Schools broadband connectivity and services

Toolkit to support your decision making v1.0

Northamptonshire Schools' Broadband working group

Summary

The present contract for broadband services comes to a natural end on 31st October 2012. You will need to have a new provider in place and have a direct contract with them.

There are two options: either purchasing directly from a choice of providers through a new framework agreement from embc or from another provider delivering a service tailored to the education sector.

This toolkit should help you through the process of selecting a provider. Suggested timeline:

January to April 2012

- Use the snapshots to help you decide where you are with your ICT development.
- Work out your requirements and note them down in the Requirements section.
- Liaise with potential providers to ensure that they will meet your needs, are cost effective and can help if you need to transition services to them.

April 2012 to August 2012

- With your preferred provider plan any transition work and reaffirm the start date of your new contract.
- You may need to sign a contract (without payment) with an overlap period to allow for transition. A new service provider may require several months notice as it takes time to order a line.

September 2012 to October 2012

- Ensure that the work is complete so that the new provider takes over the services on or before 1st November 2012 without any break in service.

Contents

What happens in October 2012?

The present contract with embc procured by the county council on behalf of Northamptonshire schools to provide broadband connectivity and services comes to its natural end on 31st October 2012. The county council has agreed a procurement strategy that allows both the county council and schools to separately purchase broadband connectivity and services.

Schools will need to choose their own broadband provider and service requirements from the end of the contract. A school will then have a direct relationship and contract with their provider. Options available:

- Purchasing directly from a choice of providers through a new framework agreement from embc.
- Purchasing from another provider delivering a service tailored to the education sector.

Doing nothing is not an option and you will have to make provision.

What do I need to do?

Each school will need to think about the broadband connectivity and services it currently receives and what it wants for the future in replacing those services.

We suggest that each school begins the process during the spring term in 2012 following the guidance in the “Steps to take” section. The sooner you can begin the process the easier it will be for you as you do not wish to be left without connectivity and services. There may be an overlap period required with a new provider for transition of services to that new provider, so that connectivity and services are not broken.

If you need any help, the Schools Broadband working group may be able to assist.

The Schools Broadband working group

The Schools Broadband working group was formed in response to requests from schools to investigate options available to schools for broadband connectivity and services after the end of the current contract. It was clear that schools wish to have choice in any future provision, whilst looking for best value for the services purchased. Schools wanted to be informed before the end of the current contract so that timely decisions can be made.

The group is made up of representatives from Primary schools, Secondary schools, Special schools, Early Years and Pupil Referral Units. It has considered requirements and sought the views of schools through a survey as it has developed this document and has been keeping schools informed via the factsheet on broadband developments as they happen.

The present contract until 31st October 2012

Services provided

The embc contract provides broadband connectivity and services, including identity management, filtered Internet and e-mail access. Schools are provided with the following services (although not all schools utilise the full provision):

- Secure managed broadband connectivity 24/7
- Regional educational network
- National Education Network – access to the dedicated network for use by UK education
- Accredited safe filtered access to the Internet which can be controlled and configured by each school.
- ISP services – Internet Service Provider
- embc portal – gateway to information and services
- Local authority portal – dedicated for local needs
- Mysite – personal space for every user
- embc email – hosted email service with built in anti-virus and filtering
- email filtering for school's own email servers
- Single sign-on and identity management – single username and password for services
- Web hosting – hosting a school's website
- Videoconferencing – 'click to meet'
- Service support desk – provides support for connectivity and applications services on the network
- Additional services – such CCTV and future Voice over IP telephony, purchased direct from embc

Benefits for all schools

- There has been investment to ensure that schools have been provisioned for broadband.
- Small schools have benefitted from the aggregated procurement that this regional contract brings since the cost for a single school to provide the quality of service and levels of filtering may be cost prohibitive. Rural schools have the same levels of bandwidth as those schools in more urban areas.
- The embc network is un-contended; this means that the line to the school isn't being shared with anyone else so is always available at the capacity (Mb) you have been provided with.

Charges for April 2012 to 31st October 2012

Schools will have received information from the county council regarding charges for the remaining period of the contract.

