

Schedule 2 (Specification)

This Schedule sets out what the Buyer wants.

For all Deliverables, the Supplier must help the Buyer comply with any specific applicable Standards of the Buyer.

1 DEFINITIONS

1.1 In this Schedule, the following terms shall have the following meanings, and they shall supplement Schedule 1 (*Definitions*):

"Change Freeze Period" a defined period during which no changes, updates, or deployments are allowed to infrastructure. During a Change Freeze Period, only emergency or pre-approved changes are permitted, and these typically require special authorization. The Supplier must consult with In-Scope Institutions on proposed Change Freeze Periods in advance and must notify the Buyer and each In-Scope Institution in writing not less than 30 calendar days before the Change Freeze Period;

"CSIRT" Cyber Security Incident Response Team;

"FE" further education;

"FE Expertise" in-depth knowledge of, and relevant experience in, the FE sector in the United Kingdom, as required by paragraph 7.1;

"In-Scope Institutions"

- (a) all institutions which are:
 - (i) further education corporations and sixth form colleges in England and institutions designated under section 28 of the Further and Higher Education Act 1992; and
 - (ii) 16-19 academies in England which were formerly sixth form colleges;
- (b) the special post-16 institutions in England listed in Annex 1;
- (c) any additional institutions in England which fall within (a) above during the Contract Period; and
- (d) any additional special post-16 institutions in England which are approved by the Buyer from time to time;

"NCSC" the National Cyber Security Centre;

"Network" has the meaning given to it in paragraph 4.1;

"NREN"	national research and education network;
"SAAG"	has the meaning given to it in paragraph 3.1(c); and
"Wider Educational ICT Data"	data generated by, or other otherwise relating to, the use of information and communication technology (including the UK NREN) by the education sector in the United Kingdom.

2 BACKGROUND

- 2.1 The Buyer is seeking to procure connectivity, cyber security and related advisory services for the FE sector with the aim of:
- (a) building the capability and capacity of FE;
 - (b) promoting and using technology to support effective curriculum delivery and to help achieve sustainable, high-quality local provision of FE; and
 - (c) supporting the FE sector in improving cyber security and dealing with cyber security threats and attacks.
- 2.2 The Buyer expects the Supplier to use its FE Expertise and in-depth understanding of Wider Educational ICT Data, and to work closely with the FE sector, to achieve these aims.
- 2.3 The Buyer may consult with others in industry when managing this Contract, taking account of the ownership structure of the Supplier, and the funding of the Supplier by other industry bodies.

3 OVERVIEW OF REQUIREMENTS

- 3.1 The Deliverables shall comprise of:
- (a) the connectivity services detailed in paragraph 4;
 - (b) the cyber security services detailed in paragraph 5;
 - (c) the specialist advice and guidance detailed in paragraph 6 ("**SAAG**"); and
 - (d) any services or activities that can be reasonably considered to be incidental and reasonably required for the proper performance of the services at (a) to (c) above.
- 3.2 The Supplier shall also comply with the requirements detailed in paragraphs 7 and 8.

4 CONNECTIVITY

- 4.1 The Supplier shall design, build, operate, maintain and support a robust, secure, geographically diverse, resilient and symmetrical private wide area network for the In-Scope Institutions that meets the requirements in this Contract and the wider evolving needs of the FE sector in England ("**Network**").
- 4.2 The demarcation point of the Network shall be the router connecting into each In-Scope Institution. In-Scope Institutions shall be expected to provide the appropriate space, equipment, power and other resource to site that router at their premises and to connect to the Network through such router.
- 4.3 In-Scope Institutions shall be permitted to contact the Supplier directly about all aspects of the Network, including setting up a connection.

Infrastructure

- 4.4 Subject to the remaining provisions of this paragraph 4, the Supplier shall use Good Industry Practice to select, install, configure and deploy the hardware, software and other technology necessary and appropriate for the provision of the Network.
- 4.5 All In-Scope Institutions connected to the Network will have the benefit of a second connection to the Network to improve resiliency. The Buyer accepts that this may not be achievable at the Start Date and the Supplier shall commit to installing and operating a resilient connection to the Network for each In-Scope Institution during the Contract Period, unless otherwise agreed with the Buyer.
- 4.6 The Supplier shall ensure that all elements of the Network remain physically located within the United Kingdom or European Economic Area. However, users must be able to access and connect to the Network remotely from outside these areas.
- 4.7 The Supplier shall ensure, subject to funding by the Buyer, that the Network is scalable to support increased use (in excess of the requirements in this paragraph 4) over the Contract Period.

