This is a published notice on the Find a Tender service: https://www.find-tender.service.gov.uk/Notice/082882-2025

Contract

Further Education Network Connectivity and Cyber Security Services (FENCCSS)

Department for Education

UK7: Contract details notice - Procurement Act 2023 - view information about notice types

Notice identifier: 2025/S 000-082882
Procurement identifier (OCID): ocds-h6vhtk-059d41 (view related notices)
Published 15 December 2025, 1:07pm

Changes to notice

This notice has been edited. The previous version is still available.

1. Included details of the top 3 KPIs of this contract.

2. Included redacted version of the contract.

Scope

Reference

project_9790

Description

Contract to provide Connectivity, Cyber Security and Specialist Advisory Services to the Further Education sector in England.

Overview of services required

DfE is proposing to contract with Jisc to deliver a comprehensive digital infrastructure and support service for the Further Education (FE) sector in England via the Janet Network. The Janet Network is the UK’s sole National Research and Education Network (NREN) linking up to the Gigabit European Academic Network (GÉANT), the pan-European data network for the research and education community. The tertiary education sector including FE relies on the Janet Network for IT connectivity and cyber security (CS) (please also see “Direct award justification” below).

The digital infrastructure and support services for the FE sector will encompass robust connectivity, sector-wide cyber security, and strategic ICT guidance.

1. Connectivity

• Private WAN: Secure, resilient, symmetrical network connecting all In-Scope Institutions.

• Dual Connections: Each institution to benefit from a second connection for improved resilience.

• Performance Standards: High bandwidth (800Gb/s), high speed (1Gb/s), low latency (1–5ms), minimal packet loss and jitter.

• Scalability & Upgrades: Network must scale with demand and support upgrades via separate contracts.

• Interoperability: Direct access to global NRENs, GEANT, cloud platforms, and peering with relevant public and private networks.

• Managed Services: Includes router management, DNS, IP address registry, network monitoring, maintenance (including hardware refresh) and support.

• Network security: threat-driven, risk-based approach to implementing physical and virtual security measures to pre-empt and respond to emerging threats.

2. Cyber Security (please also see “Direct award justification” below)

• Sector-Wide Scope: Services extend beyond the network to cover the entire UK tertiary education sector.

• Threat Detection: Uses UK tertiary education-specific data to identify vulnerabilities and sector-unique threats.

• CSIRT: A 24/7/365 incident response team offering expert support and coordinating multi-institutional responses.

• Intelligence Sharing: Disseminates threat insights across the sector to improve collective resilience.

• Government Integration: Collaborates with NCSC and other agencies; reports major incidents within 1–2 hours.

• Quarterly Reporting: Includes incident summaries, trends, and recommendations for improvement.

3. Strategic Advice and Guidance (SAAG)

• Proactive Sector-Wide Guidance: Free advice on ICT use in FE, covering (but not restricted to) curriculum, cyber security, cloud, AI, mergers, Ofsted improvement, and emerging technologies.

• Bespoke Support: Customised advice available under separate contracts.

• Named Relationship Managers: Each institution has a dedicated contact for ICT queries and access to SAAG.

• Multi-Channel Delivery: Guidance provided via blogs, webinars, training, case studies, and more.

• Performance & Reporting: Must meet service standards and be reported quarterly to the Buyer.

Unique Requirements

The proposed services reflect the unique requirements of the FE sector (please also see “Direct award justification” below), combining:

- National-level infrastructure and cyber resilience,

- Sector-specific intelligence and threat response, and

- Strategic ICT leadership and policy support.

Contract 1. FENCCSS (Further Education Network & Cyber Security Services)

Supplier

- Jisc

Contract value

- £42,000,000 excluding VAT

- £50,400,000 including VAT

Above the relevant threshold

Date signed

19 November 2025

Contract dates

- 1 December 2025 to 30 November 2026

- Possible extension to 30 November 2028
- 3 years

Description of possible extension:

The Authority may exercise the option to extend the contract by providing the Supplier with no less than 3 months written notice before the contract expires.

Main procurement category

Services

CPV classifications

- 32412110 - Internet network
- 48730000 - Security software package
- 72220000 - Systems and technical consultancy services

Contract locations

- UK - United Kingdom

Key performance indicators

Name	Description	Reporting frequency
Connectivity: Availability	Percentage of time during a Month (24/7/365) when the Network is Available, excluding periods of planned maintenance.	3 months
Connectivity: Network performance metrics		

Name	Description	Reporting frequency
Connectivity: Incident triage time		
Connectivity: Critical incident Response Time		
Connectivity: High priority incident Response Time		
Connectivity: Medium priority incident Response Time		
Connectivity: Low priority incident Response Time		
Connectivity: Critical incident resolution time	Number of Critical incidents per Month responded to within: ([REDACTED] - Text redacted under Section 94(1)(a) PA23) during Business Hours and ([REDACTED] - Text redacted under Section 94(1)(a) PA23) during On-call Hours	3 months
Connectivity: High priority incident resolution time		
Connectivity: Medium priority incident resolution time		
Connectivity: Low priority incident resolution time		
Cyber Security: Monitoring and threat detection		
Cyber Security: Critical (P1) cyber incident notification		
Cyber Security: High priority cyber incident notification		
Cyber Security: Critical (P1) cyber incident tickets Response Time	Number of Critical cyber incidents reported to CSIRT responded to within ([REDACTED] - Text redacted under Section 94(1)(a) PA23)	3 months
Cyber Security: High priority(P2) cyber incident tickets Response Time		
Cyber Security: Medium priority(P3) cyber incident tickets Response Time		