Safeguarding in schools

It is worth noting that the responsibility of safeguarding of children when using broadband services does reside with schools.

Any guidance used by schools must be in line with recommendations from UKCCIS, including the eventual replacement for the Becta Accreditation for Web Filtering.

Steps to take

Suggested timeline: January to April 2012

First thoughts

1. Look through the services provided and benefits on page 4 so that you have an understanding of the present services in your school and some of the reasons for those services needing to be in place.
2. Think about where you are in relation to your ICT plan?
3. Are there any budget constraints at this stage?
4. What do those around you think?

Snapshots

5. Look at the snapshots in Appendix A, which are based on the original Becta framework guidance for schools.
6. Decide on which snapshot fits you best?

Statement of requirement

7. Look at the detail in Appendix B against the snapshot you have chosen. We have drawn up a basic list of requirements for potential service providers to deliver this vision.
8. We suggest that you now read through the statement of requirements in Appendix C. You will notice that we have ticked the ones against the three snapshots, which should help to give you idea of what you may need.
9. However, bear in mind that the three snapshots are just that - snapshots of where you may be now. You will need to think about your school ICT development over the next few years and particularly for the duration of any contract you may sign.
10. The length of a contract that you may take will depend on the services provided, the cost and any discounts you negotiate for the length of the contract.

What are my own requirements?

11. It is best to go through the statement of requirements in Appendix C again, but this time to add in your own requirements in the column provided “My school requirements”, including your future needs in the next few years. You may not need all those requirements that have been ticked from the snapshots as these are only a guide.
12. Consider whether you are a campus school, need connectivity across several sites or need to work as a federation of schools.
13. Once you have determined your requirements we suggest that you consult with colleagues within the school to ensure that you have not missed anything.

Meeting with potential service providers

14. Arrange to meet with or find the information from a number of potential providers:
    - Discuss your requirements using Appendix C. Use the detail to ensure that you will receive what you expect. There is a glossary to help with technical terms and abbreviations which might be new to you.
    - Do the products and services meet the guidelines in the Becta requirements? (Appendix E).
    - What is the cost for each of the services, so that you can tailor your requirements?
    - Ensure that you have a true picture of what you will receive as it is important to compare like with like.
    - Are there any discounts for length of time or if bundles of services are selected.
    - Are there any discounts for schools working together in clusters?
    - What will the new provider do to help you transfer services and information from the current provider (if required) and what information is the school expected to provide? You will need to clarify:
        - The transition contact at the new provider.
        - If and when the new provider can or will get access to the settings and information you want to preserve.
        - How long will the transfer take?
        - What will the charge be for the transition?
15. Ensure at all times that you are following procurement guidance.
16. Have the potential providers submit an itemised price to meet your requirements along with a draft contract so that you can be sure that you will receive what you need.

Which provider do I choose?

17. It's important to keep in mind that you may not be able to meet all of your school's needs with one single provider. Will a single supplier provide all the services fully integrated?
18. Use the appendices to this guide to assess your requirement and inform your meetings with any providers. The table in appendix D will help you record the range of services offered by different providers. Also use the column "Services from which provider" to indicate your preferred provider for a particular service as you may use more than one provider to meet your needs.
19. What will the price be? This will depend on your requirements as you move forward. However, it is important to establish these requirements and then shop around before you sign any contract. It is important that you have understood all the 'small print' as you will be signing a contract with a commercial provider in the broadband market place.

Suggested timeline: April to August 2012

Working with a new provider

20. Once you have chosen your new provider you will need to begin the transition to their new services without any issues arising.
21. You may need to sign a contract (without payment until services are delivered) with a possible overlap period to allow for transition. We suggest an overlap of at least two months to enable a smooth transition. A new service provider may require several months notice as it takes time to order new lines into a school (possibly 3 months or more).

