



Ministerstwo Edukacji Narodowej

Departament Innowacji i Rozwoju

DIR-WTC.053.4.2026.DBK

Warszawa, 17 września 2026 r.



Szanowny Panie,

w odpowiedzi na petycję w sprawie zwiększenia ochrony dzieci w przestrzeni internetowej uprzejmie wyjaśniam.

Ministerstwo Edukacji Narodowej (MEN) odgrywa kluczową rolę w tworzeniu ram polityki oświatowej, która uwzględnia zmieniające się warunki funkcjonowania dzieci i młodzieży w środowisku cyfrowym. Do zadań resortu edukacji i instytucji podległych należy zarówno kształtowanie podstaw programowych i dokumentów strategicznych, jak i wspieranie szkół oraz placówek doskonalenia nauczycieli w realizacji działań profilaktycznych, edukacyjnych i interwencyjnych.

Bezpieczeństwo dzieci i młodzieży, w tym także bezpieczeństwo cyfrowe, dla Ministra Edukacji ma znaczenie priorytetowe.

Działania Ministra Edukacji w zakresie przeciwdziałania zagrożeniom płynącym z cyberprzestrzeni koncentrują się na projektowaniu systemowych rozwiązań gwarantujących bezpieczne warunki kształcenia, wychowania i opieki oraz wspierania szkół i placówek systemu oświaty w realizacji zadań w tym obszarze.

Bezpieczne korzystanie z mediów i informacji, przeciwdziałanie dezinformacji oraz znajomość zasad bezpieczeństwa, odpowiedzialnego i bezpiecznego korzystania z zasobów edukacyjnych i urządzeń cyfrowych są kluczowymi zagadnieniami nie tylko dla uczniów, ale również dla nauczycieli i innych pracowników szkoły. Ważnym aspektem cyberbezpieczeństwa jest profilaktyka cyberprzemocy, kontaktu z niebezpiecznymi treściami, cyberuzależnień, świadomość zagrożeń i konsekwencji prawnych prowadzonej aktywności w Internecie oraz zagrożeń związanych z wizerunkiem online i prywatnością.

Warto podkreślić, że kryzys zdrowia psychicznego dzieci, młodzieży i dorosłych jest wynikiem wielu czynników, obok problemów emocjonalnych w domu i szkole, zaburzeń psychicznych, depresji, używania substancji psychoaktywnych, jednym z jego przyczyn jest nadmierowe korzystanie z mediów.

Wśród kierunków polityki oświatowej państwa, które wskazują dla jednostek systemu oświaty główne zadania do realizacji w danym roku, ustalono:

- w roku szkolnym 2025/2026: *Profilaktykę przemocy rówieśniczej. Zdrowie psychiczne dzieci i młodzieży, wsparcie w kryzysach psychicznych oraz Promowanie higieny cyfrowej i bezpiecznego poruszania się w sieci. Rozwijanie umiejętności krytycznej analizy informacji dostępnych w Internecie. Poprawne metodyczne wykorzystywanie przez nauczycieli nowoczesnych technologii, w szczególności opartych na sztucznej inteligencji oraz korzystanie z zasobów Zintegrowanej Platformy Edukacyjnej.*
- w roku szkolnym 2026/2027: *Promowanie higieny cyfrowej i aktywności off-line. Rozwijanie umiejętności bezpiecznego poruszania się w sieci i krytycznego myślenia, w tym odpowiedzialnego korzystania ze sztucznej inteligencji, a także korzystania*

z funkcjonalności i zasobów Zintegrowanej Platformy Edukacyjnej. Profilaktykę uzależnień behawioralnych i przeciwdziałanie przemocy rówieśniczej. Wspieranie zdrowia psychicznego dzieci i młodzieży oraz udzielanie pomocy w kryzysach psychicznych.

W odpowiedzi na rosnące zagrożenia cyfrowe podejmowane są działania, których celem jest budowanie odporności cyfrowej całych społeczności szkolnych. Ich skuteczność zależy nie tylko od systemowego ujęcia, ale także od możliwości wdrożeniowych na poziomie lokalnym i szkolnym.

