

# KYBERBEZPEČNOST A KYBERPREVENCE V SOUVISLOSTI S INOVACEMI VE VZDĚLÁVÁNÍ

NÁRODNÍ PLÁN OBNOVY KOMPONENTA 3.1

**INOVACE** VE VZDĚLÁVÁNÍ V KONTEXTU **DIGITALIZACE**



STRATEGIE  
2030<sup>+</sup>

npi | Digi  
Koalice

MŠMT

MINISTERSTVO ŠKOLSTVÍ,  
MLÁDEŽE A TĚLOVÝCHOVY

PaedDr. Mgr. Anna Stočesová Martinková, Ph. D.  
vedoucí Oddělení podpory digitálního vzdělávání, vrchní ministerský rada MŠMT



Financováno  
Evropskou unií  
NextGenerationEU



NÁRODNÍ  
PLÁN OBNOVY



MINISTERSTVO ŠKOLSTVÍ,  
MLÁDEŽE A TĚLOVÝCHOVY

# Metodická podpora školám

## Digitalizujeme školu



edu.cz

### Podpora školám:



**Metodická podpora**  
digitalizujeme@msmt.cz



**IT guru <sup>npi</sup>**  
Konzultant pro školy



**Národní pedagogický institut ČR <sup>npi</sup>**  
projekt NPO 3.1 DIGI  
projekt NPO 3.1 AIDIG (v rámci DigCompEdu)



**Další podpora školám:**  
Umělá inteligence (AI), Kyberprevence,  
Projekt Albus

### Současně je zapotřebí se ve škole věnovat tématům:



**IT správa**  
Příručka pro ředitele  
k IT správě ve škole



**Bezpečná školní ICT**  
Edukační videa k bezpečné infrastruktuře



**Konektivita a bezpečnost**  
Standard konektivity a bezpečnosti školy v 21.  
století

# NÁRODNÍ PLÁN OBNOVY – KOMPONENTA 3.1

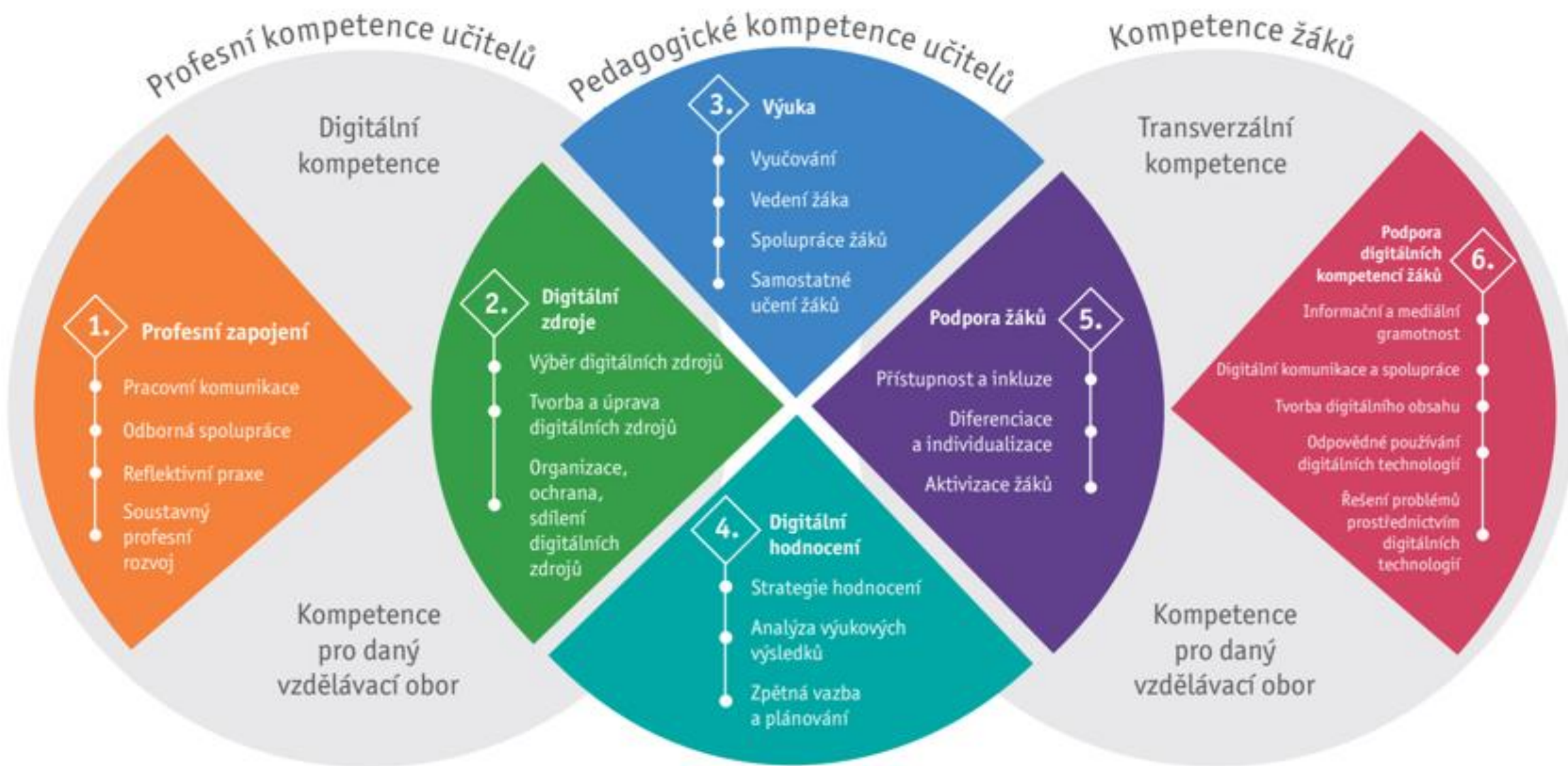
## POKRAČOVÁNÍ V ROZVOJI DIGITÁLNÍCH KOMPETENCÍ