Transition of services to a replacement provider before the end of the contract

22. A toolkit for transition is planned to be available in the spring term, but you should have an outline of the process in mind when you speak to prospective providers.
23. Which services do you use that requires information to be stored somewhere?
    - Your school's Internet domain name.
    - Hosting of the school website.
    - Information which relates to public facing equipment on the school network, such as your own web server, which could include IP addresses and firewall ports.
    - embc mailbox contents for pupils and staff.
    - Custom Internet filter settings.
    - Custom email filtering settings.
    - Any information stored on the Mysite.
    - Single sign on applications.
24. Decide on what settings and information is important to preserve with a new provider.
25. You will need to clarify the transition contact with the current provider and any charges.
26. Develop a transition plan with your new provider and include milestones along with any training requirements.
27. Providing you work with your new provider in the period leading up to them taking over the services all should run smoothly at the hand over.

Suggested timeline: September to October 2012

28. Complete user training.
29. Ensure that any transition work is complete so that the new provider takes over the services on 1st November 2012 without any break in service.
30. Begin new contract with the Service provider no later than 1st November 2012.

Appendices

A - Snapshots

SNAPSHOT ONE		
The use of ICT helps some pupils to develop their creative abilities, search for information, draft their work and pay more attention to detail and presentation.	Some pupils make decisions about when to employ ICT in some subjects but often lack confidence to take their learning forward independently or to transfer their ICT capability to new situations.	Pupils generally have few expectations about using ICT as a natural part of their learning or about applying in school their experience of using various technologies at home.
Word-processing, Desktop-publishing, PowerPoint, Internet searches	The school's overall vision includes some reference to ICT but is unclear about expectations of ICT for learning and teaching. It has been shared with staff, but is understood and embraced by only some.	Pupil-owned devices such as iPod Touches and Mobile Phone not allowed in school
ICT is mainly used to replicate traditional teaching approaches.	There is no coherent strategy for the use of ICT to support communication. Practices mainly replicate traditional processes and meet the needs of some stakeholders.	A narrow range of ICT use across curriculum areas.
Non-interactive use of interactive whiteboards	The school has a website that is maintained by a single member of staff, who is responsible for updating its content.	Opportunities to use ICT are limited to timetabled use of a computer suite or shared laptops.
Internal and online connectivity to curriculum and management resources meets the user needs in line with current usage.	The school is aware of its responsibilities to provide a safe and secure ICT environment for its staff and pupils. There are relevant policies in place, including an Acceptable Use Policy, which are understood and adhered to by many staff and pupils.	Online learning platforms allow pupils access to content in lessons and at home. In school, they are able to access curriculum related resources and engage in activities when the timetabling of resources allows.
Some staff welcome and try new ideas but the outcomes are not generally incorporated into future curriculum planning. The sharing of effective practice of ICT use is encouraged but still works only at an individual level.		The school is aware that it has responsibilities with respect to Data Protection, Freedom of Information and Copyright Protection. Some procedures, designed to ensure compliance, are in place but only a few staff understand and implement these.

SNAPSHOT TWO		
For most pupils the use of technologies in a broad range of curriculum areas improves their creativity and ability to investigate, solve problems, refine their work, learn from their mistakes, collaborate with others and reflect critically on their learning.	Most pupils have reached high levels of confidence to apply ICT independently and where appropriate. They make informed decisions across the curriculum about when and how to use ICT.	Pupils have clear expectations about using ICT to support their learning and about sharing in school their existing knowledge and experience of using various technologies at home.
Learning platforms, blogs, wikis, digital video, Most staff use ICT to enhance teaching and learning experiences with approaches not readily accessible through more traditional methods. This leads to significant gains in learning. Online collaboration, video-conferences, web 2.0 software. There is secure, reliable and fast internal and online connectivity. This provides appropriate access to curriculum and management resources from many locations within the school. Schools recognise the the need to plan for updating infrastructure to meet future demands. Most staff engage in the development of new practices with ICT. Outcomes are shared and reviewed widely and are frequently incorporated into the curriculum. The sharing of effective practice routinely occurs across the school and with other schools.	The school's overall vision clearly identifies the distinctive contributions of ICT and their potential to enhance all aspects of the school's work. It identifies how ICT supports the school's wider aims and aspirations and is understood and embraced by most staff, governors and pupils. The school strategy identifies and promotes a range of electronic approaches, including online systems, for effective and appropriate communication both within and beyond the school. These are understood and used by a range of stakeholders. Virtual school tour, text-messaging service for parents, online surveys, school email used effectively. E-safety is embedded within the wider school culture. Policies are comprehensive and regularly reviewed in line with developments in technology and practice. There is coordinated and robust implementation of safeguarding policies by all staff, governors and pupils within and beyond the school and practice is monitored. The school engages regularly with parents/carers to promote the e-safety of pupils beyond the school.	Pupil-owned devices such as iPod Touches and Mobile Phones are considered potential tools for learning in school. Most pupils extend and improve much of their learning through a wide range of ICT experiences across many curriculum areas and contexts. Classroom technology toolkits and other innovative ways of increasing availability of appropriate technologies for learning. Online learning platforms allow pupils to access, create and share content in lessons and beyond school. Pupils are able to showcase achievement. Parents and carers have online access to resources and information. The school has published clear guidelines for staff - and where appropriate for pupils - outlining their responsibilities in relation to Data Protection, Freedom of Information and Copyright Protection.

