



## **Cyfrowe portfolio**

**– bezpieczeństwo w komunikacji i w mediach**

**Warszawa, luty 2019**

## Sylabus

**opracowanie szkolenia:**

Artur Szczygieł-Ryss

**opieka merytoryczna:**

Grzegorz Cześnik - moderator

### A. Adresaci szkolenia

Szkolenie e-learningowe przeznaczone jest dla doradców zawodowych, doradców metodycznych i wszystkich nauczycieli, którzy chcą podnieść swoje kompetencje z zakresu bezpieczeństwa w komunikacji i w mediach.

### B. Zasady rekrutacji

Zgłoszenia będą przyjmowane przez system rekrutacji ORE – [www.szkolenia.ore.edu.pl](http://www.szkolenia.ore.edu.pl).

Po weryfikacji i akceptacji zgłoszeń uczestnicy otrzymają drogą mailową zaproszenia do udziału w kursie wraz z instrukcją logowania na platformie e-learningowej ORE ([www.e-kursy.ore.edu.pl](http://www.e-kursy.ore.edu.pl)). **Rekrutacja prowadzona jest w sposób ciągły i zakończy się 01.05.2019 r.**

### C. Cele szkolenia

Rozwój umiejętności związanych z bezpiecznymi i zdrowymi sposobami komunikowania się w Internecie i korzystaniem z mediów.

### D. Sposób pracy uczestnika i organizacja kursu

W trakcie całego kursu uczestnik towarzyszy rodzinie Lawendowskich. Ta czteroosobowa rodzina uczy się razem z uczestnikiem, zgłasza swoje wątpliwości, pytania, czasem wchodzi z uczestnikiem w dialog. Lawendowscy bardzo chcą się uczyć, są otwarci na eksperymenty i pokonywanie trudności, nie można im również zarzucić braku poczucia humoru. Kochają Internet. Każdy z Lawendowskich ma trochę inne podejście do Internetu i inne zainteresowania. W pierwszym module kursu uczestnik poznaje Lawendowskich i ich

specyfikę. **Zadaniem uczestnika jest zdobywać umiejętności i pomagać Lawendowskiemu<sup>1</sup> w zdobywaniu nowych kompetencji.**

W toku całego kursu uczestnik, wraz z Lawendowskimi, będzie mieć za zadanie:

- ✓ **wykonać zadania samokształceniowe wynikające z toku kursu** mające na celu podjęcie przez uczestnika praktycznej aktywności i utrwalenie umiejętności – wykonanie tych zadań warunkuje nabycie odpowiednich kompetencji;
- ✓ **wykonać test końcowy** złożony z 20 pytań w czasie 60 minut przy minimum 75% prawidłowych odpowiedzi.

Do testu można podejść trzykrotnie. Trzecia nieudana próba rozwiązania testu końcowego będzie skutkować niezaliczeniem szkolenia.

Na zakończenie szkolenia uczestnicy proszeni są o wypełnienie ankiety ewaluacyjnej.

Szkolenie prowadzone jest metodą e-learningową i ma charakter samokształceniowy.

Osoby uczestniczące w szkoleniu mogą w wybranym przez siebie tempie realizować treści kształcenia i zaliczyć test końcowy.

## E. Treści kształcenia

Treści kształcenia zawierają się w czterech częściach:

1. Dotyczące ochrony informacji i danych na swój temat. Umiejętności anonimizacji i rozumienia konsekwencji związanych z brakiem anonimowości.
2. Dotyczące zabezpieczania własnej komunikacji w Internecie w związku z korzystaniem z różnorodnych usług i mediów.
3. Dotyczące rozumienia specyfiki korzystania z urządzeń mobilnych i potencjalnie wynikających z tego konsekwencji.
4. Dotyczące nawyków reagowania na różnorodne wydarzenia w sieci i zachowania innych użytkowników i nawyków dotyczących zdrowia.