W przyjętej przez Radę Ministrów we wrześniu 2024 r. Polityce Cyfrowej Transformacji Edukacji (PCTE)¹, która ma charakter dokumentu strategicznego, wyznaczającego ramy polityki państwa i działań podejmowanych w obszarze cyfryzacji edukacji w perspektywie krótko, średnio oraz długoterminowej, zagadnieniu cyberbezpieczeństwa poświęcono osobny rozdział – „Cyfrowe bezpieczeństwo”. Wskazano, w nim, że celem działań w obszarze edukacji jest sprawienie, by użytkownik Internetu rozumiał i krytycznie oceniał różne aspekty mediów i kontekstów medialnych oraz tworzenia komunikacji w różnych kontekstach, świadomie korzystał np. z komunikatorów, platform elektronicznych, portali społecznościowych oraz miał świadomość zagrożeń związanych z dostępem do określonych treści, a także ochroną danych osobowych, w tym wizerunku.

Wśród wskazanych w PCTE działań do zrealizowania w obszarze cyfrowego bezpieczeństwa można wymienić:

1. Wspieranie nauczania o edukacji medialnej, higienie cyfrowej i cyberbezpieczeństwie.
2. Opracowanie wytycznych dla nauczycieli i ram kompetencji uczniów w zakresie cyberbezpieczeństwa i higieny cyfrowej.
3. Opracowanie zasad systematycznego przeprowadzenia szkoleń dla nauczycieli i rodziców w zakresie cyberbezpieczeństwa.

Celem zaproponowanych w PCTE działań jest podniesienie świadomości, wiedzy i umiejętności całej społeczności szkolnej, w tym rodziców, w zakresie szeroko rozumianego cyberbezpieczeństwa.

Bezpieczeństwo w sieci, w mediach społecznościowych oraz edukacja medialna są stałymi i integralnymi elementami kształcenia ogólnego na każdym etapie edukacyjnym. Obowiązkowe cele kształcenia i treści nauczania, określone w podstawie programowej kształcenia ogólnego², są realizowane w szkołach podstawowych i ponadpodstawowych w sposób dostosowany do wieku, możliwości oraz potrzeb uczniów.

Treści zawarte w podstawie programowej kształcenia ogólnego w zakresie bezpieczeństwa cyfrowego i edukacji medialnej są obecne w edukacji wczesnoszkolnej, na języku polskim i przede wszystkim na informatyce, edukacji zdrowotnej, edukacji obywatelskiej oraz edukacji dla bezpieczeństwa, a także już na etapie wychowania przedszkolnego.

¹ Uchwała nr 98 Rady Ministrów w sprawie przyjęcia polityki publicznej pod nazwą „Polityka Cyfrowej Transformacji Edukacji” z dnia 12 września 2024 r. (M.P. z 2024 r. poz. 812).

² Rozporządzenie Ministra Edukacji Narodowej z dnia 14 lutego 2017 r. w sprawie podstawy programowej wychowania przedszkolnego oraz podstawy programowej kształcenia ogólnego dla szkoły podstawowej, w tym dla uczniów z niepełnosprawnością intelektualną w stopniu umiarkowanym lub znacznym, kształcenia ogólnego dla branżowej szkoły I stopnia, kształcenia ogólnego dla szkoły specjalnej przysposabiającej do pracy oraz kształcenia ogólnego dla szkoły policealnej (Dz.U. z 2017 r. poz. 356 z późn.zm.);

Rozporządzenie Ministra Edukacji Narodowej z dnia 30 stycznia 2018 r. w sprawie podstawy programowej kształcenia ogólnego dla liceum ogólnokształcącego, technikum oraz branżowej szkoły II stopnia (Dz.U. z 2018 r. poz. 467 z późn.zm.);

Rozporządzenie Ministra Edukacji z dnia 11 marca 2026 r. w sprawie podstawy programowej wychowania przedszkolnego oraz podstawy programowej kształcenia ogólnego dla szkoły podstawowej, w tym dla uczniów z niepełnosprawnością intelektualną w stopniu umiarkowanym lub znacznym (Dz.U. z 2026 r. poz. 378)