SNAPSHOT THREE

For all or nearly all pupils the use of ICT, both within and beyond the school, significantly improves their creativity and ability to investigate, solve problems, refine their work, learn from their mistakes, collaborate with others and reflect critically on their learning.

All or nearly all pupils have reached high levels of confidence and independence to apply and develop their use of ICT. They make regular informed decisions across the curriculum about when and how to use ICT.

Pupils have have high expectations about using ICT to support their learning both within and beyond the school.

Learning platforms, blogs, wikis, digital video. Students as both producers as well consumers of learning and teaching content.

Most staff use ICT to enhance teaching and learning experiences with approaches not readily accessible through more traditional methods.

The school's overall vision includes the needs of the wider school community. It is informed by developments in ICT and exemplary educational practice nationally. It is understood and embraced by all, or nearly all, staff, governors and pupils and is supported by parents/carers and the wider community.

Pupil-owned devices such as iPod Touches and Mobile Phones are widely used for learning in school within clear guidelines.

Most pupils extend and improve much of their learning through a wide range of ICT experiences across many curriculum areas and contexts.

Global collaboration, video-conferences, web 2.0 software, live broadcasting, print-on-demand.

High-quality connectivity provides appropriate access to curriculum and management resources throughout the school and beyond. Regular review and updating ensure that new and growing demands are met. This enables innovative practice to develop which has a significant impact on the learning and management culture of the school.

Action research is embedded within a strong culture of planned and evaluated innovation. This encourages all or nearly all staff to take calculated risks in pushing the boundaries of the use of ICT to make significant improvements to learning, teaching and organisational effectiveness and efficiency. The school is successful in sharing practice within and beyond the school.

The school explores and exploits new and emerging technologies to ensure effective communication within, and beyond, the school. These are integrated effectively with other means of communication

Communicating with parents via Twitter, Facebook. Secure internet broadcasts of school assemblies. Virtual Parents evenings. Online payment for trips etc.

The school is vigilant in identifying and responding to new challenges for e-safety. Through constructive dialogue it encourages pupils, parents/carers, other stakeholders and the wider community to contribute to ongoing developments in e-safety policy and practice, and helps them to deal with e-safety challenges they encounter.

Opportunities to use ICT is available as required by pupils and teachers.

Online learning platforms support a wide range of innovative learning activities within and beyond the school. Regular review and updates incorporate new and emerging technologies and practices. All stakeholders have opportunities to access and exchange appropriate information and resources.

The school regularly reviews and updates its procedures relating to Data Protection, Freedom of Information and Copyright Protection. There is full compliance by all staff and pupils. The school takes steps to make parents/carers aware of current legislation.