### Projekt NPO 3.1 – **AIDIG** (1. 1. 2024 – 31. 1. 2026)

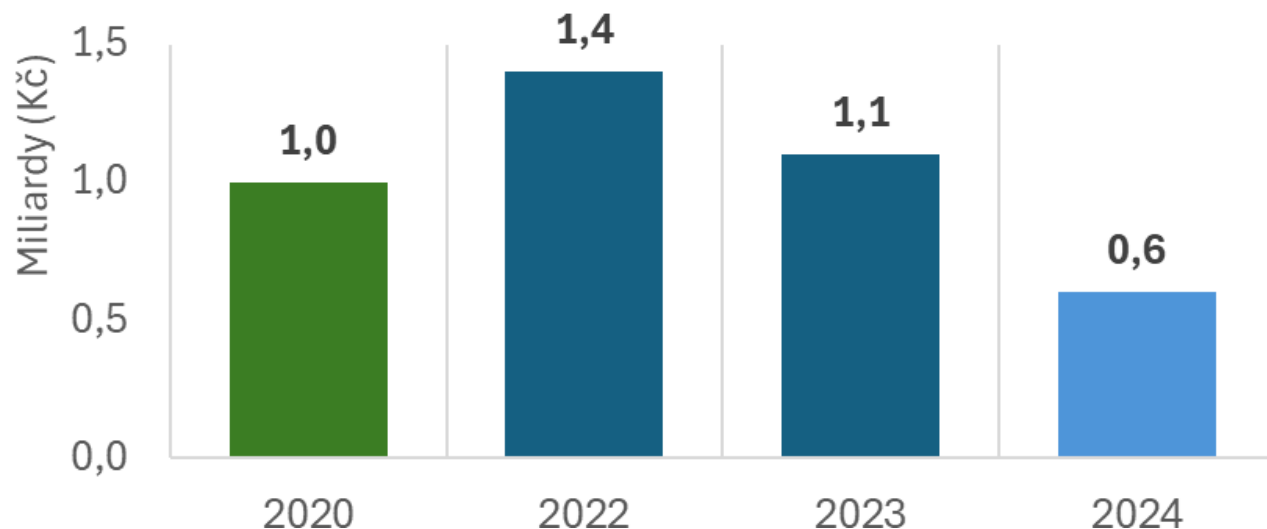
- Na základě výzvy MŠMT **DigCompEdu** realizuje NPI ČR **rozvoj digitálních kompetencí učitelů v MŠ, ZŠ a SŠ** podle evropského rámce DigCompEdu
- **Aktivity: pro lektory** (DigCompEdu kuchařka), kteří budou v navazující výzvě vzdělávat učitele, **pro učitele ZŠ a SŠ** aktuální témata AI ve výuce, dezinformace, mediální a finanční gramotnost, kyberbezpečnost, digitální wellbeing a digitální pedagogický leadership a metodická podpora a vzdělávání **pedagogů předškolního vzdělávání**

### Projekt NPO 3.1 **DIGI** (1. 1. 2022 – 31. 1. 2026)

§ Metodická podpora školám ke zdárné implementaci RVP: digitální platforma vzdělávacích zdrojů, kurzy, webináře, **AI**sborovny, **Kyber**sborovny... **IT guru**, KIM



# PŘÍMÁ FINANČNÍ INTERVENCE ŠKOLÁM (ALOKACE)



Next GenerationEU

Nástroj pro oživení a odolnost

Pilíř: Vzdělávání a trh práce

[edu.cz/digitalizujeme](https://edu.cz/digitalizujeme)



