwolone i niedozwolone w relacjach między uczniami

Za działania pożądate między uczniami uważa się każde zachowanie pozostające w zgodzie z normami akceptowanymi społecznie z uwzględnieniem płci, pochodzenia, wyznania oraz orientacji seksualnej ucznia, a także zachowaniem równości w relacjach między uczniami. W przypadku braku zgody na dane zachowanie uczeń odpowiadający za to działanie powinien ją zaakceptować i zmienić sposób postępowania lub zaniechać kontaktu w danej chwili. Dopuszcza się żartowanie z siebie między uczniami o ile wyrażona jest obopólna zgoda oraz żadna z osób nie doznaje w jego wyniku szeroko pojętego cierpienia lub krzywdy. Uczniowie powinni szanować siebie nawzajem i zważać na własne zachowanie, które może bezpośrednio lub pośrednio wpływać na ich otoczenie (np. głośne słuchanie muzyki na przerwach, które przeszkadza w prowadzeniu rozmów przez innych uczniów). Od uczniów oczekuje się kultury osobistej oraz chęci pomocy w przypadkach, które tej pomocy wymagają.

Za działania niepożądane między uczniami uważa się:

narażające na niebezpieczeństwo utraty życia i/lub zdrowia w tym posiadanie, podawanie lub udostępnianie niedozwolonych substancji psychoaktywnych, alkoholu, nikotyny, wyrobów tytoniowych, dopalaczy itp.

naruszanie spokoju (głośne zachowanie oraz słuchanie muzyki, odpalanie petard itp.) oraz mienia, z którego korzystają wszyscy uczniowie (toalety, sprzęt komputerowy itd.)

zachowania poza granicami dobrego smaku m.in. prowokacyjny ubiór, obsceniczne gesty, narzucanie się, obłapianie, obmacywanie, poklepywanie, natarczywe wyrażanie uczuć do drugiej osoby w przestrzeni publicznej;

zachowania niszczące opinię szkoły, w szczególności w rozumieniu społeczności uczniowskiej; wszelkie przejawy przemocy fizycznej i seksualnej tj.:

bicie, popychanie, szarpanie, przypalanie, szturchanie, kopanie itp.

niszczenie przedmiotów należących do ucznia;

nadużywanie swojej przewagi nad inną osobą,;

rzucanie w kogoś przedmiotami;

przymuszanie do czynności o charakterze seksualnym;

zmuszanie do innych zachowań wbrew woli ucznia;

wszelkie przejawy przemocy psychicznej tj:

wyśmiewanie, poniżanie i ubliżanie (zarówno w formie kontaktu bezpośredniego jak i pośredniego), obraźliwe plotki i żarty;

prowokowanie, podburzanie, podpuszczanie;

grożenie, zastraszanie, szantażowanie;

izolowanie i wykluczanie z grupy;
 przemoc słowna wymierzona w rodzinę ucznia, przyjaciół i jego najbliższe otoczenie;
 pisanie na ścianach i innych powierzchniach użyteczności publicznej informacji o uczniu;
 wulgarne gesty;
 śledzenie/szpiedgowanie;
 wszelkie przejawy cyberprzemocy tj.:
 naruszanie dobrego imienia ucznia z wykorzystaniem jego wizerunku w sieci;
 obraźliwe komentarze w sieci pod adresem ucznia;
 produkowanie lub udostępnianie innym za pomocą cyfrowych technologii zdjęć, filmów ośmieszających ucznia i publikowanie ich w sieci, także modyfikowanie treści z udziałem ucznia w celu ośmieszenia go (w tym patostreaming);
 podszywanie się za ucznia w sieci i tworzenie treści w jego imieniu;
 nakłanianie innych użytkowników technologii cyfrowych do określonych działań na szkodę ucznia (np. wykluczania go z grupy, hejtowanie, udostępnianie szkalujących treści);
 każde wykorzystanie jego wizerunku (np. zdjęcia) w sieci bez zgody opiekuna prawnego dziecka.
 każde inne działania naruszające prawa ucznia lub jego dobra osobiste w szczególności:
 narażające tę osobę na niebezpieczeństwo utraty życia, zdrowia lub mienia,
 naruszające jego godność, nietykalność cielesną lub wolność, w tym seksualną,
 powodujące szkody na jego zdrowiu fizycznym lub psychicznym, wywołujące u niego cierpienie lub krzywdę,
 istotnie naruszające jego prywatność lub wzbudzające w nim poczucie zagrożenia, poniżenia lub udręczenia, w tym podejmowane za pomocą środków komunikacji elektronicznej.

