National Engineering Policy Centre

Royal Academy of Engineering

Post-16 L2 and L3 qualifications: 2027 proposed subject content

Consultation Response

June 2026

Question A

> *Which qualification(s) are you responding about?*

V Level in Digital Systems and Data

Question 1

> *To what extent does the proposed content enable students to achieve the aims of the qualification?*

Mostly

Please explain your answer:

Overall, the proposed occupational standards represent a strong and thoughtful framework for the proposed V level. Collectively, they demonstrate a clear attempt to balance technical capability, workplace authenticity, responsible practice and future relevance. There is particularly positive recognition of the growing importance of AI-enabled systems, ethical awareness, accessibility, and the relationship between technical activity and organisational decision-making. In many respects, these standards are more mature and occupationally grounded than comparable digital specifications currently in use.

WP1 is ambitious in scope and already contains many strengths. The coverage of data preparation, analysis, interpretation, governance, transparency, communication and accessibility reflects contemporary workplace expectations well. The inclusion of AI-assisted analytics, bias awareness and responsible presentation of findings is especially welcome, as these are increasingly central to real-world data practice. The standard also makes useful connections between analytical activity and organisational decision-making, helping to position data analysis as a practical workplace function rather than a purely academic exercise.
WP2 is particularly strong in terms of focus and occupational coherence. Compared with WP1, it is more tightly scoped and has a very clear progression from applying controls, through

monitoring and interpretation, to escalation of concerns. The emphasis on human judgement, interpretation of alerts, recognition of false positives and balancing usability with security reflects authentic workplace cyber-security practice very effectively. The standard also avoids many common weaknesses seen in cyber specifications, such as overemphasis on offensive security, unrealistic technical depth or dependence on vendor-specific tools.

WP3 is arguably the strongest and most occupationally balanced of the three standards. It demonstrates excellent alignment between knowledge and skills and maintains a strong focus on operational realism without drifting into unnecessary software engineering or infrastructure specialism.

Question 2

> *How well does the proposed content support progression to higher-level study (defined as level 4+), or an apprenticeship?*

Fairly well

What changes, if any, should be made to the content to strengthen progression?:

The most significant issue that impacts on progression is the extent to which the qualification prepares students for the ways of working in higher level study. There is strong alignment between the proposed content and how that content is built upon in level 4+ vocational pathways. However, the link with academic pathways is less clear. Getting this right will require clearer articulation between the skills identified in the proposed content and any underpinning theoretical knowledge, particularly as this forms the basis of academic study at level 4+. This is an inevitable given the challenges presented by the embedded differences in approach to the balance between skills and knowledge in different pathways.

Question 3

> *Is the content set at an appropriate level of demand for level 3 students?*

Appropriate

What changes, if any, are needed to the content to ensure it meets the expected level of learner demand for a Level 3 qualification?:

The most significant gap relates to statistical reasoning. While the standard references trends, averages, percentages and variability, it does not explicitly address concepts such as distributions, outliers, sampling bias, uncertainty or confidence in findings. Without these elements there is a risk that learners develop procedural analytical skills without understanding the evidential strength or reliability of conclusions. Similarly, the standard would benefit from clearer treatment of uncertainty communication, particularly in the context of AI-generated insights, so that learners are able to qualify conclusions appropriately and avoid overstating certainty.

The most important area for development within WP2 is the treatment of incident response. While escalation and protective actions are mentioned, there is little explicit reference to containment, evidence preservation, response sequencing or minimising operational

disruption. These are fundamental concepts in operational cyber-security and would significantly strengthen the standard.

Similarly, there should be clearer recognition of risk assessment and prioritisation. Learners need to understand how likelihood, impact and organisational context influence the urgency and severity of security concerns.

Some wording would also benefit from clarification to avoid ambiguity in assessment. For example, the phrase “apply protective actions” is potentially too broad and could imply responsibilities beyond the intended level of learner autonomy. Framing this instead as “first-line” or “authorised” protective actions would improve clarity.

The standard could also more explicitly address the causes of vulnerabilities, including misconfiguration, weak authentication, delayed patching and insecure network practices, as well as practical phishing-verification behaviours such as checking URLs, verifying sender identity and handling suspicious attachments.