Financováno  
Evropskou unií  
NextGenerationEU



Financováno  
Evropskou unií  
NextGenerationEU



NÁRODNÍ  
PLÁN OBNOVY



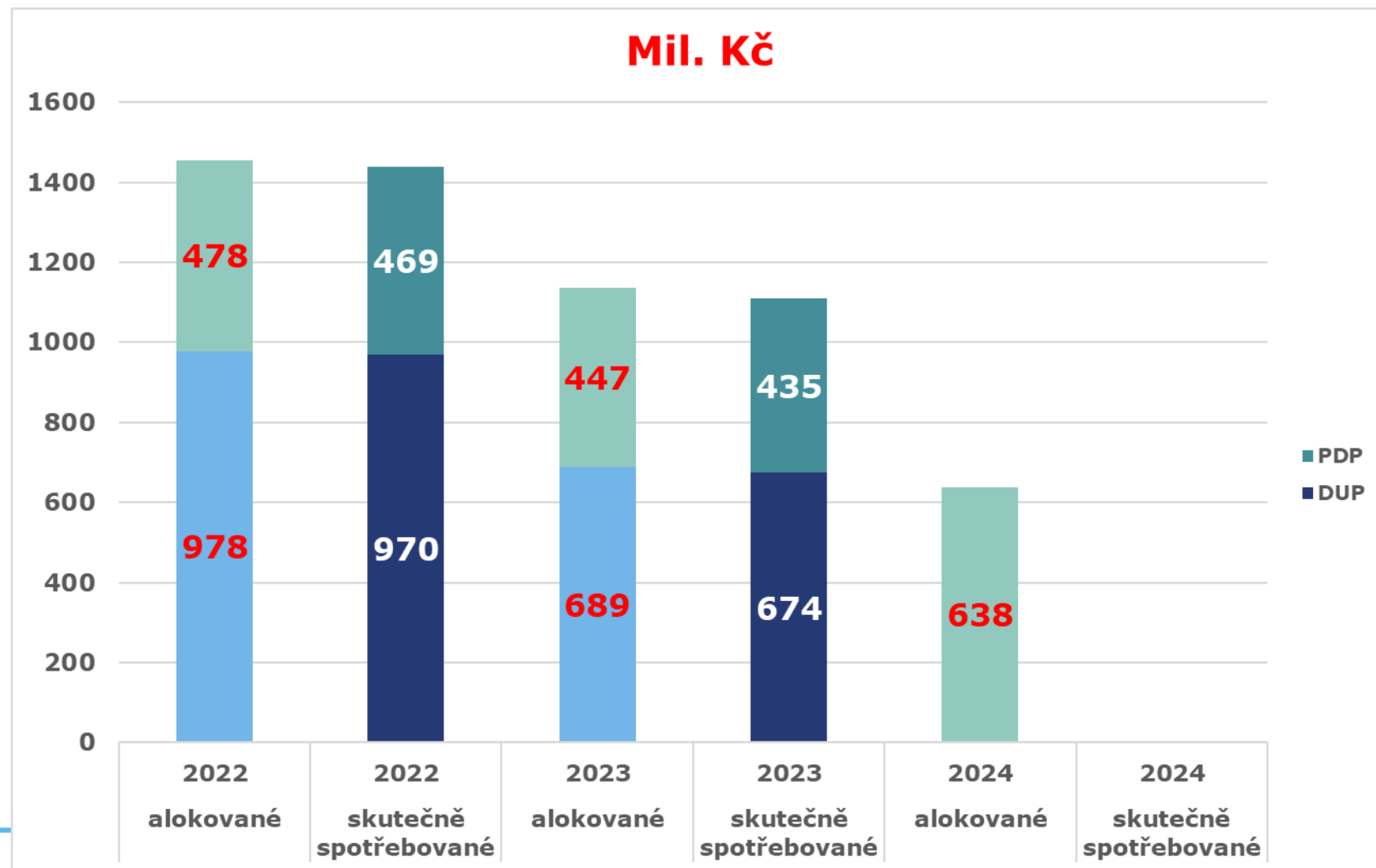
MINISTERSTVO ŠKOLSTVÍ,  
MLÁDEŽE A TĚLOVÝCHOVY

