

*Fisa de lucru***“Decalogul Securitatii Digitale”**

## Instrucțiuni pentru un nivel mai ridicat de securitate

- ✓ Alege o **parola** sigura. Folosește o combinație de cel puțin șase numere, litere și semne de punctuație (cum ar fi “!” sau “&”). Parola trebuie să fie diferită de alte parole pe care le-ai folosit pe Internet.
- ✓ Schimba parola periodic, mai ales dacă vezi un mesaj care îți cere să faci asta. În timpul controlului automat de securitate, uneori Instagram retrage accesul la informațiile care au fost furate de pe alte site-uri. Dacă Instagram descoperă că parola ta ar fi putut fi furată, schimbarea parolei pe Instagram sau alte site-uri, ajută la protejarea contului tău și previne atacul hackerilor pe viitor.
- ✓ Nu spune niciodată parola unei persoane necunoscute sau uneia în care nu ai încredere.
- ✓ Asigura-te că ai un cont e-mail protejat. Persoanele care îți pot citi e-mailurile, pot, de asemenea, să-ți acceseze contul.
- ✓ Deconectează-te de la media socială când folosești un computer sau smartphone cu care lucrează și alte persoane. Nu bifa casuta “Ține-mă minte” când te conectezi la un computer public, deoarece accesul tău va fi păstrat chiar dacă închizi fereastra de căutare (browser window)
- ✓ Personalizează-ți setările de confidențialitate a mediei sociale pe care o folosești.
- ✓ În unele cazuri este mai util să selectezi din modul de căutare anonim sau confidential, pentru protejarea informațiilor bancare pentru plăți sau informații personale – cum ar fi detalii de logare în media socială, ori de câte ori computerul este utilizat de mai multe persoane sau când este supus la risc de furt.
- ✓ Informează-te dacă contul tău este public sau privat și cum vor fi diseminate/răspândite conținuturile.
- ✓ Închide funcția locație geografică a smartphone-ului tău dacă nu vrei ca alții să știe unde te afli.

## Comportamente adecvate

- ✓ Dacă cineva a distribuit fotografii/video care te deranjează, poți să ștergi sau să blochezi persoana. Poți, de asemenea, raporta conținuturi neadecvate direct din aplicație, dacă ești convins că acestea violează principiile aplicației.
- ✓ Asigura-te că nu ai probleme dacă fotografiile/video pe care le postezi și le distribuie arată cine ești, unui public mult mai mare decât dorești (cum ar fi părinți, profesori, sau viitori angajați).
- ✓ Reflectează mult înainte de a autoriza aplicații de la terți (intermediary)
- ✓ Nu accepta niciodată să faci sau să distribuie ceva ce te face să te simți jenat.
- ✓ Dacă ești agresat, cere ajutorul familiei sau al unui profesor de încredere. Poți, de asemenea, să ștergi comentariile la o fotografie pe care ai distribuit-o și să raportezi acte de violență și intimidare la Centrul de ajutor pentru media socială
- ✓ Cere permisiunea înainte de a posta fotografii cu alte persoane