Od 1 września 2026 r. będzie obowiązywać nowa podstawa programowa wychowania przedszkolnego dla przedszkoli, oddziałów przedszkolnych w szkołach podstawowych oraz innych form wychowania przedszkolnego, która mówi m.in., że przedszkole zapewnia warunki do zdobywania i doskonalenia kompetencji niezbędnych m.in. do przygotowania się do funkcjonowania w społeczeństwie cyfrowym:

- dzieci nie są świadome zagrożeń, jakie niesie ze sobą korzystanie z nowych technologii, w tym z Internetu – dlatego w przedszkolu dzieci nie korzystają indywidualnie i samodzielnie z urządzeń ekranowych (z wyjątkiem dzieci ze specjalnymi potrzebami edukacyjnymi, które korzystają z racjonalnych usprawnień polegających na zastosowaniu takich urządzeń), a nauczyciel do celów dydaktycznych korzysta z nich tylko w niezbędnym zakresie, z zachowaniem ważnej dla prawidłowego rozwoju dziecka higieny cyfrowej; w przygotowaniu dzieci do bezpiecznego funkcjonowania w społeczeństwie cyfrowym aktywny udział muszą brać rodzice.

Na lekcjach języka polskiego uczniowie m. in. kształcą umiejętności rozumienia roli mediów oraz ich wpływu na zachowania i postawy ludzi, a także krytycznego odbioru przekazów medialnych, świadomego korzystania z nich oraz rozpoznawania manipulacji językowej, dezinformacji. Warunki i sposób realizacji tego przedmiotu wyraźnie podkreślają, że edukacja polonistyczna ma przygotować młodych ludzi do świadomego odbioru, krytycznej analizy i przetwarzania przekazów i komunikatów medialnych. Uczniowie powinni także rozumieć znaczenie i rolę mediów we współczesnym świecie, a także świadomie z nich korzystać.

Informatyka to przedmiot, który pozwala rozwijać kompetencje społeczne uczniów, czyli m.in. poznawać zagrożenia związane z powszechnym dostępem do technologii oraz do informacji, potrafić ocenić krytycznie informacje i ich źródła, pod względem rzetelności i wiarygodności w odniesieniu do rzeczywistych sytuacji oraz docenić znaczenie otwartych zasobów w sieci i korzystać z nich we właściwy sposób. Uczeń dowiaduje się jak bezpiecznie budować swój wizerunek w przestrzeni medialnej. Dowiaduje się jak postępować zgodnie z zasadami netykiety oraz regulacjami prawnymi dotyczącymi: ochrony danych osobowych, ochrony informacji czy prawa autorskiego i ochrony własności intelektualnej w dostępie do informacji i jest świadomy konsekwencji łamania tych zasad. Ponadto respektuje obowiązujące prawo i normy etyczne dotyczące korzystania i rozpowszechniania oprogramowania komputerowego, aplikacji cudzych i własnych oraz dokumentów elektronicznych. Stosuje dobre praktyki w zakresie ochrony informacji wrażliwych (np. hasła, pin).

Jednocześnie podczas zajęć z informatyki uczniowie zdobywają praktyczne umiejętności z zakresu programowania i podstaw programowania, rozwijają myślenie algorytmiczne oraz umiejętność rozwiązywania problemów z wykorzystaniem technologii cyfrowych. Uczą się także sprawnego i świadomego korzystania z e-usług oraz narzędzi cyfrowych wykorzystywanych w życiu codziennym, edukacji i przyszłej pracy, a także tworzenia i edytowania dokumentów, prezentacji, arkuszy kalkulacyjnych oraz innych zasobów cyfrowych. Dzięki temu przygotowują się do świadomego, odpowiedzialnego i efektywnego funkcjonowania w społeczeństwie cyfrowym.

