

# Appendix 2: Suggested roles and responsibilities

Roles and responsibilities of those using artificial intelligence (AI) enabled tools and systems

First published 17 June 2025

2 mins read

## Chief constable

- authorise the procurement of tools and systems, as well as their use in force
- responsible and accountable for these tools and systems, and need to be satisfied of their effectiveness, safety and integrity
- need to be satisfied that clear command structures, decision-making processes and comprehensive operational guidance and policy are in place

## AI lead

- horizon scans
- leads on engagement with AI Board and regional innovation lead
- oversees central AI register if this is being used
- leads on project landscape review, in collaboration with project lead

## Senior reporting officer or project lead

- scoping
- co-ordinates specialist advice
- engages stakeholders
- collaborates with AI lead on landscape review
- leads supplier engagement
- information asset owner for project duration
- designs governance arrangements
- leads delivery team
- co-ordinates validation and verification testing and evaluation

- sets ongoing monitoring requirements
- hands over to product manager
- oversees safe closure of project if AI is to be discontinued

## Delivery team

- sets up tool or system for testing, either by incorporating the AI components themselves or working with supplier to bring it onboard
- includes data preparation and test design, as well as equality impact assessment
- ensures knowledge capture from supplier and transfer to wider organisation

## Product manager

- takes over from project lead, including as information asset owner
- oversees ongoing monitoring of tool or system and provision of contingency plans

## Wider team

### IT team

- provide advice to project on prospective tools and systems, including data requirements, capabilities needed and interoperability
- provide ongoing technical support as needed

## Data protection officer

- conducts data protection impact assessment

## Information security officer

- conducts risk assessment
- supports engagement with prospective suppliers on information security risk

## Head of information security

- their authorisation is required to deploy the tool

## Legal team

- identify legal implications of AI tool or system
- assess overall legal and regulatory compliance as part of the validation process

## Procurement

- advise and support on procurement strategy and process

## Analyst

- advises on testing and evaluation design during scoping
- leads on validation and verification testing and evaluation, unless bringing in external expertise
- supports delivery team to interpret results

## Business change

- work with delivery team and supplier, if a supplier is being used, to plan for skills and knowledge transfer to wider workforce

## HR

- work with delivery team to identify and plan how to fill skills gaps through upskilling and recruitment if necessary

## Officers and staff

- as end-users of the tool or system, they will need to use it in adherence with force policy, professional standards, the Code of Ethics and their professional judgement on when to follow or depart from the AI

## Tags

Artificial intelligence