1. Za działania niedozwolone uważa się wszelkie przestępstwa ścigane z urzędu wskazane w Kodeksie Karnym:

- 107 k.k.- dokuczanie, złośliwe niepokojenie
- 156 Kodeksu karnego (dalej k.k.) – ciężki uszczerbek na zdrowiu,
- 160 §§ 1, 3 k.k. – narażenie na niebezpieczeństwo,
- 190 §§1,2 kk- groźby, zgłoszenie,
- 190a §§ 1,2,3,4 k.k. nękanie, podszywanie się, wykorzystywanie wizerunku, sprawstwo targnięcia się na życie, zgłoszenie,
- 191 § 1 k.k. – zmuszanie przemocą lub groźbą bezprawną osoby do określonego zachowania,
- 200 k.k. – czynność seksualna z małoletnim poniżej 15 roku życia, pornografia z udziałem małoletniego,
- 202 k.k. – prezentacja i rozpowszechnianie pornografii,
- 203 k.k. – przymuszanie do prostytucji,
- 204 k.k. – stręczycielstwo, sutenerstwo,
- 207 k.k. – znęcanie się,
- 208 k.k. – rozpijanie małoletniego,
- 210 k.k. – porzucenie nieporadnego,
- 211 k.k. – uprowadzenie małoletniego lub nieporadnego,
- 212 k.k. pomawianie,
- 216 k.k.- znieważanie w środkach masowego komunikowania się,
- 217 k.k.- naruszenie nietykalności,
- 276 k.k. – zniszczenie, uszkodzenie, ukrycie lub usunięcie dokumentu,
- 280 k.k. – rozbój,
- 281 k.k. – kradzież rozbójnicza,
- 282 k.k. – wymuszenie rozbójnicze,

- 284 §§ 1, 3 k.k. – przywłaszczenie mienia
- 288 k.k.- niszczenie cudzej rzeczy

W przypadku zidentyfikowania czynników ryzyka, pracownicy szkoły podejmują działania zgodnie z przyjętymi w Zespole procedurami.

Procedury interwencji w przypadku krzywdzenia dziecka

Każdy pracownik szkoły/uczeń/rodzic/opiekun prawny, który uzyskał informację o krzywdzeniu małoletniego przez osobę dorosłą zatrudnioną w placówce, rodzica/ opiekuna oraz innego ucznia, ma obowiązek powiadomienia o tym dyrektora szkoły/ jego zastępcę/wychowawcę/pedagoga szkolnego/psychologa szkolnego.

Na podstawie zgłoszenia krzywdzenia małoletniego szkoła podejmuje działania zgodnie z procedurami zawartymi w dokumencie głównym.

W każdym przypadku zauważenia krzywdzenia ucznia należy wypełnić Kartę Interwencji. Kartę tę załącza się do dokumentacji ucznia.

Karta Interwencji zawiera następujące informacje:

imię i nazwisko skrzywdzonego ucznia, przyczynę interwencji, imię i nazwisko osoby zgłaszającej naruszenie bezpieczeństwa małoletniego, opis działań podjętych przez pracownika, opis spotkania z opiekunem małoletniego, formy zastosowanej interwencji, nazwa organu, do którego zgłoszono interwencję, wyniki interwencji, podpis osoby przyjmującej interwencję.

Każda osoba, która uczestniczy w rozwiązywaniu problemów ucznia, zobowiązana jest do zachowania tajemnicy. Zauważony problem jest procedowany tylko z osobami uprawnionymi.

Po zastosowaniu procedur, każdorazowo, w sposób dostosowany do konkretnego przypadku, ustala się plan wsparcia małoletniego w celu zapewnienia bezpieczeństwa. Wsparcie może obejmować w szczególności pomoc psychologiczną, medyczną oraz prawną.

