

**22. KONFERENCJA  
MIASTA  
W INTERNECIE**

GDAŃSK

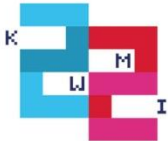
**27-29/06**

2018

# Puzzle

*Miasta przyszłości - Technologie transformacji - Cyfrowa szkoła*

# Cyfrowej Polski



22. KONFERENCJA  
MIASTA  
W INTERNECIE

# Puzzle Cyfrowej Polski

Miasta przyszłości – Technologie transformacji – Cyfrowa szkoła

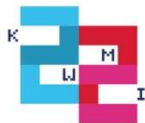


**Szkoła epoki smartfona – przeciwdziałanie zagrożeniom ze strony otoczenia cyfrowego.**

**Nowe obowiązki szkół i organów prowadzących wynikające z Prawa Oświatowego.**

**ARTUR KRAWCZYK**

STOWARZYSZENIE "MIASTA W INTERNECIE"




# Quiz!

Plickers

Bezpieczna | <https://www.plickers.com>

**plickers** Library Reports Classes Live View Cards Help A. KRAWCZYK

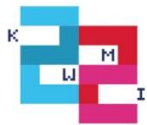


Plickers is a powerfully simple tool that lets teachers collect real-time formative assessment data without the need for technology.

Download on the **App Store**

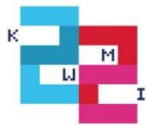
ANDROID APP ON **Google play**

**Pomoc**



# Dzieci w sieci – świat cyfrowy jest światem rzeczywistym, nie wirtualnym

- | **95% dzieci**, które jeszcze nie rozpoczęły nauki w szkole podstawowej, wychowuje się w rodzinach, posiadających dostęp do Internetu
- | Dzieci rozpoczynają korzystanie z Internetu **w coraz młodszym wieku**. W 2015 roku z Internetu (na ogół pod nadzorem rodziców) korzystało **21%** dzieci w wieku trzech lat (wzrost 100% od 2014)
- | **86 proc. rodziców lub dziadków**, mających dzieci lub wnuki w wieku od 6 do 19 lat, które pozostają z nimi we wspólnym gospodarstwie domowym deklaruje, że przynajmniej jedno z nich korzysta z Internetu
- | W populacji gimnazjalistów **wszyscy korzystają z Internetu** (0,7% nie korzysta w ogóle). **80 proc.** z nich korzysta z Internetu wiele **razy dziennie lub przez cały czas**.



# Dzieci w sieci – świat cyfrowy jest światem pierwszego wyboru

- | Zagrożenia wynikające z życia w sieci nie są wirtualne, lecz **realne**. Co więcej, jedno nakładają się na drugie, **wzmacniają się**, stają się jeszcze **bardziej niebezpieczne**.
- | Polskie szkoły **nie mają** wypracowanych, rutynowych metod reagowania w przypadku wystąpienia incydentu zagrożenia cyberbezpieczeństwa, co gorsza skłonne są bardzo często **bagatelizować** występujące zagrożenia (*zamiatanie pod dywan*)
- | Tymczasem, dla młodych ludzi świat Internetu jest światem **pierwszego wyboru** – nawet w sytuacjach społecznych/rodzinnych, **zachowują łączność z siecią i są w niej aktywni**.
- | Zmienia się zasadniczo **model behawioralny** ludzi młodych, prowadząc do reakcji **niezrozumiałych, nieakceptowalnych, „wynaturzonych”** w ocenie osób pokolenia „internetowych emigrantów”.

# Świat dorosłych próbuje radzić sobie ze *smombies*...



## Jak znika 24 letni Jonas?



**Bochum,**  
Niemcy



**Szanghaj,**  
Chiny



# Ustawa prawo oświatowe z 14 grudnia 2016r.

## Art. 1

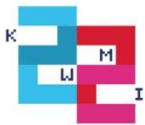
---

- Pkt 21** upowszechnianie wśród dzieci i młodzieży **wiedzy o bezpieczeństwie oraz kształtowanie właściwych postaw wobec zagrożeń, w tym związanych z korzystaniem z technologii informacyjno-komunikacyjnych**
- Pkt 22** kształtowanie u uczniów umiejętności sprawnego posługiwania się technologiami informacyjno-komunikacyjnymi

## Art.27

---

Szkoły i placówki zapewniające uczniom dostęp do Internetu są **obowiązane podejmować działania zabezpieczające uczniów przed dostępem do treści, które mogą stanowić zagrożenie dla ich prawidłowego rozwoju**, w szczególności zainstalować i aktualizować oprogramowanie zabezpieczające.