---

<sup>1</sup> Z rodziną Lawendowskich uczestnik może spotkać się również w kursie „Korzystanie z informacji” na platformie ORE

## F. Treści kształcenia w ramach poszczególnych modułów

**Moduł 01. Anonimizacja** – zrozumienie specyfiki funkcjonowania Internetu, sieci komputerowych i wynikających z tego problemów z anonimowością, narzędzia do ochrony danych, narzędzia do anonimizowania swojej obecności w Internecie.

**Moduł 02. Hasła i logowanie** - metody tworzenia mocnych haseł, jako techniki zabezpieczania swoich danych i dostępu do usług internetowych.

**Moduł 03. Phishing** – mechanizm oszustw w Internecie, diagnozowanie i przeciwdziałanie oszustwom i utracie danych i środków finansowych.

**Moduł 04. Utrata danych** – inne mechanizmy utraty danych, świadomego lub nieświadomego przekazywania i udostępniania danych na swój temat.

**Moduł 05. Szyfrowanie** – szyfrowanie danych i informacji w komunikacji i na urządzeniach mających dostęp do Internetu, oprogramowanie szyfrujące i sposoby szyfrowania.

**Moduł 06. Netykieta i hejt** – zasady zachowania się w Internecie w komunikacji z internautami i zagrożenia z tego wynikające, cyberprzemoc i mowa nienawiści, opis zjawiska i sposoby radzenia sobie z hejtem.

**Moduł 07. Uzależnienie** – jako zjawisko towarzyszące powszechnemu dostępowi do Internetu i różnorodnych urządzeń TIK, mechanizm i specyfika uzależnienia, fonoholizm, pomoc osobom uzależnionym.

## G. Efekty:

Po ukończeniu szkolenia osoba uczestnicząca w kursie będzie:

- rozumieć specyfikę komunikacji w sieci pod kątem ochrony danych i przesyłanych informacji,
- znać narzędzia do zabezpieczania się przed różnorodnymi negatywnymi zjawiskami w sytuacjach komunikacji związanymi z technologią i z relacjami z innymi użytkownikami,
- znać zasady zdrowego, bezpiecznego i przyjaznego korzystania z sieci i z mediów.

## H. Czas trwania szkolenia

Szkolenie e-learningowe realizowane będzie od 15.02.2019 r. do 15.05.2019 r. Na szkolenie można zapisać się najpóźniej do dnia 01.05.2019 r. Zaświadczenia dla uczestników spełniających warunki zaliczenia będą dostępne w koncie Uczestnika na platformie [www.szkolenia.ore.edu.pl](http://www.szkolenia.ore.edu.pl) do samodzielnego pobrania i wydrukowania po 20.05.2019 roku.

Orientacyjny czas przewidziany na pracę własną osób biorących udział w szkoleniu to 60 godzin (realizacja każdego z siedmiu modułów oraz czas przeznaczony na wykonanie poszczególnych zadań, zadania głównego i testu końcowego).

## I. Wsparcie w trakcie szkolenia

### Kierownik kursu:

Paweł Stępniać (mail: [pawel.stepniak@ore.edu.pl](mailto:pawel.stepniak@ore.edu.pl))

### Koordynator i moderator kursu:

Grzegorz Cześnik – (mail: [grzegorz.czesnik@hotmail.com](mailto:grzegorz.czesnik@hotmail.com))

### Wsparcie techniczne:

Zespół Wydziału Rozwoju Kompetencji Kluczowych ORE ([wrkk-tech@ore.edu.pl](mailto:wrkk-tech@ore.edu.pl))

## J. Narzędzia stosowane podczas szkolenia

1. Platforma e-learningowa online.
2. Edytor tekstu (np. MS Word, Wordpad, itp.).
3. Poczta elektroniczna.
4. Przeglądarka internetowa – zalecana Mozilla Firefox (minimum wersja 58.0), Chrome (minimum wersja 64.0).
5. Edytor prezentacji (np. MS PowerPoint, itp.).
6. Przeglądarka dokumentów pdf (np. Acrobat Reader, itp.)
7. Dowolna przeglądarka plików graficznych