Plan interwencyjny ustalany jest przez zespół interwencyjny w składzie wychowawca klasy, pedagog szkolny, psycholog szkolny a w przypadku ucznia z orzeczeniem o potrzebie kształcenia specjalnego także pedagog specjalny. Plan jest przedstawiany rodzicom/opiekunom małoletniego.

Jeżeli podejrzenie skrzywdzenia małoletniego nie zostało potwierdzone, o tym fakcie Szkoła informuje rodziców/ opiekunów na piśmie.

Wszyscy pracownicy szkoły i inne osoby, które w związku z wykonywaniem obowiązków służbowych podjęły informację o krzywdzeniu małoletniego lub informacje z tym związane, są zobowiązani do zachowania tych informacji w tajemnicy, wyłączając informacje przekazywane uprawnionym instytucjom w ramach działań interwencyjnych.

Zasady ochrony danych osobowych i wizerunku małoletniego

Dane osobowe ucznia są udostępniane wyłącznie osobom i podmiotom uprawnionym;

ochrona danych osobowych i wizerunku opiera się na opracowanych w placówce zasadach.

Dzielenie się zdjęciami i filmami z naszych aktywności służy celebrowaniu sukcesów uczniów, dokumentowaniu naszych działań i zawsze ma na uwadze bezpieczeństwo uczniów. Wykorzystujemy zdjęcia/nagrania pokazujące uczniów w różnym wieku, o różnych uzdolnieniach, stopniu sprawności i reprezentujące różne grupy etniczne.

Uczniowie mają prawo zdecydować, czy ich wizerunek zostanie zarejestrowany i w jaki sposób zostanie przez nas użyty.

Zgoda rodziców/opiekunów prawnych na wykorzystanie wizerunku ich dziecka jest tylko wtedy wiążąca, jeśli uczniowie i rodzice/opiekunowie prawni zostali poinformowani o sposobie wykorzystania zdjęć/nagrań i ryzyku wiążącym się z publikacją wizerunku.

Dbamy o bezpieczeństwo wizerunków uczniów poprzez:

Pytanie o pisemną zgodę rodziców/opiekunów prawnych uczniów na pierwszych spotkaniach z rodzicami w klasie pierwszej. Zgoda wyrażana jest na czas nauki w Zespole Szkół Mechanicznych nr. 3 w Krakowie. Rodzic ma prawo do wycofania zgody w dowolnym momencie.

Udzielenie wyjaśnień, do czego wykorzystamy zdjęcia/nagrania i w jakim kontekście.

Rezygnację z ujawniania jakichkolwiek informacji wrażliwych o uczniach dotyczących m.in. stanu zdrowia, sytuacji materialnej, sytuacji prawnej i powiązanych z wizerunkiem uczniów (np. w przypadku zbiorów indywidualnych organizowanych przez naszą instytucję).

Zmniejszenie ryzyka kopiowania i nieestosownego wykorzystania zdjęć/nagrań uczniów poprzez przyjęcie zasad:

sytuacja zdjęcia/nagrania nie jest dla uczniów poniżająca, ośmieszająca ani nie ukazuje ich w negatywnym kontekście,

zdjęcia/nagrania uczniów powinny się koncentrować na czynnościach wykonywanych przez uczniów

Rezygnację z publikacji zdjęć uczniów, nad którymi nie sprawujemy już opieki, jeśli oni lub ich rodzice/opiekunowie prawni nie wyrazili zgody na wykorzystanie zdjęć po odejściu z instytucji.

Przyjęcie zasady, że wszystkie podejrzenia i problemy dotyczące niewłaściwego rozpowszechniania wizerunków uczniów należy rejestrować i zgłaszać dyrekcji, podobnie jak inne niepokojące sygnały dotyczące zagrożenia bezpieczeństwa uczniów.

Dane osobowe będą przetwarzane zgodnie z RODO w celu wykonywania obowiązków prawnych ciążących na Administratorze, tj. realizacji zadań dydaktycznych, wychowawczych i opiekuńczych na podstawie ustawy z dnia 7 września 1991 r. o systemie oświaty, ustawy Prawo oświatowe z dnia 14 grudnia 2016 r. oraz innych ustaw i aktów wykonawczych zgodnie z art. 6 ust. 1 lit. c) oraz e) RODO, mając na względzie obowiązek edukacji do 18 roku życia wynikający z art. 70 ust. 1 Konstytucji RP.