# MEN opracowało rekomendacje i procedury dla szkół oraz pracuje nad zmianami w prawie

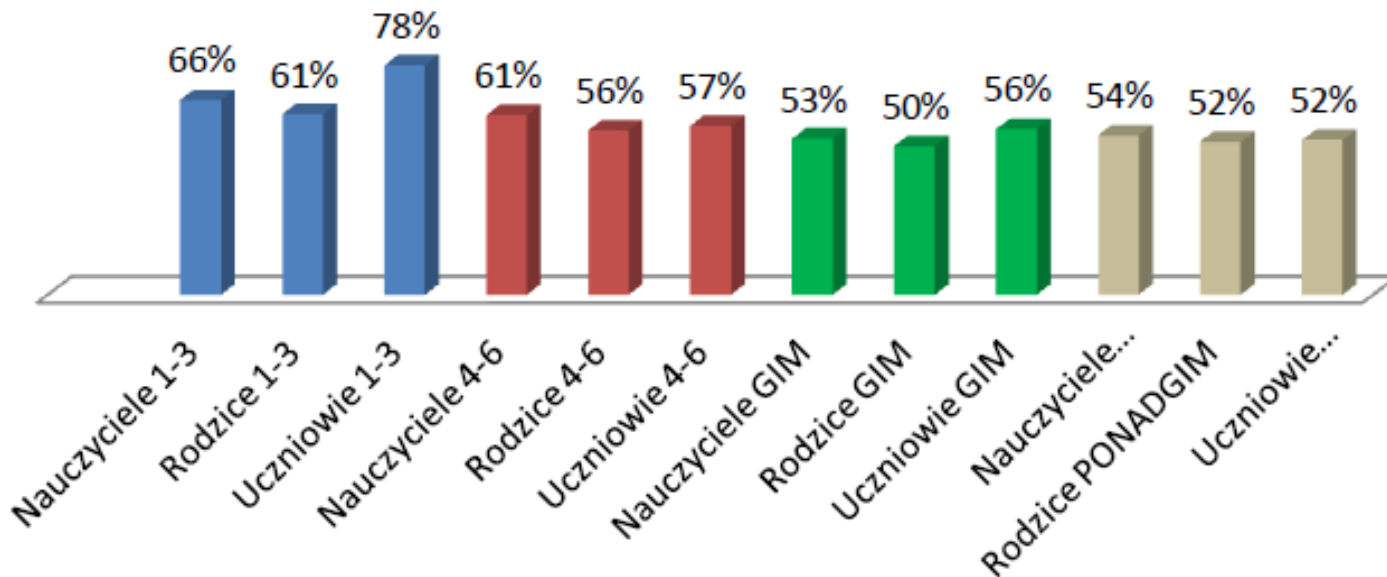
planowane są zmiany **w rozporządzeniu Ministra Edukacji Narodowej i Sportu w sprawie bezpieczeństwa i higieny w publicznych i niepublicznych szkołach i placówkach** dnia 31 grudnia 2002 r. (Dz. U. z 2003 Nr 6, poz. 69 z późn. zm.). Ostatnia zmiana: 22 lipca 2011 r – Dz. U. Nr 161, poz. 968)

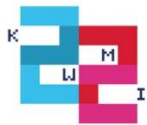
**zespół ekspertów** opracował **procedury na wypadek zagrożenia**, które w części odnoszą się do zagrożeń bezpieczeństwa cyfrowego, a także **rekomendacje profilaktyczne** – do realizacji w szkołach

## planowane wprowadzenie zmian

## rok szkolny 2017/2018

# Kompetencje w zakresie bezpieczeństwa cyfrowego nauczycieli, uczniów oraz rodziców są niskie i niewystarczające



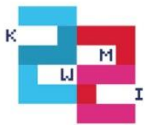


# Prawo nie wystarczy, konieczne działania profilaktyczne wprowadzone do rutyny szkolnej

Powstał **pakiet rekomendacji** dla dyrektorów szkół i grona pedagogicznego:

## 1. Opracowanie, realizacja i aktualizacja Szkolnego Planu Bezpieczeństwa Cyfrowego

- | element Programu Wychowawczo- Profilaktycznego szkoły
- | aktualizowana, np. co 3 lata, strategia bezpieczeństwa cyfrowego w szkole
- | przygotowanie przez całą społeczność szkolną – w tym rodziców (Rada Szkoły), uczniów (samorząd uczniowski)
- | jego elementem powinna być tzw. polityka bezpieczeństwa cyfrowego – dokument związany z zapewnieniem cyberbezpieczeństwa na poziomie technicznym
- | **polityka bezpieczeństwa cyfrowego** – opracowana w uzgodnieniu z organem prowadzącym oraz dokumentem: *BEZPIECZNA SZKOŁA CYFROWA - Zalecenia i rekomendacje dla samorządów - realizatorów projektów w ramach unijnej perspektywy budżetowej 2014-2020*:  
<https://www.cyfrowobezpiecni.pl/biblioteka-materialow/pobierz/123>

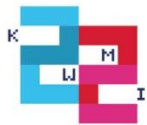


# Nowe działania w szkole, wplecione w codzienną praktykę dydaktyczną i aktywności środowiskowe

## 2. Działania wychowawcze i edukacyjne adresowane do uczniów

- | apele tematyczne – z udziałem gości
- | lekcje wychowawcze i komponenty lekcji przedmiotów przyrodniczych i humanistycznych
- | konkursy szkolne i udział w konkursach centralnych
- | zajęcia pozalekcyjne z udziałem gości, także akcje informacyjne w lokalnym środowisku
- | publikacja informacji w szkolnym serwisie www, gazetce szkolnej, plakaty
- | prelekcje i warsztaty ze specjalistami (Policja, edukatorzy)
- | wdrożenie i przećwiczenie procedur reagowania w wypadku zagrożenia cyberbezpieczeństwa
- | korzystanie z ofert edukacyjnych projektów realizowanych przez NGO
- | ważne tematy: prawo autorskie, fake news, cyberprzemoc, seksting

## 3. Wyłonienie z kadry szkolnej, powołanie przez dyrektora i przeszkolenie Szkolnego Mentora Bezpieczeństwa Cyfrowego, odpowiedzialnego za realizację planu.



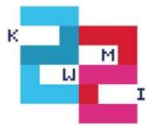
# Uruchomienie potencjału wychowawczego i edukacyjnego szkoły oraz działań środowiskowych

## 4. Nabycie przez dyrektorów, wszystkich nauczycieli i innych pracowników szkoły podstawowych kompetencji w zakresie bezpieczeństwa cyfrowego

- | szkolenia dla rad pedagogicznych – 4h
- | każdy nauczyciel powinien ukończyć **bezpłatne szkolenie** online:  
<https://www.cyfrowobezpieczni.pl/kursy-e-learningowe> lub inne np. w zasobach NASK
- | ogromne zasoby edukacyjne w Internecie, dostępne bezpłatnie.

## 5. Uwiadomienie rodzicom i opiekunom prawnym uczniów znaczenia działań wychowawczych z zakresu bezpieczeństwa cyfrowego

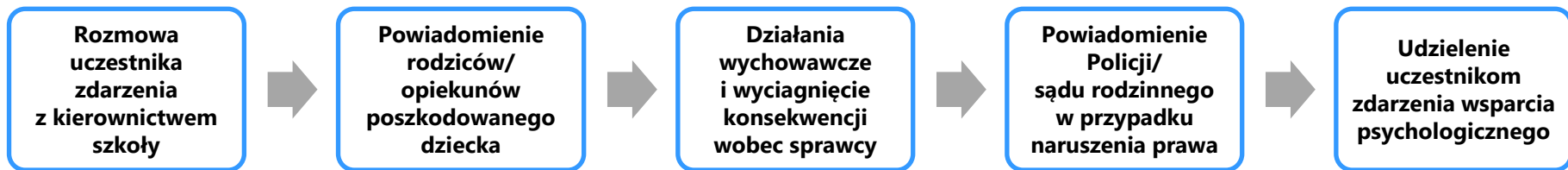
- | spotkanie na zakończenie roku
- | wywiadówki
- | informacje dystrybuowane przez e-dziennik
- | festyn szkolny i inne wydarzenia lokalne (współpraca na tym polu z innymi szkołami i NGO)