Nowy przedmiot – edukacja zdrowotna, realizowany w szkołach podstawowych i ponadpodstawowych od 1 września 2025 r. jako przedmiot nieobowiązkowy, a od 1 września 2026 r. jako obowiązkowy, umożliwia uczniom uzyskanie i rozwijanie wiedzy, umiejętności i kompetencji społecznych pozwalających na trafne rozpoznanie potrzeb zdrowotnych własnych i otoczenia oraz podejmowanie odpowiednich działań profilaktycznych czy naprawczych.

Treści zawarte w podstawie programowej kształcenia ogólnego w zakresie nowego przedmiotu edukacja zdrowotna mają pełnić rolę prewencyjną, szczególnie w przypadku

przewidywanego możliwego pojawienia się u dzieci i młodzieży zachowań ryzykownych. Dział X dla szkół podstawowych oraz dział IX dla szkół ponadpodstawowych w całości poświęcony jest Internetowi i profilaktyce uzależnień. Uczy m.in.: przestrzegania zasad higieny cyfrowej; omawia: zagrożenia wynikające z niewłaściwego używania technologii informacyjno-komunikacyjnych, w tym, cyberprzemoc, hejt, mowę nienawiści, patostreaming, uzależnienie od gier i Internetu, niebezpieczne kontakty w sieci np.: uwodzenie w sieci; korzyści i zagrożenia związane z AI; zagrożenia związane z zażywaniem substancji psychoaktywnych oraz sposoby reagowania w sytuacjach występowania zagrożeń z korzystaniem z Internetu i substancji psychoaktywnych i ochronę prywatności, dezinformację, uzależnienia.

W ramach realizowanego od 1 września 2025 r. w szkołach ponadpodstawowych, nowego przedmiotu edukacja obywatelska uczniowie w ramach wymagań szczegółowych wyjaśniają wpływ mediów tradycyjnych i społecznościowych na przekonania i postawy opinii publicznej oraz funkcjonowanie społeczeństwa, państwa i demokracji oraz wyjaśniają zagrożenia związane z upowszechnianiem niesprawdzonych informacji.

Na przedmiocie edukacja dla bezpieczeństwa omawiane są treści dotyczące cyberbezpieczeństwa w wymiarze wojskowym. Uczeń poznaje istotę cyberbezpieczeństwa, cyberprzestępstwa, w tym cyberprzestępstwa militarne. Uczniowie są zachęceni do poszerzania wiedzy w tym zakresie. W szkole ponadpodstawowej uczniowie poznają znaczenie cyberprzemocy, poznają procedury postępowania w przypadku jej wystąpienia, wskazują niewłaściwe zachowania dotyczące cyberprzemocy i wiedzą, jaka powinna być na nie właściwa reakcja. Poznają znaczenie cyberzagrożeń w wymiarze cywilnym i potrafią je rozpoznać oraz znają procedury postępowania w przypadku ich wystąpienia.

Obecnie w Instytucie Badań Edukacyjnych trwają również prace eksperckie nad przygotowaniem projektu nowej podstawy programowej dla szkół ponadpodstawowych.

Jednocześnie mając na uwadze ochronę dzieci przed negatywnymi skutkami korzystania z Internetu oraz nowych technologii z dniem z dniem 1 września weszły w życie przepisy wprowadzające zakaz korzystania z telefonów komórkowych oraz innych urządzeń elektronicznych na terenie szkół podstawowych i przedszkoli³. Ustawa wprowadza zakaz korzystania z telefonów przez uczniów szkół podstawowych wraz z możliwością stworzenia miejsca lub miejsc ich przechowywania. W przypadku szkół ponadpodstawowych zasady używania (bądź całkowitego zakazu) urządzeń elektronicznych podczas pobytu w placówce zostaną określone w statucie szkoły. Przewiduje również wyjątki od powyższych zasad – m.in. ze względu na stan zdrowia, niepełnosprawność czy szczególne potrzeby ucznia, a także za zgodą nauczyciela w celach dydaktyczno-wychowawczych.