A further strength of WP2 is its recognition that operational issues may sometimes indicate cyber concerns. However, the current wording risks conflating general IT support activity with cyber-security monitoring. Greater distinction between routine operational faults and indicators requiring security escalation would improve occupational precision.

Finally, the inclusion of secure remote working practices and emerging AI-enabled threats such as impersonation, synthetic content and automated phishing would help ensure future relevance.

The most significant omission in WP3 is explicit troubleshooting methodology. While structured fault-finding is referenced, the standard would benefit from clearer inclusion of behaviours such as reproducing faults, isolating variables, testing hypotheses, identifying root causes and confirming resolution. These are core operational competencies within technical support and systems environments.

The specification would also be strengthened by greater emphasis on change control, version management and rollback procedures, as configuration activity in modern workplaces is rarely undertaken without controlled implementation processes.

Backup and recovery awareness is another notable omission. Concepts such as restoration testing, recovery readiness and backup verification are central to operational resilience and should be reflected within the standard.

Similarly, the treatment of security could move beyond generic permissions and updates to include secure default configurations and system hardening principles.

WP3 would also benefit from clearer recognition of user acceptance and operational suitability. While user needs and accessibility are addressed well, there is limited reference to user validation or acceptance criteria in determining readiness for deployment. In addition, some acknowledgement of interoperability, connected services and shared authentication environments would help future-proof the standard without requiring excessive technical depth.

Question 4

> *Are there any issues associated with delivering the content that should be considered to ensure that the content is manageable for providers to deliver?*

Don't Know

Question 5

> *Does the content have the potential to have a disproportionate impact, positive or negative, on specific groups, in particular those who share a 'protected characteristic' (age, disability, gender reassignment, marriage and civil partnership, pregnancy and maternity, race, religion or belief, sex and sexual orientation) or those from lower socio-economic backgrounds?*

Yes

If Yes/Don’t know, please explain:

Given the persistent under-representation of girls in digital pathways (e.g. 10.5% female completion in Digital Production, Design and Development T Level in 2025, EngineeringUK, 2025), we suggest it may be valuable to test the subject content and example contexts with a diverse range of learners. This would help ensure the qualification is accessible and engaging across different demographic groups, including for both male and female students, without altering the technical standard.

Question 6

> *Is the title of the qualification appropriate?*

Yes

Question 7

> *Is any of the content unclear or ambiguous?*

Yes

If Yes/Don't Know, what is unclear and how might it be re-worded?:

There is some wording that could be improved. For example, some wording would also benefit from clarification to avoid ambiguity in assessment. For example, the phrase “apply protective actions” is potentially too broad and could imply responsibilities beyond the intended level of learner autonomy. Framing this instead as “first-line” or “authorised” protective actions would improve clarity.

Question 8

> *Is there anything else about the content that you would like to provide feedback on?*

Across the standard there is evidence of careful thinking about responsible AI use, accessibility, procedural discipline and workplace authenticity. The challenge moving forward will be maintaining this strength while ensuring the specifications remain assessable and appropriately scoped for 16–18 learners.

Collectively, the standards provide a strong foundation for contemporary digital technology qualifications. With refinement around statistical reasoning, incident response, troubleshooting methodology, operational realism and future-facing workplace practices, the standards could become highly credible representations of entry-level digital competence that employers would recognise as both relevant and practical.

We have carried out a detailed analysis of the content and would be delighted to provide further feedback on matters of detail. The more significant issue is the alignment between the assessment regime for this qualification to meet the need to prepare students for vocational and assessment regimes. This is outside the scope of this consultation but is a matter we will raise in our response to the Ofqual consultation.

While the qualification is intentionally broad, it would be helpful to ensure that progression routes into engineering and technology pathways are clearly signposted, including how this V Level aligns with related occupations, apprenticeships and higher education routes. We welcome the emphasis on varied organisational scenarios and would encourage ensuring that examples include a wide range of sectors, including engineering, manufacturing and infrastructure, to reflect the breadth of digital applications and careers. This qualification represents an important opportunity to strengthen understanding of how digital systems underpin careers across varied sectors – including engineering and technology- and it will be important that this applied, cross-sector relevance is clearly communicated.

End of Survey

> *Do you want to provide feedback on any other qualifications?*

No