B - Snapshots summary

Based on Snapshots using Self Review Framework (BECTA)

Snapshot	Vision	Snapshot summary	Requirements to deliver vision	Services to be provided at school	Key services from broadband provider
1	Includes some reference to ICT but is unclear about expectations of ICT for learning and teaching. It has been shared with staff, but is understood and embraced by only some.	• Curriculum network/computer suite • Office applications • Access to Internet • Access to some management resources • Website • Aware of security for staff and pupils • Some individual staff use online learning resources	• Internal network • Office suite • Internet connectivity • Access to some MIS • NCC Email access (for Head, Bursar, Senco) • Host website • Filtering for Internet • Curriculum resources available in school	• Managed service to support network (DNS, Public IP addressing) • Applications - Access to licensing • 2M bandwidth, Support helpdesk, training, documentation • On-network MIS (available to more than 1 PC) or hosted MIS • Minimum email accounts (SMTP gateway) • Hosted website • Internet filtering , firewall	➢ Internet connectivity (2M-4M) ➢ Internet filtering - managed ➢ Website hosting ➢ Helpdesk support with agreed reliability ➢ Email relaying for accounts ➢ Security safeguards (firewalls, not eCAF compliant)
2	Clearly identifies the distinctive contributions of ICT and their potential to enhance all aspects of the school's work. Supports school's wider aims and aspirations and	• Used by most staff to enhance teaching and learning • Sharing of resources and good practice • Office applications, Learning Platform, blogs, wikis, digital video • Fast internal and Internet access • Access to management resources within the school • Access from home and by	• Internal network • Pupils both consumers and producers • Learning Platform access • Internet connectivity • Access to full MIS • NCC Email access (for Head, Bursar, Senco) • Engage parents/carers	• Managed service to support network and external access 24/7 (DNS, Public IP addressing) • Upload speed same as download for Internet • Applications - Access to licensing • Access to Learning Platform (Hosted/in-house/cloud) • 4-10M bandwidth, Support helpdesk, training, documentation • Single network • Minimum email accounts (SMTP gateway) • Link to MIS (webparts)	➢ Internet connectivity (4M -10M upwards) ➢ Internet filtering - managed ➢ Website hosting ➢ Helpdesk support with agreed reliability ➢ Email relaying for accounts ➢ Email for pupils and staff ➢ Email filtering - managed ➢ Learning Platform access or hosting ➢ Access to NEN

	understood by most staff, governors, and pupils.	parents/carers to Learning Platform • Website • Safety embedded • online learning, web 2.0 software, Video Conferencing • School Email • Use of mobile technology such as smartphones and tablets	• Remote learning • Host website • Filtering for Internet /email • Curriculum resources available in/out of school • Email for staff and pupils • Secure internal network – wireless access	• Remote access to school resources • Hosted website • Internet filtering , firewall (VPN) • Fast broadband with VC facility • Email and filtering • Secure wireless access	➢ Security safeguards (firewalls, eCAF compliance) ➢ Fast broadband with VC facility
3	Identifies the needs of the wider school community. Informed by ICT developments and exemplary educational practice. Understood and embraced by all and is supported by parents/carers and the wider community.	• Used by all staff to enhance teaching and learning • Sharing of resources and good practice with global collaboration • Office applications, Learning Platform, blogs, wikis, digital video , print on demand • Quality connectivity - internal and Internet access • Access to management resources in/out of school • Access from home and by parents/carers to Learning Platform, broadcasts, online payments etc • Website • Safety embedded and	• Internal integrated network with wireless access • Pupils both consumers and producers in and out of school • Learning Platform access, learning tools • Seamless Internet connectivity • Access to full MIS • NCC Email access (for Head, Bursar, Senco) • Parental/carer engagement with access to tools for example to online payment • Host website • Filtering for Internet /email/	• Managed service to support network and external access 24/7 (DNS, Public IP addressing) • Upload speed same as download for Internet • Applications - Access to licensing • Access to Learning Platform (Hosted/in-house/cloud) • Applications • 10-40M bandwidth, Support helpdesk, training, documentation • Single network • Minimum email accounts (SMTP gateway) • Link to MIS (webparts), other applications for example online payment • Hosted website (blended with LP) • Internet filtering , firewall (VPN)	➢ Internet connectivity (10M -100M upwards) ➢ Website hosting ➢ Helpdesk support with agreed reliability ➢ Email relaying for accounts ➢ Email for pupils and staff ➢ School control of Internet and email filtering ➢ Learning Platform access or hosting ➢ Access to NEN ➢ Security safeguards (firewalls, eCAF compliance) ➢ Very fast broadband with VC facility ➢ Access for other groups – Health, Police etc

		responsive • online learning, web 2.0 software, VC, live broadcasts • School Email • Services and technologies overlap (blended) • Exploits new technologies	all applications • Curriculum resources available in/out of school • Remote learning • Email for all including governors and other community members • Secure network – guest access	• Very fast broadband with VC facility and to allow for broadcasting • Remote access to school resources • Email and filtering • Secure access	

