

AI SAFE



S SENSE CHECK

- **AI can sound confident and still be wrong. Don't trust answers just because they sound smart.**
- **AI outputs can be flawed or tricked. Code and info may hide mistakes or be manipulated.**
- **Pause. Check. Verify. Always double-check before you use, share, or act on it.**

A ASSESS DATA

- **AI runs on data you give it. What you type in can be stored or shared.**
- **Public AI tools aren't private. Don't put in personal, school, or sensitive info.**
- **Think before you share. Protecting data = using AI responsibly.**

F FOLLOW THE FLOW

- **AI tools are connected behind the scenes. They often talk to other systems you can't see.**
- **One answer can come from many AIs. Info gets passed along a chain, not just one tool.**
- **Trust isn't just one app. Risks can come from anywhere in that hidden chain.**

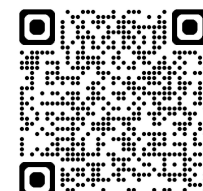
E EVALUATE ACTIONS

- **AI can now act, not just answer. Some systems do things for you without checking every step.**
- **Automation doesn't remove responsibility. If AI acts in your name, you're still accountable.**
- **Stay alert, even when AI runs alone. Oversight and thinking matters, every time.**



CYBERFIRST
WALES

cyberfirstwales.co.uk



AI SAFE



S SENSE CHECK / Gwirio'n feirniadol

- Gall AI swnio'n hyderus ac eto fod yn anghywir. Peidiwch ag ymddiried mewn atebion dim ond am eu bod yn swnio'n glyfar.
- Gall allbynnau AI fod yn ddiffygiol neu gael eu twyllo. Gall cod a gwybodaeth guddio camgymeriadau neu gael eu trin.
- Seibiwch. Gwiriwch. Dilyswch. Gwiriwch bob amser cyn ei ddefnyddio, ei rannu, neu weithredu arno.

A ASSESS DATA / Aseu data

- Mae AI yn rhedeg ar ddata rydych chi'n ei roi iddo. Gall yr hyn rydych chi'n ei deipio gael ei storio neu ei rannu.
- Nid yw offer AI cyhoeddus yn breifat. Peidiwch â rhoi manylion personol, gwybodaeth ysgol, na data sensitif i mewn.
- Meddyliwch cyn rhannu. Mae diogelu data = defnyddio AI yn gyfrifol.

F FOLLOW THE FLOW / Dilyn y llif

- Mae offer AI wedi'u cysylltu y tu ôl i'r llenni. Maen nhw'n aml yn cyfathrebu â systemau eraill nad ydych chi'n gallu eu gweld.
- Gall un ateb ddod o sawl system AI. Mae gwybodaeth yn cael ei phasio ar hyd cadwyn, nid dim ond o un offeryn.
- Nid yw ymddiriedaeth yn ymwneud ag un ap yn unig. Gall risgiau ddod o unrhyw fan yn y gadwyn gudd honno.

E EVALUATE ACTIONS / Gwerthuso gweithredoedd

- Gall AI weithredu nawr, nid dim ond ateb. Mae rhai systemau'n gwneud pethau ar eich rhan heb wirio pob cam.
- Nid yw awtomeiddio'n dileu cyfrifoldeb. Os yw AI yn gweithredu yn eich enw chi, rydych chi'n dal yn atebol.
- Cadwch yn effro drwy'r amser, hyd yn oed pan fo AI yn rhedeg ar ei ben ei hun. Mae goruchwyliaeth a meddwl beirniadol yn bwysig — bob tro.



CYBERFIRST
WALES

cyberfirstwales.co.uk