Capacity and transmission

- 4.8 The Network must be capable of supporting high performance computing. The Supplier shall use reasonable endeavours to ensure the following applies to all main and resilient connections:
- a) access bandwidth of 1Gb/s to In-Scope Institutions;
 - b) latency (from In-Scope Institution to closest Janet node) between 1-5ms;
 - c) packet loss under 0.5%;
 - d) jitter under 5ms.
- 4.8 The Network must be symmetrical, and all traffic must be treated equally.
- 4.9 Links into the Network for In-Scope Institutions must, where practicable, be uncontended, such that the ability of each In-Scope Institution to benefit from the metrics set out in paragraph 4.8 in full is not in any way affected or prevented by the activity of any other In-Scope Institution.
- 4.10 The Supplier must be capable of providing upgraded links into the Network for In-Scope Institutions on request. Such upgrades shall be subject to separate contracts between the Supplier and the relevant In-Scope Institution.
- 4.11 The Supplier shall deploy the latest version of the Internet Protocol as the network layer communications protocol for the Network and shall ensure that the Network is upgraded to remain on the latest version of the Internet Protocol during the Contract Period.
- 4.12 The Supplier shall provide complete management of IP addresses and domain registry of ".ac.uk" addresses for In-Scope Institutions.
- 4.13 The Supplier shall provide a reliable and resilient nameserver service, hosted within the Network. This must:
- (a) maintain web, email and DNS presence;
 - (b) provide a mechanism for In-Scope Institutions to manage DNS records or a subdomain; and

- (c) be accompanied by a protective DNS service (advanced DNS and malware protection) applied to In-Scope Institutions.

4.14 The Supplier shall synchronise time on the Network using the Network Time Protocol.

Interconnectivity and interoperability

4.15 The Network must provide its users with:

- (a) direct secure access to the public internet;
- (b) peered connectivity into all global NRENs via GÉANT;
- (c) peered connectivity into private networks worldwide relevant to the tertiary education sector; and
- (d) peered connectivity into other networks, cloud platforms, systems and applications as may be appropriate or relevant to users of the Network.

4.16 The Supplier shall continually review the connections provided under paragraph 4.16 throughout the Contract Period to ensure that they keep pace with the evolving needs of the users of the Network.

For the avoidance of doubt, the Supplier may determine, and change during the term of this Agreement, the method and manner in which it designs and operates the Network in order to deliver the connectivity service described in this paragraph 4. Any changes required or initiated by the Supplier in order to deliver the connectivity services e.g. to topography, routing, layout, hardware refresh etc will be at the cost of the Supplier

Managed router service

4.17 The Supplier shall provide a managed router service to In-Scope Institutions. Such service shall be subject to separate contracts between the Supplier and the relevant In-Scope Institution

Network monitoring

4.18 The Supplier shall implement and operate a network monitoring system which shall enable the Supplier to see the live performance of the Network, record incidents and their status and enable the Supplier to provide the reporting required by this Contract.

4.19 The Supplier shall also implement and operate an appropriate system to provide In-Scope Institutions with, as a minimum, the ability to check the overall status of the Network and determine if there are localised issues.

Network security

4.20 The Buyer places great emphasis on the availability and capability of FE (including In-Scope Institutions) and, consequently, on the integrity and security of the Network.

4.21 The Supplier shall, using its FE Expertise and Good Industry Practice, build resilience and protection against cyber attack into the design, implementation, operation and management of the Network. Without limiting the generality of the foregoing, the Supplier must:

- (a) understand, based on extensive analysis of, and insights into, Wider Educational ICT Data, where to focus its resources to maximise the cybersecurity of the Network;
- (b) adopt a threat-driven, risk-based approach to implement all security measures (physical and virtual) appropriate and proportionate to the prevailing risk within FE and

to effectively limit opportunities for attackers to compromise the Network, keep the information held on and transmitted through the Network secure, and prevent loss of operational efficiency of In-Scope Institutions; and

- (c) continually increase resilience and protection by deriving intelligence from use and operation of the Network and keeping pace with the changing threat landscape within FE (including through continued examination of Wider Educational ICT Data) to shape and prioritise the review and implementation of security measures.