Summary of Key Services: The Key Services above include one or more elements of a broadband connection. This list shows which elements make up each service. Numbers (in brackets) indicate the appropriate section in Appendix C.

- Internet connectivity 24/7 – Bandwidth (1), Contention ratio (2), Symmetrical (3), Latency(4), Router (5), IP (6), DNS (7), Access management (11),
- Internet filtering – managed – (13)
- Website hosting – (14)
- Helpdesk support – Service desk (9), Service Management (10)
- Agreed and guaranteed levels of reliability and resilience – Availability (8),
- Email relying for accounts – (15)
- Security safeguards (firewalls) – (12)
- Security safeguards (eCAF compliance) – (21)
- Email for pupils and staff – (16)
- Email filtering – managed – (17)
- Learning Platform access or hosting – (19)
- Access to NEN – (18)
- Video Conferencing facility – (20)
- School control of Internet and email filtering – (13, 16)
- Access for other groups – Health, Police etc – (25)
- Other services – Cloud based (22), Remote access (23), Single sign on (24), Mobile Services (26), Support for clusters (27), Support for Campus (28), Community Broadband (29).

C - Statement of Requirements

Schools need an educational Internet Service Provider (ISP) to supply Internet connectivity 24 hours a day, every day. The connection needs to handle access to media-rich resources such as Learning Platforms and to the school's Management Information System (MIS), and enable communication between the school population including parents. Schools should be able to choose from a range of services to meet their needs. The solution must provide for the future increases in capacity and capability. The services may be provided by a number of providers.

Requirement		Detail	Snapshot			My school's requirement
			1	2	3	
1	**Bandwidth**	Bandwidth is the rate of data transfer or "speed" of a broadband connection. What is needed varies with the size of school and school phase and the educational emphasis given to using ICT. *The DfE Review of Education Capital* by James (April 2011) suggested that primary schools require a minimum bandwidth of 10 megabits per second (Mbps) and secondary schools 100 Mbps. Demand in school is rising rapidly (over 40% per year). Bandwidth provided from ADSL (home broadband) to multi-Gigabit Ethernet is a function of the physical connection to the school, sometimes referred to as the edge circuit or tail circuit. This is usually either copper wire or optical fibre. The carrier, who owns the physical connection, sets costs based on what connections are available and the required bandwidth. The provider, who rents the connection from the carrier, should offer a choice of bandwidths and associated costs. Any contract must be flexible to meet future demand. After 3 years you may wish to move from 4 Mbps to 10 Mbps, so any contract must take into account future needs for increased bandwidth during the contract term. It should at least guarantee the initial bandwidth will be maintained in respect of factors like circuit degradation. Moving to a new broadband provider may involve a change in the physical connection, which may incur a set-up charge for engineering costs to dig up roads, install new cable ducts or run new cables.	✔ **4M**	✔ **10 M**	✔ **100 M**	
2	**Contention ratio**	Contention ratio is the number of users sharing a connection. For example; home users may share at a ratio of 50:1 and businesses may share at a ratio of 20:1. Schools should ask providers directly about their contention ratio, it should be un-contended at the point of use. An "up to 4Mb service" may be slower if you share it with others using the same	✔	✔	✔	

