

Załącznik nr 6. Zasady bezpieczeństwa cyfrowego i reagowania na cyberprzemoc

Dla uczniów

- nie nagrywaj innych bez zgody i nie publikuj materiałów, które mogą ich ośmieszyć lub narazić;
- nie wysyłaj nikomu swoich haseł, kodów, intymnych zdjęć ani danych logowania;
- nie odpowiadaj na szantaż samodzielnie; zachowaj dowody i pokaż je zaufanemu dorosłemu;
- nie przysyłaj dalej krzywdzącego materiału, nawet aby „pokazać, co się stało”;
- w razie przejęcia konta zmień hasło, wyloguj inne sesje i zgłoś incydent.

Dla personelu - procedura

1. Sprawdź, czy istnieje bezpośrednie zagrożenie i czy dziecko potrzebuje natychmiastowej pomocy.
2. Zabezpiecz dowody bez dalszego rozpowszechniania: zrzuty, linki, identyfikatory kont, daty i opis kontekstu.
3. Zablokuj dostęp sprawcy w zakresie możliwym organizacyjnie, zgłoś treść platformie i administratorowi szkolnemu.
4. Poinformuj Koordynatora i rodzica bezpiecznego, chyba że rodzic jest podejrzanym lub kontakt zwiększa ryzyko.
5. Zawiadom Policję lub prokuraturę przy groźbach, szantażu, seksualnym wykorzystaniu, materiałach intymnych dziecka, uporczywym nękanii lub innych znamionach przestępstwa.
6. Ustal plan wsparcia i monitoruj odwet, wykluczenie oraz dalsze publikacje.