Maintenance and refresh

- 4.22 The Supplier shall perform, in accordance with Good Industry Practice, appropriate and regular preventative maintenance on the Network to ensure its integrity and optimal performance.
- 4.23 The Supplier shall bear the cost of any technology refresh activity that is required during the Contract Period as a result of any hardware, software or other technology used in the Network becoming end of life or otherwise not meeting the requirements of this Contract. The Supplier shall ensure that any such refresh does not negatively affect the Services and, in particular, that performance against the Key Performance Indicators can be maintained (and, where possible, improved).
- 4.24 The Supplier shall provide no less than two (2) weeks' notice to the Buyer and In-Scope Institutions before carrying out any maintenance, including the duration of the maintenance and its likely effect on the Network (if any). The Supplier shall notify the Buyer and In-Scope Institutions of any emergency maintenance as soon as practicable, including the threat being addressed and the anticipated duration of the maintenance.
- 4.25 The Supplier shall not carry out any planned maintenance and will use reasonable endeavours to procure that its circuit suppliers shall not carry out any planned maintenance during any Change Freeze Period.

Support

- 4.26 The Supplier shall provide and maintain an easily accessible repository of information to assist users of the Network in making use of all the features of the Network and troubleshooting common issues.
- 4.27 The Supplier shall provide a service desk for technical support of the Network, which must:
 - (a) provide support over the phone ;
 - (b) be available 24/7/365;
 - (c) classify the priority of incidents in accordance with Schedule 10 (*Performance Levels*);
 - (d) update users on the status of incidents no less than once per Working Day until resolution; and
 - (e) keep records of all incidents, including their classification, response time and resolution time.
- 4.28 Where necessary to resolve incidents, the Supplier shall physically attend the In-Scope Institutions' site to resolve incidents.

Key Performance Indicators

- 4.29 The Supplier shall at all times provide the Services to comply with Schedule 10 (*Performance Levels*).

5 CYBER SECURITY

Scope of cyber security service

- 5.1 The Service provided by the Supplier under this paragraph 5 is not limited to the Network or to In-Scope Institutions, but is applicable to the FE sector in the United Kingdom as a whole.

Monitoring and threat detection

- 5.2 The Supplier shall, using its FE Expertise, and based on extensive analysis of, and insights into, Wider Educational ICT Data, implement and operate a cost-effective monitoring and threat detection system with the aim of:
- (a) tracking the ongoing effectiveness of the security measures implemented to protect the Network and the UK NREN;
 - (b) detecting indicators of vulnerability or compromise of the Network and the UK NREN in a timely manner so that appropriate preventative or corrective action can be taken;
 - (c) identifying:
 - (i) cyber security events adversely affecting, or with the potential to adversely affect, FE sector organisations; and
 - (ii) known and unknown cyber security threats unique to the FE sector, so that appropriate action can be taken; and
 - (d) generating a sufficient volume of data to contribute to the existing Wider Educational ICT Data and continue to make effective analyses and judgments in the provision of the Services.
- 5.3 For the purposes of paragraph 5.2(c), the Supplier will not be expected to monitor any individual In-Scope Institution's or other FE sector organisation's local area network.
- 5.4 Subject to paragraph 5.3, the Supplier shall utilise all sources which are relevant to achieving the aims of the monitoring and threat detection system.
- 5.5 The Supplier shall use its expert judgment to: triage incidents, events and threats detected and identified in accordance with the provisions of Schedule 10 (*Performance Levels*); determine the appropriate response to contain the spread of, and minimise the impact of, the incident, event or threat; and deliver such response.

CSIRT

- 5.6 The Supplier shall act as a central, national body to coordinate cyber intelligence and response to cyber incidents in the FE sector.
- 5.7 The Supplier shall provide a CSIRT which must:
- (a) be contactable by phone by FE sector organisations and the Buyer 24/7/365 for initial engagement (as per the definition of initial engagement of the NCSC Cyber Incident Response assurance provider programme.);
 - (b) be prepared to provide, and actually provide when an incident or event occurs, appropriate and proportionate (depending on the priority classification of the incident or event) experienced, professional advice, support and guidance to any FE sector

organisation which requests support to respond to, manage, mitigate and resolve a cyber incident or event;

- (c) co-ordinate responses to cyber security incidents and events which affect more than one FE sector organisation;
- (d) be appropriately staffed by individuals with relevant qualifications and experience, and an excellent understanding of cyber security in FE (including through the intelligence generated by the monitoring and threat detection system above); and
- (e) classify incidents and events in accordance with the provisions of Schedule 10 (*Performance Levels*).