Zasady dostępu małoletnich do internetu oraz ochrony przed szkodliwymi treściami

Placówka, zapewniając małoletnim dostęp do internetu, jest zobowiązana podejmować działania zabezpieczające małoletnich przed dostępem do treści, które mogą stanowić zagrożenie dla ich prawidłowego rozwoju oraz bezpieczeństwa.

Zasady bezpiecznego korzystania z internetu i mediów elektronicznych uwzględnione zostały w regulaminie obowiązującym w pracowniach informatycznych.

Zasady bezpiecznego korzystania z internetu

1. Ogranicz dane osobowe, które udostępniasz w sieci

Im mniej Twoich **danych osobowych** w sieci, tym lepiej – taka jest podstawowa zasada bezpiecznego korzystania z Internetu. Każda, nawet banalna informacja, może posłużyć przestępcom do ataku.

Imię i nazwisko, data urodzenia, numer karty kredytowej, numer PESEL, adres zamieszkania, bank, z którego usług korzystasz – to wszystko **informacje bezcenne dla cyberprzestępców**. Mogą wykorzystać je np. do phishingu (więcej na ten temat dowiesz się niżej) czyli **najbardziej popularnego rodzaju ataku** wymierzonego w każdego użytkownika sieci.

Im mniej prywatnych informacji podasz w Internecie, tym mniejsze ryzyko, że padniesz ofiarą np. **cyberstalkingu** czyli nękanie, grózb i ataków przy użyciu sieci.

2. Używaj silnych i unikalnych haseł

Używanie **słabego hasła** lub jednego hasła do zabezpieczenia wielu kont, to recepta na kłopoty. Przestępca może okraść Twoje konto, zaciągnąć kredyt, użyć skrzynki e-mail do ataku na innych użytkowników czy też wykraść dane.

Używaj silnych, nie powtarzających się haseł. To podstawowa zasada higieny korzystania z m.in. bankowości elektronicznej, poczty e-mail i niezliczonej ilości usług w sieci, w których musisz używać hasła.

Hasła możesz tworzyć polegając na własnej przemyślności i sprawdzonych [porad dot. tworzenia silnych i trudnych do złamania haseł](#) lub skorzystać z [menedżera haseł](#). Menedżer haseł to program, który generuje i przechowuje dane logowania powiązane z kontami internetowymi. Dzięki niemu musisz pamiętać wszystkich haseł, wystarczy **hasło główne do menedżera**. Użycie takiego programu to praktyczny i zaawansowany sposób na poprawę bezpieczeństwa w sieci. Warto wybrać program typu open source z **szyfrowaniem typu end-to-end** i **weryfikacją dwuskładnikową**.

3. Używaj weryfikacji dwuetapowej

Weryfikacja dwuetapowa (2FA) to opcja dostępna w wielu serwisach (Facebook, Google), która zdecydowanie poprawi Twoje cyberbezpieczeństwo. Tego typu uwierzytelnienie wymaga przynajmniej dwóch kroków: podania hasła oraz wprowadzenia tymczasowego kodu wysłanego przez serwis w sms-ie lub przy użyciu specjalnej aplikacji (np. Google Authenticator).

Możesz również zdecydować się na **stosowanie klucza U2F** czyli fizycznego przedmiotu przypominającego pendrive'a lub brelok do kluczy – ta metoda jest najbardziej odporna na phishing.

Pamiętaj, że uwierzytelnienie przy użyciu SMS jest mniej bezpieczne od dobrej aplikacji do weryfikacji dwuetapowej.

Oto **zestawienie weryfikacji 2FA** od najbardziej do najmniej bezpiecznych:

- klucz U2F,
- kody czasowe w aplikacji,
- kody jednorazowe SMS,
- kody wysyłane przez e-mail.

Dzięki uwierzytelnieniu wieloskładnikowemu skomplikujesz życie cyberprzestępcom i lepiej zabezpieczysz się jeżeli dane Twoje konta wyciekną lub zostaną wykradzione.