## Souhrn finančních prostředků

**alokovaných** na:

- prevenci digitální propasti
- pokročilé digitální učební pomůcky

**3,2 mld.  
Kč**





Financováno  
Evropskou unií  
NextGenerationEU



NÁRODNÍ  
PLÁN OBNOVY



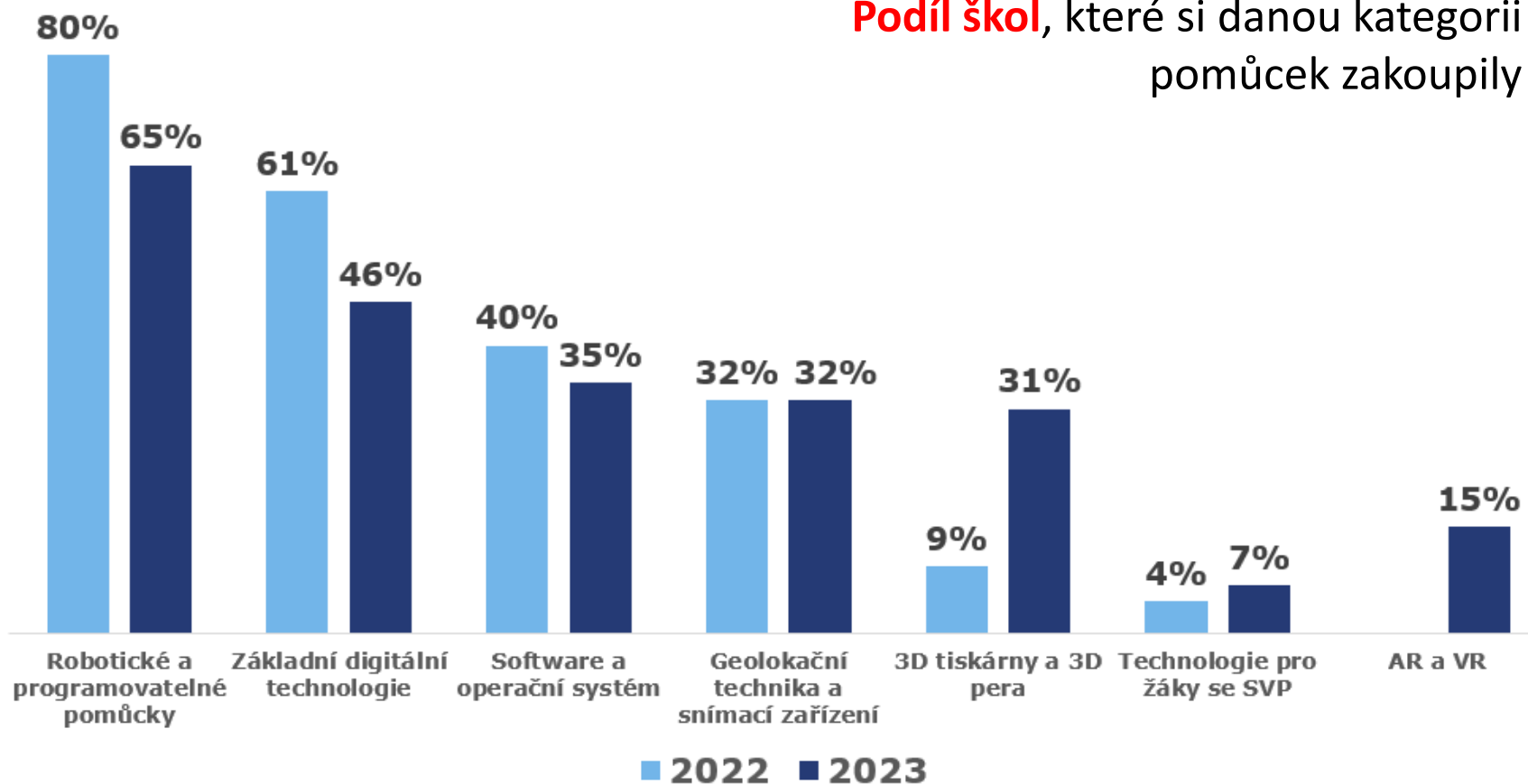
MINISTERSTVO ŠKOLSTVÍ,  
MLÁDEŽE A TĚLOVÝCHOVY

## POKROČILÉ DIGITÁLNÍ UČEBNÍ POMŮCKY

**Základní a střední školy** si v obou letech nejčastěji pořizovaly taktéž **robotické a programovatelné pomůcky**.

V roce 2023 se zvýšil podíl škol, které si pořizovaly **3D pomůcky**.