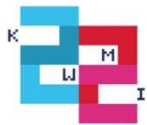


# Procedury reagowania w przypadku zagrożeń bezpieczeństwa cyfrowego w szkole

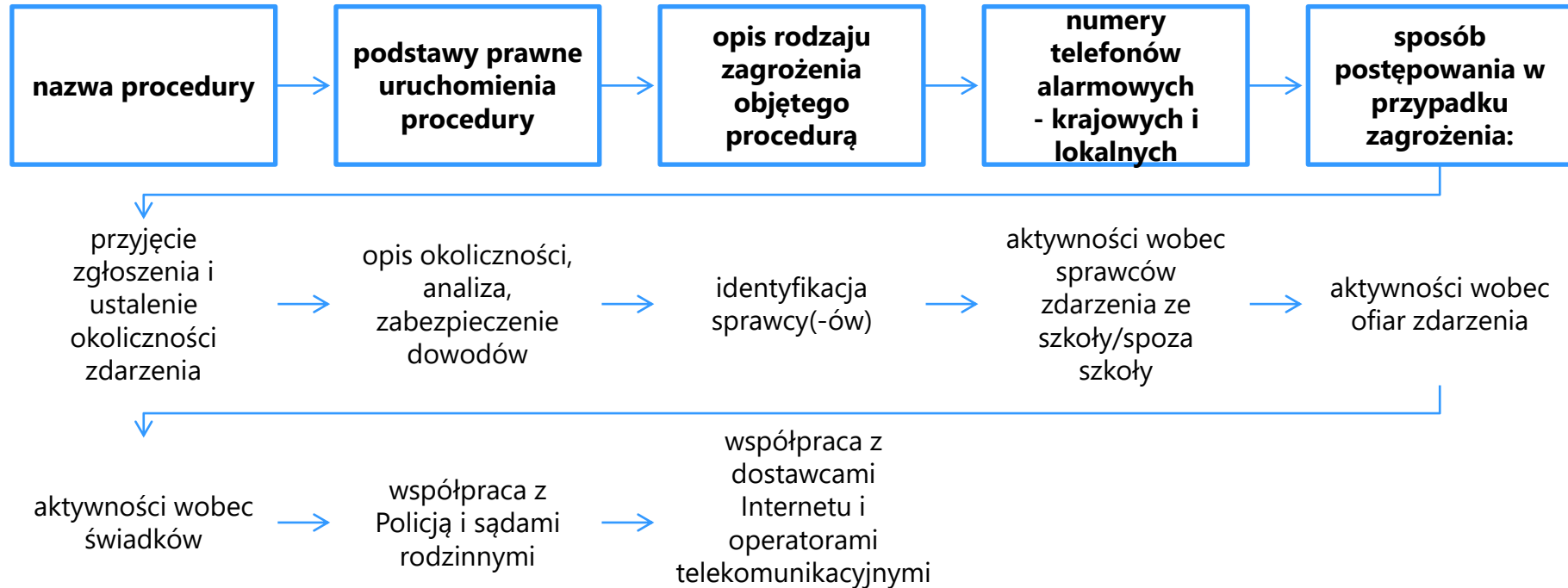
W ramach **prac zespołu** powołanego przez MEN wypracowano formalne procedury reagowania w przypadkach incydentów zagrożenia bezpieczeństwa cyfrowego. Odnoszą się one do **najważniejszych typów zagrożeń**.

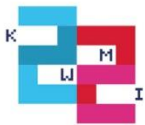
Na każdą z procedur składa się:





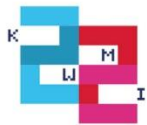
# Procedura to sformalizowane reguły rutynowego i wyćwiczonego postępowania w przypadku zagrożenia





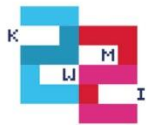
# Procedury reagowania w przypadku zagrożeń bezpieczeństwa cyfrowego ucznia (1)

- | **Dostęp do treści** szkodliwych, niepożądanych, nielegalnych publikowanych w Internecie (np. przemoc, pornografia, sekty, popularyzacja faszyzmu, nawoływanie do samokaleczeń, werbunek do org. Terrorystycznych, promowanie korzystania z narkotyków)
- | **Cyberprzemoc** - nękanie, straszenie, szantażowanie z użyciem sieci, publikowanie lub rozsyłanie ośmieszających, kompromitujących informacji, zdjęć, filmów z użyciem sieci oraz podszywanie się w sieci pod kogoś wbrew jego woli
- | **Naruszenia prywatności** dotyczące nieodpowiedniego lub niezgodnego z prawem wykorzystania danych osobowych lub wizerunku dziecka i pracownika szkoły (przestępstwo)
- | **Zagrożenia dla zdrowia dzieci** w związku z **nadmiernym korzystaniem z Internetu** - infoholizm (sieciholizm) – nadmierne, obejmujące niekiedy niemal całą dobę korzystanie z zasobów Internetu i gier komputerowych (najczęściej sieciowych) i portali społecznościowych przez dzieci



