

The AI-embedded Essential Digital Skills Framework

The AI-embedded Essential Digital Skills Framework sets out the digital skills and tasks all workers need to be able to carry out in an AI-driven world of work.

The wider Essential Digital Skills Framework also includes Skills for Life and the Foundation Skills that enable an individual to access technology at the most basic level (e.g., turning on a device, using a mouse).

FutureDotNow, in partnership with the Department for Science, Innovation and Technology, conducted a review of the Work element of the Essential Digital Skills Framework and made specific recommendations to ensure it reflects how AI, automation, and emerging technologies are reshaping the world of work. These recommendations are reflected in the AI-embedded Essential Digital Skills Framework.

For more information about the Framework and our work to ensure it keeps pace with evolving technology, visit www.futuredotnow.uk/framework.

25 tasks for work

Handling information and content

- 1. You can follow your organisation’s IT policies when sharing information internally and externally (e.g. classifying emails/documents, encrypting sensitive information, sharing appropriate information on social media, avoiding sharing sensitive data with unauthorised generative AI tools).
- 2. You can securely access, synchronise and share information at work across different devices (e.g. manage email, calendar or appointment system via different devices).

Communicating

- 3. You can communicate in the workplace digitally using messaging applications (e.g. Email, Microsoft Teams, Zoom, Slack, internal Intranet, WhatsApp).
- 4. You can use workplace digital tools to appropriately create, share and collaborate with colleagues (e.g. Microsoft Teams, OneDrive, G-Suite including Gemini, Office 365 including Copilot, WeTransfer, DropBox, WebEx, Slack, ChatGPT).
- 5. You can set up and manage an account on a professional online network/community/job site (e.g. LinkedIn, Total Jobs, Indeed).

Transacting

- 6. You can complete digital records on behalf of, or within my organisation (e.g. absence management, holidays, timesheets, expenses, tax returns)
- 7. You can access salary and tax information digitally (e.g. password protected payslips, P60, P45)
- 8. You can complete online financial transactions while understanding how AI systems support these processes, and can identify potential risks such as AI-generated scams or deceptive interfaces designed to manipulate your purchasing decisions.

Problem solving

- 9. You can find information online and use appropriate digital tools that help you solve work-related problems (e.g. search engines, IT helpdesk, AI assistants, software providers, peer networks, authorised generative AI).
- 10. You can improve your skills and ability to do new things at work using online tutorials, learning platforms, AI-assisted tools and how-to guides (e.g. LinkedIn Learning, YouTube, AI learning assistants, internal learning platforms).

Problem solving (cont.)

- 11. You can use appropriate software that is required of your day-to-day job (e.g. spreadsheets, online booking systems, HR management, workflow or sales management, AI-powered analytics, automated scheduling, intelligent document processing).
- 12. You can improve your own and/or the organisation’s productivity using digital tools and appropriate AI solutions (e.g. project management tools, collaboration platforms, AI-assisted task automation, meeting transcription tools).
- 13. You can develop effective prompts for AI systems to solve specific workplace problems while understanding AI’s role as a complementary resource rather than a replacement for human judgement.

Staying safe, legal and responsible online

- 14. You can act with caution online and understand that there are risks and threats involved in carrying out activities online, including when using AI tools (e.g. use anti-virus software, classify and share information securely, follow data handling policies for AI systems, or avoid certain types of websites such as piracy websites, unauthorised AI services, deepfakes and AI powered scams).
- 15. You can follow data protection guidelines online (e.g. following data storage and retention guidelines, not sharing or using other people’s data or media such as movies or music without their consent, understanding consent for AI training data, avoiding sharing copyrighted content with AI systems).
- 16. You can recognise suspicious links and content, whether human or AI-generated, and know that clicking on these links or downloading unfamiliar attachments is a risk (e.g. spam/phishing emails, AI-enhanced scams, deceptive texts, pop ups).
- 17. You can be careful with what you share online as you know that online activity produces a permanent record that can be accessed by others, and may be used to train AI systems or influence algorithmic decisions about you (e.g. publicly shared photos, forums, personal information or opinions, understanding how shared content may be used by AI systems).

Staying safe, legal and responsible online (cont.)

- 18. You can respond to requests for authentication for online accounts (e.g. resetting your password when you’ve forgotten it, two factor authentication, using a remote access key or an authenticator app).
- 19. You can identify secure websites (e.g. by looking for the padlock and ‘https’ in the address bar).
- 20. You can identify secure Wi-Fi networks to connect to (e.g. Wi-Fi networks where a unique password is required, trusted source or padlock next to Wi-Fi network).
- 21. You can update your device software/operating systems when necessary to prevent viruses and other risks (e.g. enabling automatic updates, or installing when prompted to do so).
- 22. You can set privacy and marketing settings for websites and your accounts (e.g. managing social media privacy settings, managing cookie settings, updating contact preferences, opting out of AI-powered personalisation where appropriate)
- 23. You can understand the basic principles of AI, including how it works, its limitations, and when it is appropriate to use (e.g. understanding AI training, data requirements, and evaluating when AI tools are suitable for specific tasks).
- 24. You can recognise the ethical implications of AI use and its societal impact (e.g. understanding AI biases, human oversight requirements, environmental impact and potential effects on privacy, fairness, and human rights).
- 25. You can understand and manage AI risks in your job (e.g. keeping up with new AI technology, understanding how it affects data privacy, and following AI guidelines for your industry).