**Podíl škol**, které si danou kategorii pomůcek zakoupily



# Metodická podpora školám

Podpora školám:



Metodická podpora  
digitalizujeme@msmt.cz



IT guru **npi**  
Konzultant pro školy



Národní pedagogický institut ČR **npi**  
projekt NPO 3.1 DIGI  
projekt NPO 3.1 AIDIG (v rámci DigCompEdu)



Další podpora školám:  
Umělá inteligence (AI), Kyberprevence,  
Projekt Albus

Současně je zapotřebí se ve škole věnovat tématům:



IT správa  
Příručka pro ředitele  
k IT správě ve škole



Bezpečná školní ICT  
Edukační videa k bezpečné infrastruktuře



Konektivita a bezpečnost  
Standard konektivity a bezpečnosti školy v 21.  
století

## Digitalizujeme školu



edu.cz



MINISTERSTVO ŠKOLSTVÍ,  
MLÁDEŽE A TĚLOVÝCHOVY

MINISTERSTVO



# Bezpečná školní ICT infrastruktura – edukační videa

[edu.cz](#) > [Digitalizujeme školu](#) > [Bezpečná školní ICT infrastruktura – edukační videa](#)



## BEZPEČNÁ ŠKOLNÍ ICT INFRASTRUKTURA

**Bezpečná a kvalitní ICT infrastruktura** se stává v souvislosti s rychlým a rostoucím počtem **technologií do škol** zásadní a klíčovou oblastí. Školy začínají v současnosti stále častěji využívat **digitální zdroje** (digitální obsah, digitální nástroje, digitální hodnocení, administrativní aplikace apod.). To způsobuje, že se ve školských institucích, respektive v jejich datových a cloudových úložištích, začíná shromažďovat mnohem více **dat a informací** než v předchozích letech. Obzvláště distanční vzdělávání způsobilo nárůst dat z důvodů sdílené spolupráce v cloudových platformách pro vzdělávání. Učitelé během krátké doby zdigitalizovali své vzdělávací zdroje nebo je vytvořili samotní žáci. V této souvislosti je zapotřebí, aby školy věnovaly pozornost prevenci před kybernetickou kriminalitou, uvědomily si možná rizika, identifikovaly kritická místa ve své školní ICT infrastruktuře, vytvořily si preventivní bezpečnostní pravidla, aby hrozby byly předem identifikovány a předcházelo se vzniku kybernetickým útokům a zneužití.

Následující edukační videa mají pomoci školám k zajištění bezpečné a kvalitní ICT infrastruktury.


### Obsah

- Proč
- Cíl videí
- Seznam všech videí
  - 1. video: Bezpečná školní ICT infrastruktura (1. díl)
  - 2. video: Bezpečná školní ICT infrastruktura (2. díl)

## 2. video: Bezpečná školní ICT infrastruktura (2. díl)

Bezpečná školní ICT infrastruktura – nastavení a zabezpečení (2.díl)

Přehrát po... Sdílet 2/5



bezdátová síťová Wi-Fi zařízení

Využití síťové sítě protokol IEEE 802.11, pouze schválená zařízení?

Vysílá: YouTube

### 3. video: Plánování bezpečnostní politiky a bezpečnostní ICT checklist (1. díl)

Plánování bezpečnostní politiky a bezpečnostní ICT checklist (1.díl)

Přehrát po... Sdílet 3/5

**V bezpečnostní politice musí být jasně definováno:**

The diagram features a central shield with a red play button icon. Seven blue arrows radiate from the shield to seven text boxes, each describing a required element of a security policy:

- Pokyny pro vyžádání, schválení a zamítnutí vzdáleného přístupu.
- Zásady vzdáleného přístupu.
- Kdo má a nemá přístup k síti a za jakých podmínek.
- Definice zakázaných činností v ICT infrastruktuře.
- Informace o monitorování pohybu v ICT prostředí.
- Důsledky při porušování nastavených pravidel.
- Zveřejnění osoby odpovědné za prosazování bezpečnostní politiky.
- Kontaktní informace pro hlášení škodlivých a podezřelých aktivit.

Vysílá: YouTube



#### 4. video: Bezpečnostní ICT checklist (2. díl)

Bezpečnostní ICT check-list - základní klasifikace kybernetických útoků (2.díl)

**b) rozsáhlý incident**

- *menší závažnost kybernetických útoků*



Vysílá:  YouTube

Přehrát po... Sdílet 4/5

## 5. video: Bezpečnostní ICT politika a minimalizace rizik


Bezpečnostní ICT politika a minimalizace rizik.


Přehrát po... Sdílet 5/5

# Minimalizace rizik

### 1. Plánování bezpečnostních politik a bezpečnostní check-list

Má školské zařízení sestavený zvláštní tým pro nastavování bezpečnostních politik?  
Takový tým by měl být složen z následujících zástupců:

 zástupce vedení školy

 zástupce

DALŠÍ VIDEA

# Standard konektivity a bezpečnosti škol

[edu.cz](#) > [Digitalizujeme školu](#) > [Standard konektivity a bezpečnosti škol](#)