## Procedury reagowania w przypadku zagrożeń bezpieczeństwa cyfrowego ucznia (2)

- | **Nawiązywanie niebezpiecznych kontaktów w Internecie** - zagrożenie obejmuje kontakty osób dorosłych z małoletnimi w celu zainicjowania znajomości prowadzących do wyłudzenia poufnych informacji, nawiązania kontaktów seksualnych, skłonienia dziecka do zachowań niebezpiecznych dla jego zdrowia i życia lub wyłudzenia własności (np. danych, pieniędzy, cennych przedmiotów rodzinnych)
- | **Seksting, prowokacyjne zachowania i aktywność seksualna jako źródło dochodu osób nieletnich** - przesyłanie drogą elektroniczną lub publikowanie w portalach (społecznościowych) prywatnych treści, głównie zdjęć, o kontekście seksualnym, erotycznym i intymnym
- | **Bezkrytyczna wiara w treści zamieszczone w Internecie**, nieumiejętność odróżnienia treści prawdziwych od nieprawdziwych, bezkrytyczne uznawanie za prawdę też publikowanych w forach internetowych, kierowanie się informacjami zawartymi w reklamach
- | **Łamanie prawa autorskiego** - ryzyko poniesienia odpowiedzialności cywilnej lub karnej z tytułu naruszenia prawa autorskiego albo negatywnych skutków pochoptego spełnienia nieuzasadnionych roszczeń (tzw. *copyright trolling*)



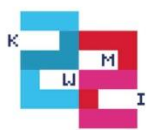
# Zalecenia odnośnie zagrożeń cyfrowego bezpieczeństwa technicznego w szkołach

Zawiera je III rozdział dokumentu *Bezpieczna szkoła cyfrowa. Zalecenia i rekomendacje dla samorządów - realizatorów projektów w ramach unijnej perspektywy budżetowej 2014-2020* zatwierdzonego przez MEN.

Rekomendacje odnoszą się do tematyki bezpieczeństwa technicznego:

- szkolnych sieci komputerowych i sieci dostępu do Internetu
- urządzeń cyfrowych – laptopów, tabletów, smartfonów, tablic multimedialnych
- systemów operacyjnych urządzeń cyfrowych
- korzystania z zasobów sieci w modelu chmury obliczeniowej
- oprogramowania edukacyjnego i funkcjonalnego

Konieczność zapewnienia profesjonalnego serwisu infrastruktury cyfrowej szkoły.



# Zaproponuj swoim uczniom grę edukacyjną na smartfon!

## CyberNinja

gra w formie quizu inspirowanego popularnym teleturniejem „Milionerzy”

## Defendix

gra skierowana do uczniów starszych, sprawdzająca ich wiedzę na temat bezpieczeństwa cyfrowego

## CyberClash

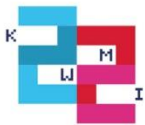
gra w formie quizu skierowana do najmłodszych przybliżająca podstawy bezpieczeństwa w sieci

## Obróńca sieci

Obróńca sieci – to gra zręcznościowa dzięki której gracze poznają niebezpieczeństwa czyhające w Internecie.

Wszystkie gry bezpłatnie do zainstalowania na smartfonach z systemem Android w Google Play oraz w serwisie <https://www.cyfrowobezpieczni.pl/biblioteka-materialow/gry>





# SMWI wspiera polskie szkoły w nabywaniu nowych kompetencji przez dyrektorów/nauczycieli

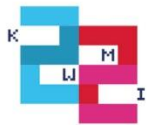
Prowadzimy szkolenia w **zakresie bezpieczeństwa cyfrowego dla Rad Pedagogicznych** (2h.)

Prowadzimy w szkołach stacjonarne szkolenia z **kompetencji metodyczno-cyfrowych**

- w modułach **8, 16 i 30 - godzinnych**
- w grupach **8-16 - osobowych**
- w warunkach korzystania ze sprzętu i oprogramowania **1 nauczyciel - 1 urządzenie**
- na terenie **szkoły** lub w innym miejscu wskazanym przez zamawiającego, posiadającym **odpowiedniej jakości dostęp do Internetu**

organizujemy **obozy edukacyjne dla nauczycieli - „edukampy”** - 5 dni, w grupach do 20 osób

organizujemy **„cyfrowe obozy”** dla klas szkół podstawowych, gimnazjów i liceów/techników – 7 dni, w Tarnowie (programowanie, robotyka, aplikacje edukacyjne, e-gry edukacyjne, gry miejskie, pływanie, wspinaczka, etc.)



# Dziękuję za uwagę i zapraszam do kontaktu!

**Artur Krawczyk**

[a.krawczyk@mwi.pl](mailto:a.krawczyk@mwi.pl)

+48 502 357 587