5.8 Where an incident or event reported by one FE sector institution is relevant to others in FE, the Supplier will share relevant threat intelligence information to other FE sector organisations and provide guidance and advice on relevant protections and mitigations.

Key performance indicators

5.9 The Supplier shall provide during their operational hours the Services to comply with Schedule 10 (*Performance Levels*).

Reporting

5.10 The Supplier shall:

- (a) Notify the Buyer, NCSC, and any other appropriate Government authority (depending on the circumstances) of any:
 - (i) Major Cyber Incident, within 1 hour of notification or detection; and
 - (ii) Significant Cyber Incident, within 2 hours of notification or detection; and
- (b) Provide updates as frequently as necessary to keep the Buyer and other notified persons informed of the progress of the incident notified under (a), steps taken by the Supplier to respond, assist and mitigate, and developments of the incident (provided that such reporting should not take precedence over responding to the incident).
- (c) Inform the FE sector organisation of their obligation to promptly notify the Buyer, NCSC, and any other appropriate Government authority (depending on the circumstances) of any Cyber Incident.

5.11 The Supplier shall provide the Buyer with quarterly reports which shall contain, as a minimum, the following information:

- (a) the number of security incidents and events notified to, and handled by, CSIRT in that quarter;
- (b) a summary of all Major Cyber Incidents and Significant Cyber Incidents in that quarter
- (c) insight into trends in monitoring and threat detection and CSIRT activity, across the quarter and relative to the elapsed portion of the Contract Period;

- (d) a summary narrative on recommendations for improvement of cyber security, based on the insights in (c); and
- (e) such other details as the Buyer may reasonably require from time to time.

Cooperation with other bodies

- 5.12 The Supplier shall, on request and as reasonably necessary, collaborate and cooperate with the NCSC and other Government agencies in relation to cyber security. This may include (without limitation) making available monitoring and threat detection data, sharing lessons learned from Major Cyber Incidents, and supporting investigations into, and responses to, cyber crime.

Additional services

- 5.13 The Supplier must have the ability to offer additional cyber security services to organisations in the FE sector on request, which shall be subject to separate contracts and costs between the Supplier and the relevant recipient.

6 SPECIALIST ADVICE AND GUIDANCE

- 6.1 Without prejudice to the Services set out in paragraphs 4 and 5, the Supplier shall apply its FE Expertise, in-depth understanding of Wider Educational ICT Data, learnings from the provision of the Services generally, and Good Industry Practice to deliver the following to FE sector organisations (including In-Scope Institutions) and Government in England:

- (a) proactive advice, guidance and thought leadership that is generally applicable to the FE sector as a whole or a significant part of it, which:
 - (i) shall be available free of charge to its recipients (i.e., it shall be covered by the Charges);
 - (ii) shall cover the following:
 - (A) all aspects of the use of information and communication technology in FE, including (without limitation) curriculum delivery, remote and blended learning, business-as-usual functions, cyber security, data and data analytics, cloud technologies, and developing and emerging technologies such as artificial intelligence and quantum computing;
 - (B) new trends, developments, threats or issues with the use of information and communication technology in FE;
 - (C) information and communication technology integration during mergers in the FE sector;
 - (D) use of information and communication technology in FE to move to a "good" or "outstanding" Ofsted rating;
 - (E) input into, and support of the development of, Government advice, guidance and policy relating to information and communication technology in FE; and
 - (F) any other similar topics which the Supplier considers will be beneficial to the needs and aims of the FE sector (including topics that the Supplier identifies through horizon scanning, targeted research or other innovation activities);