W ramach szkoleń dla nauczycieli realizowanych ze środków europejskich zarówno Krajowego Planu Odbudowy i Zwiększania Odporności (KPO) jak i Funduszy Europejskich na rzecz Rozwoju Społecznego (FERS) planowane jest do 2029 r. przeszkolenie ponad 100 tys. nauczycieli z umiejętności cyfrowych o różnym stopniu zaawansowania. Szkolenia oparte są na standardach kompetencji cyfrowych nauczycieli wypracowanych przez MEN, obejmujących m. in. kwestie związane z przepisami prawa, ochrona danych osobowych, i zasadami bezpieczeństwa dotyczącymi korzystania z zasobów dostępnych w sieci czy korzystania z mediów i informacji.

Mając na uwadze potrzebę stałego doskonalenia kompetencji nauczycieli, podległy Ministrowi Edukacji Ośrodek Rozwoju Edukacji (ORE) realizuje liczne szkolenia, konferencje i seminaria w zakresie działań wychowawczych i profilaktycznych.

³ Wprowadzony ustawą z 3 lipca 2026 r. o zmianie ustawy – Prawo oświatowe (Dz.U. z 2026 r. poz. 1036)

Na stronie Ośrodka Rozwoju Edukacji udostępniane są materiały informacyjne i publikacje dotyczące m.in. zagrożeń związanych z korzystaniem przez uczniów z nowych technologii komunikacyjnych oraz badań tego zagadnienia. Równocześnie na Zintegrowanej Platformie Edukacyjnej⁴ zgromadzono wiele zasobów nt. bezpiecznego korzystania z nowych technologii i internetu wśród dzieci i młodzieży. Materiały przeznaczone są dla nauczycieli w celu wsparcia i uatrakcyjnienia realizowanych przez nich zajęć.

Na stronie internetowej Ministerstwa Edukacji Narodowej dostępny jest poradnik *Bezpieczna szkoła. Zagrożenia i zalecane działania profilaktyczne w zakresie bezpieczeństwa fizycznego i cyfrowego uczniów*

Materiał to kompendium wiedzy na temat rozpoznawania sytuacji zagrożeń i reagowania na nie. Poradnik jest przeznaczony dla dyrektorów szkół, nauczycieli, rodziców i uczniów i obejmuje również zagadnienia bezpieczeństwa w cyberprzestrzeni.

Wśród zagadnień można wyróżnić np.:

- *Zagrożenia w świecie cyfrowym – procedury reagowania w przypadku wystąpienia zagrożenia cyfrowego,*
- *Podstawowe działania na rzecz bezpieczeństwa cyfrowego w szkole,*
- *Dostęp do treści szkodliwych, niepożądanych, nielegalnych – procedura reagowania,*
- *Dezinformacja, bezkrytyczna wiara w treści zamieszczone w internecie, nieumiejętność odróżnienia treści prawdziwych od nieprawdziwych, w tym szkodliwość reklam – procedury reagowania,*
- *Bezprawne użycie cudzego wizerunku w sieci – procedura reagowania,*
- *Niebezpieczne kontakty w internecie – procedura reagowania.*

Wszystkie szkoły w Polsce mogą korzystać z bezpłatnego, bezpiecznego i symetrycznego łącza o przepustowości minimum 100 Mb/s.

Projekt funkcjonuje na mocy ustawy z dnia 27 października 2017 r. o Ogólnopolskiej Sieci Edukacyjnej. Za kwestie techniczne i bezpieczeństwo odpowiada operator OSE – Naukowa i Akademicka Sieć Komputerowa (NASK – PIB). Do sieci OSE podłączonych jest już ponad 19 tys. szkół. Dzięki korzystaniu z OSE szkoły są chronione przed:

- szkodliwym oprogramowaniem i wirusami,
- atakami sieciowymi,
- treściami nielegalnymi i szkodliwymi (np. przemoc, pornografia).

Dyrektorzy szkół otrzymują raporty dotyczące wykrytych w sieci zagrożeń.

Z poważaniem

Tomasz Kulasa
Dyrektor
/ – podpisano cyfrowo/

⁴ <https://zpe.gov.pl/>