4. Nie korzystaj z jednej skrzynki pocztowej

Wiele osób używa jednego adresu e-mail do obsługi spraw związanych z pracą/firmą, rejestracji do najróżniejszych newsletterów, zakupów czy też aplikacji w chmurze. To nie jest dobry pomysł.

Adres e-mail używany w celach służbowych/biznesowych często zawiera Twoje imię i nazwisko. Warto mieć **nieformalny adres mailowy**, który zapewni Ci większą [anonimowość w sieci](#). Ciekawym rozwiązaniem jest **Proton** – to cały ekosystem, którego celem jest zapewnienie użytkownikowi bezpieczeństwa podczas korzystania z sieci (dostępny również w opcji darmowej). Najbardziej ceniony jest [Proton Mail](#). To usługa, w której **każdy mail i załącznik jest zaszyfrowany** – odczyta go tylko zamierzony odbiorca. Proton korzysta z szyfrowania typu end-to-end (E2EE). E2EE uchodzi za **złoty standard zabezpieczenia komunikacji** w poczcie elektronicznej.

5. Skasuj niepotrzebne/nieużywane konta

Im więcej masz kont założonych na różnych serwisach, tym **większe ryzyko wycieku** Twoich danych. Większość z nas ma konta na stronach, z których już nie korzysta. Dobrym pomysłem jest ich skasowanie.

6. Uważaj na phishing i ransomware – podejrzane maile i SMS-y

Największym zagrożeniem w sieci jest [malware](#) czyli **złośliwe oprogramowanie**. Wśród takich programów prym wiodą ransomware i programy do phishingu.

7. Zainstaluj mocny program antywirusowy

Są osoby, które nie używają antywirusów. Jednak dla większości osób, to nie jest optymalne rozwiązanie. Antywirus da Ci spokojną głowę oraz **zabezpieczenie przed najbardziej popularnymi zagrożeniami**.

Dobrym pomysłem jest **przejrzenie testów programów antywirusowych** wykonanych przez niezależne laboratoria, m.in. AV-Comparatives i AV Test. Eksperci oceniają m.in. skuteczność ochrony, jak bardzo antywirus obciąża procesor komputera, jak często myli się ogłaszając fałszywe alarmy czy też jego zdolność obrony urządzenia przed zaawansowanymi atakami.

Inne kryteria wyboru to cena, dostępność na różne urządzenia i systemy operacyjne oraz **dodatkowe funkcje** oferowane przez producenta. Te dodatkowe funkcje to m.in. VPN, ochrona rodzicielska, menedżer haseł, szyfrowanie plików.

8. Używaj sieci Tor i/lub VPN

Sieć Tor to bardzo skuteczny sposób na bezpieczne i prywatne korzystanie z sieci. Zapytanie z komputera przechodzi przez kolejne węzły (serwery) i **jest szyfrowane**. Twój **adres IP jest maskowany**, a potencjalny obserwator nie wie jakie strony odwiedziłeś i co na nich robiłeś.

9. Unikaj przeglądania stron bez certyfikatu SSL

SSL to protokół sieciowy, który **służy do bezpiecznych połączeń** internetowych. Takie połączenia nawiązywane są przy użyciu certyfikatów – dlatego mówimy o **certyfikacie SSL**. Strony z takim certyfikatem poznasz na pierwszy rzut oka – mają w adresie URL oznaczenie **https://** oraz symbol kłódki (w przeciwieństwie do stron **http://**).

SSL szyfruje połączenie między serwerem, a przeglądarką **www**. **Chroni dane**, które podajesz na odwiedzanych stronach – od imienia i nazwiska, przed adres e-mail, po numer karty kredytowej – przed dostępem niepowołanych osób. Takich informacji nie należy podawać na stronach z **http** czyli bez certyfikatu.

10. Zwiększ ustawienia prywatności na swoich kontach w mediach społecznościowych

Z zasady osoby, które korzystają z mediów społecznościowych mają **ograniczoną prywatność**. Właściciele serwisów zbierają informacje na temat ich zachowania w sieci, a potem wykorzystują do targetowania reklam lub **sprzedają zewnętrznym marketerom**.