## KONEKTIVITA A BEZPEČNOST

V digitální transformaci je třeba školy podporovat a udělat maximum pro to, aby byla jejich **digitální infrastruktura funkční a bezpečná**. Funkční proto, aby byli učitelé motivováni využívat digitální technologie ve výuce a rozvíjet digitální gramotnost a inženýrské myšlení žáků. Bezpečná proto, aby školy uměly čelit hrozbám z vnějšího online světa. Podrobněji se kyberprevenci věnujeme také zde: [edu.cz/digitalizujeme/kyberprevence](#)

## MŠMT ve spolupráci s partnery zpracovalo a vydalo v roce 2022 STANDARD KONEKTIVITY ŠKOL

Dokument Standard konektivity škol definuje základní technická **kritéria cílového stavu školní síťové infrastruktury** a přijatelnosti **aktivit projektů** naplňující požadavky na školy v 21. století mj. i strategický **cíl Integrovaného regionálního operačního programu 2021-2027 4.1** v oblasti zajištění vnitřní konektivity škol a připojení k internetu – rozvoj vnitřní konektivity v prostorách škol a školských zařízení a připojení k internetu.

K tomuto dokumentu jsme zveřejnili také 3 metodické materiály:

- [Průvodce ke Standardu konektivity škol](#)
- [Prokázání a kontrola naplnění Standardu konektivity škol](#)
- [Bezpečná digitální infrastruktura školy](#)

Více ve článcích:

- [Vydán Standard konektivity škol \(4. 9. 2022\)](#)
- [Digitalizujeme školství: Standard konektivity pro školy \(21. 3. 2024\)](#)



V digitální transformaci je třeba školy podporovat a udělat maximum pro to, aby byla jejich **digitální infrastruktura funkční a bezpečná**. Funkční proto, aby byli učitelé motivováni využívat digitální technologie ve výuce a rozvíjet digitální gramotnost a informatické myšlení žáků. Bezpečná proto, aby školy uměly čelit hrozbám z vnějšího online světa. Podrobněji se kyberprevenci věnujeme také zde: [edu.cz/digitalizujeme/kyberprevence](https://edu.cz/digitalizujeme/kyberprevence)

### MŠMT ve spolupráci s partnery zpracovalo a vydalo v roce 2022 STANDARD KONEKTIVITY ŠKOL

Dokument Standard konektivity škol definuje základní technická **kritéria cílového stavu školní síťové infrastruktury** a přijatelnosti **aktivit projektů** naplňující požadavky na školy v 21. století mj. i strategický **cíl Integrovaného regionálního operačního programu 2021–2027 4.1** v oblasti zajištění vnitřní konektivity škol a připojení k internetu – rozvoj vnitřní konektivity v prostorách škol a školských zařízení a připojení k internetu.

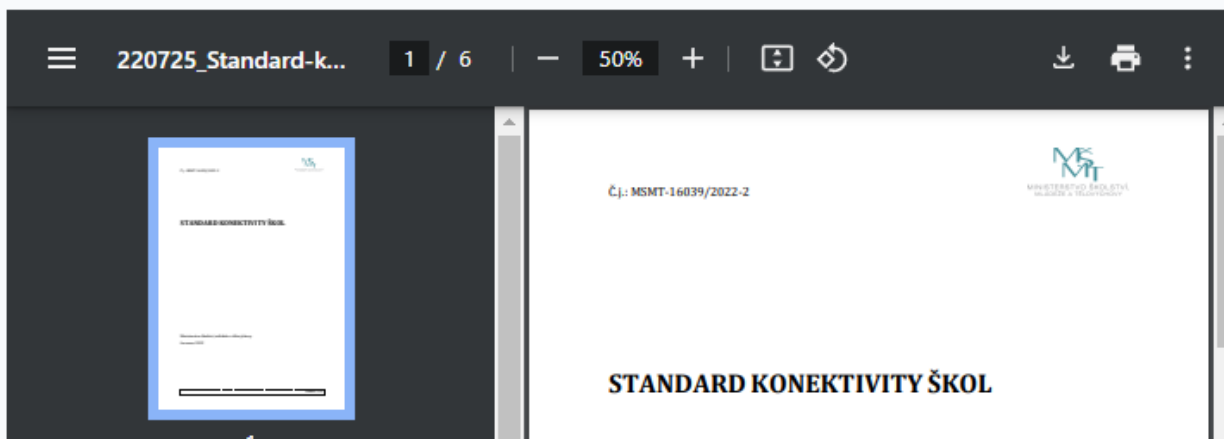
K tomuto dokumentu jsme zveřejnili také 3 metodické materiály:

- [Průvodce ke Standardu konektivity škol](#)
- [Prokázání a kontrola naplnění Standardu konektivity škol](#)
- [Bezpečná digitální infrastruktura školy](#)

Více ve článcích:

- [Vydán Standard konektivity škol \(4. 9. 2022\)](#)
- [Digitalizujeme školství: Standard konektivity pro školy \(21. 3. 2024\)](#)

Níže jsou anotace k metodickým materiálům a možnost stažení. Parametry konektivity uvedené ve Standardu konektivity škol jsou relevantní pro **základní školy, střední školy, vyšší odborné školy a konzervatoře**, u kterých Integrovaný regionální operační program 2021–2027 stanovuje ve specifickém cíli **4.1. intervenci v oblasti budování vnitřní konektivity škol**.