Name	Description	Reporting frequency
Cyber Security: Low priority(P4) cyber incident tickets Response Time		
Specialist Advice and Guidance: Quarterly report submissions		
Specialist Advice and Guidance: Annual satisfaction surveys		
Social Value: Number of training opportunities (Level 2, 3, and 4+) other than apprentices created or retained under this contract		
Social Value: Number of people-hours of learning interventions delivered under this Contract, by UK region		

Signed contract documents

FENCCSS Redacted Contract - PDF.zip

Redacted Contract

Other information

Conflicts assessment prepared/revised

Yes

Procedure

Procedure type

Direct award

Direct award justification

- Single supplier - intellectual property or exclusive rights
- Single supplier - technical reasons

Jisc operates the Janet Network which is the UK's sole NREN linking up to GÉANT, the pan-European data network for the research and education community. The tertiary education sector including Further Education (FE) relies on the Janet Network for IT connectivity and cyber security (CS). Jisc also hosts and operates the .ac.uk domain used by all UK tertiary education establishments, providing additional CS capability.

Underpinning the Janet Network and therefore curriculum delivery and BAU operations of all FE colleges is the provision of appropriate CS. Combating the more serious cyber attacks (i.e. ransomware) requires the use of threat intelligence to identify, anticipate and mitigate attacks. In turn this requires a critical mass of network data to analyse. The Janet Network is a private network solely for tertiary education users and is therefore able to collect detailed data on network traffic and potential threats specific to the tertiary education sector. Only the Janet Network has access to the volume and quality of data needed to combat serious cyber attacks and the DfE Chief Information Security Officer has assessed that no other provider can offer the level of cyber security as appropriate for the sector.

It is proposed to award the contract directly to Jisc that is not an excluded supplier because a direct award justification applies in accordance with section 41(1)(a) of the Procurement Act 2023. DfE is relying on the single supplier direct award justifications in paragraphs 6 and 5 of schedule 5 of the Procurement Act 2023:

• paragraph 6 (a) due to an absence of competition for technical reasons, only a particular supplier can supply the goods, services or works required, and (b) there are no reasonable alternatives to those goods, services or works ; and

• paragraph 5 (a) due to a particular supplier having intellectual property rights or other exclusive rights, only that supplier can supply the goods, services or works required, and

(b) there are no reasonable alternatives to those goods, services or works.

The explanations for why the justifications apply are as follows.

Absence of competition for technical reasons - paragraph 6

This justification applies because all FE colleges obtain their connectivity from the Janet Network. Their use of the Janet Network also provides the data on which the CS services specifically tailored to FE institution are based. It is therefore not possible to separate the IT connectivity services from the CS services and both services need to be provided via the Janet Network, which is specifically configured to provide both connectivity services and specifically tailored CS services to FE institutions. No other internet service provider is able to provide the combination of IT connectivity services and bespoke CS services which are the direct result of the Janet Network being the UK's sole NREN.

No reasonable alternative.

In the absence of another NREN, the only potential alternative would be for another supplier to develop a replacement solution to the requirements for FE institutions which would require building a NREN from scratch with the features of being a private network for the tertiary education sector to provide the required IT connectivity services and specifically tailored CS. A replacement NREN would also be required to meet the stringent requirements of GÉANT to continue being able to connect to it . In addition to creating such a replacement NREN which would create significant upfront costs, sufficient time for testing and mobilisation of that replacement NREN would also be required. There is not sufficient funding and time for any alternative supplier to design, build, test, and deploy an alternative solution to ensure the continuation of IT connectivity and CS services delivered via a NREN required for FE institutions to continue to provide education services to their students.

Therefore, there are no reasonable alternatives.

The second justification is intellectual property rights - paragraph 5

This justification applies because Jisc owns the intellectual property rights to the Janet Network, therefore only Jisc is able to provide the proposed services via the Janet Network. The same justifications regarding limb (a) of paragraph 6 of Schedule 5 of the PA also apply for limb (a) of paragraph 5 of Schedule 5 of the PA.

No reasonable alternatives.

The same justifications, stated above, for why there are no reasonable alternatives for paragraph 6 absence of competition for technical reasons, apply to the justification for paragraph 5. Therefore, there are no reasonable alternatives.

Supplier

Jisc

- Companies House: 05747339

4 Portwall Lane

Bristol

BS1 6NB

United Kingdom

Email: funders@jisc.ac.uk

Website: https://www.jisc.ac.uk/

Region: UKK11 - Bristol, City of

Small or medium-sized enterprise (SME): No

Voluntary, community or social enterprise (VCSE): No

Supported employment provider: No

Public service mutual: No

Contract 1. FENCCSS (Further Education Network & Cyber Security Services)

Contracting authority

Department for Education

- Public Procurement Organisation Number: PDZG-3487-DPVD

Sanctuary Buildings, 20 Great Smith Street

London

SW1P3BT

United Kingdom

Email: Technology.CATEGORY@education.gov.uk

Region: UKI32 - Westminster

Organisation type: Public authority - central government