Jeżeli chcesz być bardziej bezpieczny – mniej narażony na szpiegowanie i precyzyjnie dobierane reklamy – możesz **ograniczyć zakres informacji** zbieranych o tobie przez Facebooka, Twittera, Tik Toka czy Instagram. Zrobisz to w ustawieniach prywatności.

Dobrym pomysłem jest również ograniczenie innym osobom możliwości **oznaczania Cię na zdjęciach lub w wydarzeniach**. Po wprowadzeniu zmian zatwierdzisz lub odrzucisz tagowanie. Sprawdź również, kto może widzieć Twoje posty i mieć dostęp do informacji o wspólnych znajomych.

Serwisy społecznościowe często zmieniają regulaminy i wprowadzają nowe zasady dotyczące prywatności użytkowników. Regularnie monitoruj, co zbierają o tobie serwisy społecznościowe i reaguj w razie konieczności.

11. Aktualizuj system operacyjny i programy

Jednym z poważniejszych zagrożeń w sieci są **złośliwe programy typu exploit**. To malware, które wyszukują luki w programach, a potem wykorzystują je do zainfekowania urządzenia innymi złośliwymi programami.

12. Zasztyfruj dysk komputera i laptopa, zabezpiecz router i sieć WiFi

Odpowiednie **zabezpieczenie urządzeń**, których używasz podczas korzystania z sieci, może przesądzić o bezpieczeństwie Twoich pieniędzy i danych.

Router to brama, która oddziela Twoją domową sieć od Internetu i czyhających w nim zagrożeń. Może być otwarta dla przestępców lub zamknięta i zabezpieczona solidnym zamkiem.

13. Zdobywaj wiedzę na temat bezpieczeństwa w sieci

Wiedza to potężna broń – to zasada dotyczy również bezpiecznego korzystania z Internetu. Dodam: aktualizowana wiedza.

Cyfrowy świat zmienia się każdego dnia. Informacje sprzed roku o cyberzagrożeniach i sposobach ich zwalczania mogą być dzisiaj nieskuteczne. Warto sprawdzać dobre serwisy, które na bieżąco informują o najważniejszych wydarzeniach ze świata cyberbezpieczeństwa.

Rozmawiaj z dorosłymi o internecie, powiedz dorosłemu, któremu ufasz, gdy coś w internecie cię zaniepokoi.

Za kontrolę tabletów, smartfonów używanych przez uczniów odpowiedzialni są rodzice/ prawni opiekunowie!

Monitoring stosowania Polityki

Osobą Odpowiedzialną za Politykę Ochrony Dzieci w szkole oraz za monitorowanie realizacji niniejszej Polityki jest wicedyrektor Krzysztof Lignar i pedagog szkolny Monika Harabasz.

Osoby, o których mowa w punkcie 1 prowadzą rejestr zgłoszeń, monitorują poziom realizacji polityki i reagują na naruszanie przyjętych w placówce standardów oraz proponują zmiany.

Zasady i sposób udostępniania rodzicom albo opiekunom prawnym lub faktycznym oraz małoletnim standardów w celu zaznajomienia się z nimi i ich stosowania

Polityka Ochrony Dzieci w Zespole Szkół Mechanicznych nr 3 w Krakowie jest dokumentem ogólnodostępnym. Każdy może się z nim zapoznać w dowolnej chwili.

Polityka Ochrony Dzieci jest dostępna w dzienniku elektronicznym Szkoły oraz w formie fizycznej w sekretariacie szkoły dla personelu placówki, rodzica małoletniego i samego małoletniego. Placówka udostępnia dwie wersje POD: podstawową oraz skróconą, dla małoletnich.

Wychowawcy klas mają obowiązek zapoznania uczniów ze Standardami, w tym procedur reagowania na krzywdzenie oraz przeprowadzenia zajęć dotyczących praw dziecka, przemocy rówieśniczej i jej skutków oraz zagrożenia bezpieczeństwa w internecie.

Pedagog szkolny/psycholog szkolny/ pedagog specjalny posiadają i udostępniają materiały informacyjne dotyczące instytucji pomocowych dla dzieci i dorosłych.