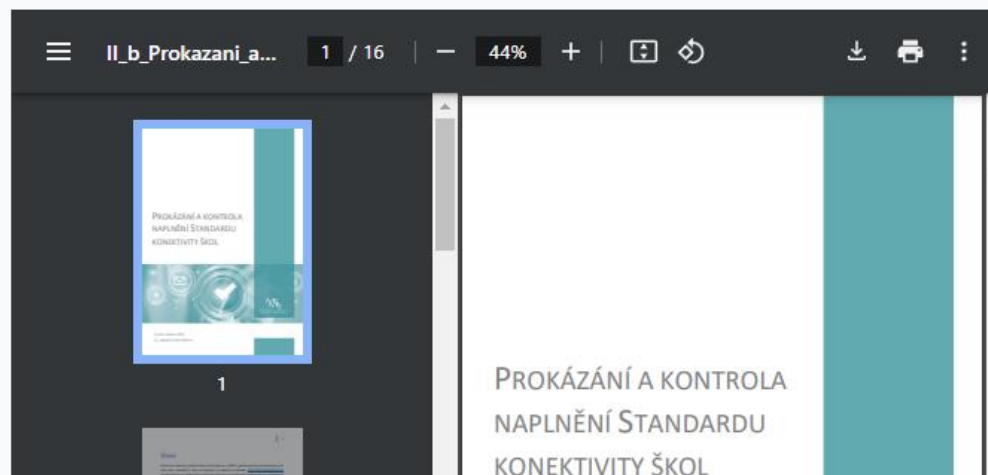




[220725\\_Standard-konektivity-skol\\_final](#) Stáhnout

## Prokázání a kontrola naplnění Standardu konektivity škol

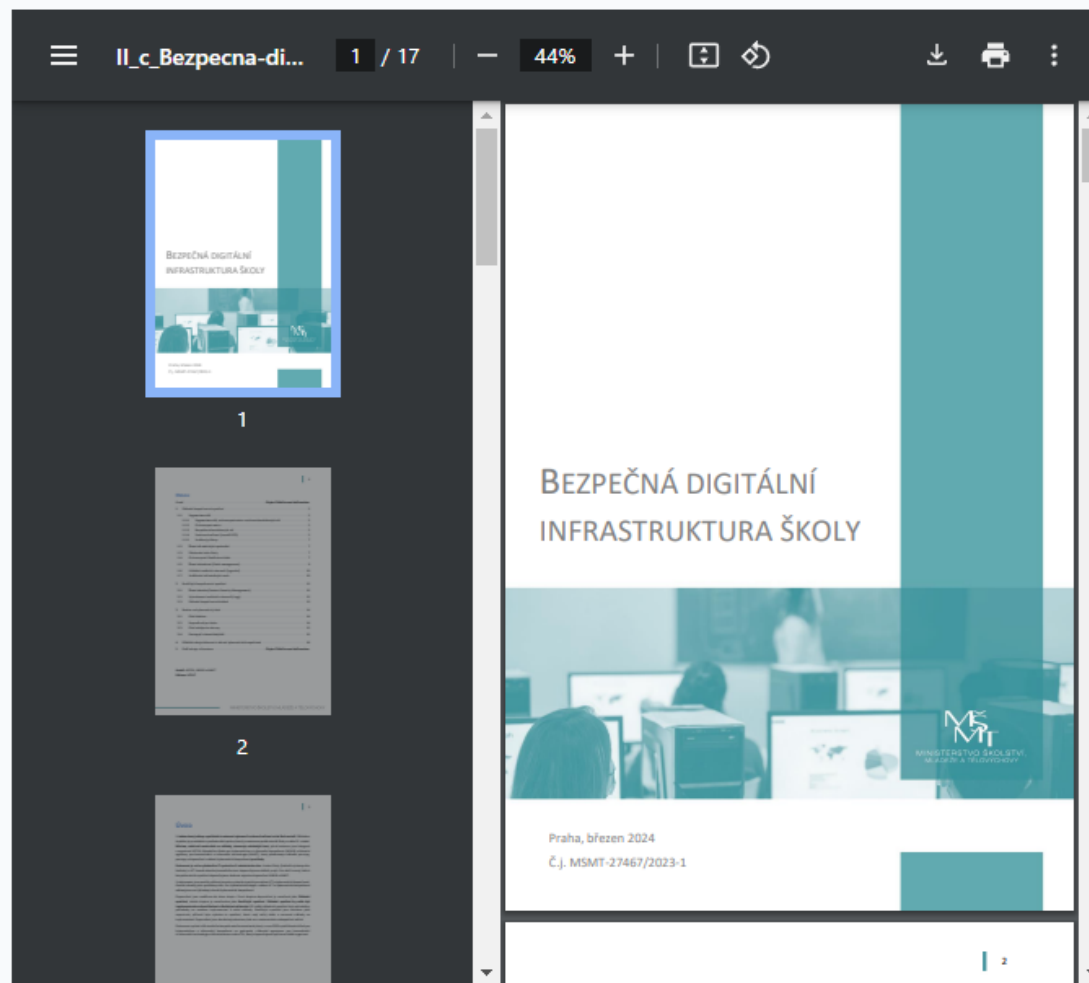
Jedná se o dokument pro všechny školy/příjemce, které mají prokázat naplnění parametrů uvedených ve Standardu konektivity škol.