- (iii) shall be delivered with sufficient regularity to ensure the FE sector and Government are informed and knowledgeable about current and developing issues relevant to information and communication technology in FE, including where the advice or guidance is originally delivered in response to a specific request from a single institution under (b) below but is generally applicable to the FE sector as a whole or a significant part of it; and
 - (iv) shall be made available by whatever medium is most appropriate on a case-by-case basis, including (without limitation) notes, blogs, webinars, online training, case studies, in-person seminars and conferences, case studies, pilot studies, exemplar documentation, and forums; and
 - (b) bespoke advice and guidance to the In-Scope Institutions and Government in England on request, which shall be subject to separate contracts between the Supplier and the relevant recipient.
- 6.2 The Supplier shall ensure that each In-Scope Institution has a named relationship manager who shall:
- (a) act as the first point of contact for information and communication technology questions;
 - (b) either direct the In-Scope Institution to readily-available SAAG to answer the question or confirm that bespoke SAAG on the question can be provided by the Supplier for an additional fee; and
 - (c) seek to ensure all In-Scope Institutions receive reasonable and equitable access to SAAG.
- 6.3 The Supplier shall at all times provide the SAAG to comply with Schedule 10 (*Performance Levels*).
- 6.4 The Supplier shall provide the Buyer with quarterly reports which shall provide an accurate overview of the SAAG provided in that quarter and such other details as the Buyer may reasonably require from time to time.

7 OTHER REQUIREMENTS

- 7.1 The Supplier must demonstrate (to the Buyer's reasonable satisfaction) expert knowledge of the FE sector in the United Kingdom and experience in enabling information and communication technology in the FE sector in the United Kingdom.
- 7.2 The Supplier must hold the following accreditations and certifications during the Contract Period:
- (a) NCSC Cyber Incident Response (Level 2 minimum);
 - (b) CREST or CHECK (if the Supplier offers penetration testing under paragraph 5.13 above);
 - (c) Cyber Essentials Plus;
 - (d) ISO27001 to cover as a minimum:
 - (i) federated roaming services;
 - (ii) cloud services;
 - (iii) trust and identity services;

- (iv) cyber security services; and
 - (v) network operations; or
- an equivalent recognised scheme or standard; and
- (e) ISO9001 to cover as a minimum:
 - (i) network operations;
 - (ii) cyber security services;
 - (iii) connectivity and federated roaming services;
 - (iv) training services;
 - (v) cloud services – consultancy, professional, and managed services; and
 - (vi) trust and identity services.

For the avoidance of any doubt, this list shall apply in addition to the Relevant Certifications as those are defined in Schedule 16 (*Security*).

- 7.3 The Services shall meet or exceed, and the Supplier shall support the In-Scope Institutions to meet or exceed, the following guidelines published by the Buyer (as these may be updated from time to time):

- (a) *"Meeting digital and technology standards in schools and colleges - Broadband internet standards for schools and colleges"*, available at the following address: <https://www.gov.uk/guidance/meeting-digital-and-technology-standards-in-schools-and-colleges/broadband-internet-standards-for-schools-and-colleges> ; and
- (b) *"Meeting digital and technology standards in schools and colleges - Cyber security standards for schools and colleges"*, available at the following address: <https://www.gov.uk/guidance/meeting-digital-and-technology-standards-in-schools-and-colleges/cyber-security-standards-for-schools-and-colleges>.

8 SOCIAL VALUE PRIORITIES

- 8.1 The Buyer's social value priority in this procurement is Outcome 2 Skills for growth: supporting growth sectors and addressing skills gaps.

ANNEX 1

IN-SCOPE SPECIALIST POST-16 INSTITUTIONS

- | | |
|--|---|
| 1. Beaumont College - A Scope College | 27. The Congregation Of The Daughters Of The Cross Of Liege |
| 2. Bridge College, Manchester | 28. The David Lewis Centre |
| 3. Derwen College | 29. The National Centre for Young People with Epilepsy |
| 4. Doncaster Deaf Trust | 30. The Royal National College for the Blind |
| 5. Education and Services for People with Autism Limited | 31. Treloar Trust |
| 6. Exeter Royal Academy for Deaf Education | 32. WESC Foundation |
| 7. Fairfield Farm Trust | 33. William Morris Camphill Community |
| 8. Fortune Centre of Riding Therapy | |
| 9. Foxes Academy | |
| 10. Henshaws Society for Blind People | |
| 11. Homefield College Limited | |
| 12. Landmarks | |
| 13. Langdon College | |
| 14. Linkage Community Trust | |
| 15. Nash College | |
| 16. National Star Foundation | |
| 17. New College Worcester | |
| 18. Pennine Camphill Community Limited | |
| 19. Percy Hedley College | |
| 20. Portland College | |
| 21. Queen Alexandra College | |
| 22. Regent College Limited | |
| 23. RNIB College Loughborough | |
| 24. Ruskin Mill Trust Limited | |
| 25. Seashell Trust | |
| 26. The Cambian Group | |