## Bezpečná digitální infrastruktura školy

Kybernetická bezpečnost je v dnešní digitální době zásadním hlediskem pro každou instituci, včetně škol. Tento dokument představuje základní principy, postupy a doporučení v oblasti bezpečnosti školní digitální infrastruktury. Je určen především pro IT správce a administrátory, kteří mají za úkol zajistit, aby školní sítě a data byly chráněny před různými online hrozbami a útoky. Doplňkem jsou edukační videa BEZIT dostupná na <https://www.edu.cz/digitalizujeme/bezpecna-skolni-ict-infrastruktura/>



220725\_Standard-konektivity-skol\_finalStáhnout

# KURZ DÁVEJ KYBER

NŮKIB



Národní úřad  
pro kybernetickou  
a informační  
bezpečnost



MINISTERSTVO ŠKOLSTVÍ,  
MLÁDEŽE A TĚLOVÝCHOVY

## „DÁVEJ KYBER“ PRO UČITELE

Vítejte v otevřeném on-line kurzu základů kybernetické bezpečnosti, který  
je připravený na míru školnímu prostředí.

# KURZ DÁVEJ KYBER

NÚKIB



Národní úřad  
pro kybernetickou  
a informační  
bezpečnost

## Sociální sítě a věková hranice

Sociální média a aplikace mívají spodní věkovou hranici pro jejich využívání. Žáci ji často ignorují. Jaké to může mít důsledky?

Otevřít

## Nebezpečné výzvy

Výzvy mohou být úsměvné, ale i nebezpečné. Proč se mezi žáky těší oblibě, jak vznikají a na co se jako učitel soustředit?

Otevřít

## Kyberšikana ve třídě

Kyberšikana, která mívá až fatální následky, může vyburcovaný kolektiv chápat jako legraci. Na co dávat pozor?

Otevřít

## Kybergrooming a predátoři

Falešné profily vrstevníků, vydírání a manipulace jsou praktiky dospělých útočníků, se kterými se setkává mnoho dětí.

Otevřít

  
 MINISTERSTVO ŠKOLSTVÍ,  
 MLÁDEŽE A TĚLOVÝCHOVY

# KURZ DÁVEJ KYBER

NŮKIB



Národní úřad  
pro kybernetickou  
a informační  
bezpečnost

## On-line sexuální chování

Období dospívání je spojeno s objevováním sexuality. S tím však souvisí i sdílení intimních fotografií. Jak to s žáky řešit?

Otevřít

## Nenávist a on-line agrese

Žáci se na internetu mohou setkat s projevy nenávisti a on-line agrese. Je důležité zamezit tomu, aby takové chování přebírali.

Otevřít

## Digitální pohoda žáků

I když žákům ukazujeme rizika a nástrahy internetu, důležité je žáky nestrašit, vést je k uvědomění a digitální pohodě.

Otevřít

**MŠMT**  
MINISTERSTVO ŠKOLSTVÍ,  
MLÁDEŽE A TĚLOVÝCHOVY

# DĚKUJI ZA POZORNOST

[www.msmt.cz](http://www.msmt.cz)    [www.edu.gov.cz/digitalizujeme](http://www.edu.gov.cz/digitalizujeme)

[digitalizujeme@msmt.gov.cz](mailto:digitalizujeme@msmt.gov.cz)



MINISTERSTVO ŠKOLSTVÍ,  
MLÁDEŽE A TĚLOVÝCHOVY

PaedDr. Mgr. Anna Stočesová Martinková, Ph. D.  
vedoucí Oddělení podpory digitálního vzdělávání, vrchní ministerský rada MŠMT