		line. It is important that no-one else shares the capacity between the school and the Internet.				
3	**Symmetrical or asymmetrical bandwidth?**	Bandwidth on an Internet connection operates in two directions, downloading (receiving) and uploading (sending). An asymmetrical connection normally means the upload speed is lower than the download speed. A symmetrical connection means the upload speed is the same as the download speed. Many schools use Learning Platforms, remote working, backup and videoconferencing (VC), all of which need good uploading bandwidth. Most schools require the bandwidth to be symmetrical.	✔	✔	✔	
4	**Latency**	Latency is the round-trip time for a request for data on the Internet to return. It is an important factor in the performance of hosted Management Information Systems (MIS) and online learning tools. Applications like VC require lip movement to be synchronised with sound. As a guide a total round trip time of 50 ms locally and 150 ms over the whole path should suffice.	✔	✔	✔	
5	**Router**	The provider should install a router at the school to enable Internet connectivity. This should be a fully managed device offering software and hardware maintenance linked to a specified service level agreement (SLA).	✔	✔	✔	
6	**IP Management**	Under the embc contract schools are provided with a set of IP network addresses, some of which are reserved for specific network devices or functions, as defined in the embc standard network build. If a school hosts its own website, Learning Platform or learning resources some of these internal addresses will need to be mapped to addresses visible to the public over the Internet. A new provider should let schools keep their existing IP address structure, or provide an equivalent defined structure. The provider must allocate and manage the public-facing IP address ranges. The solution needs to enable the use of Virtual Private Networks (VPN). This includes inter VPN access between schools to allow collaboration. This means secure network access to shared data and applications. The security controls at the boundary of each VPN should be compliant with the HM Government (HMG) security policy framework.	✔	✔	✔	
7	**DNS**	The Domain Name System (DNS) is what translates the words in Internet addresses like *www.myschool.northants.sch.uk* into IP network addresses. Many schools believe that the ".sch.uk" domain name used in their email address and/or web-site is owned by the Local Authority (LA) or their broadband provider. The LA doesn't own or have any other responsibility for schools' domain names. The current broadband provider may manage	✔	✔	✔	

		some or all aspects of the domain name administration. A new broadband provider should be prepared to take on the management of an existing ".sch.uk" domain. They should also provide a management facility for external (outward facing) DNS.				
8	**Agreed and guaranteed levels of reliability and resilience**	Schools and teachers need to be confident that connectivity is going to be available when needed so that on-line learning can take place. It would be expected that a school broadband connection should be available for over 99.9% of the time. Some providers offer a more resilient connection to allow for the loss of an Internet feed or when there is high demand on that Internet feed. The provider should also guarantee that the initial bandwidth will be maintained in respect of factors like circuit degradation. The security of the Internet connection must prevent the school from denial of service attacks and other network based threats and must be in line with HMG security standards. A service provider should offer a monitoring service and begin to restore service even before you report the fault. A school should have visibility of the network availability in real time and have regular service reports from the service provider (see 10). If there has been a break in service, the service provider should have agreed response and resolution times within the contract and keep the school informed of progress in dealing with the incident.	✔	✔	✔	
9	**Service desk support**	It is vital to understand the support that you should expect to receive from the provider. The main contact is through a dedicated Service desk (helpdesk), which should be responsive and sensitive to the needs of the school and willing to work with your ICT support provider. In any contract the provider to include but not be limited to: **1. A service desk** • A Service desk that follows IT Information Library (ITIL) and/or Framework for ICT Technical Support (FITS) best practice to deal with the day-to-day support for faults and service requests, and Incident Management, Problem Management, Configuration Management and Release Management processes for all offered services. • A Service desk system on which all faults and service requests are logged, to which all authorised customer personnel have access, enabling progress to be reviewed. • Clear and explicit charges for telephone access to support. • The ability to log faults via email and a website, with an automated email response to the school as a customer to acknowledge communication by these methods has been	✔	✔	✔	

		received. **2. First Line support** • Services provided. • Hours of Cover. • Methods for contacting the Service Desk (phone, online etc.). • How calls are answered (by person, by answer phone, hours covered by type of answer service, time to respond, etc.). • Service provided outside normal school hours, outside normal hours of cover, and on statutory holidays. • How service incidents / problems are prioritised and classified by level of severity, how progress is communicated, and how calls are closed. • Methods available to customers to monitor call status and progress. • Access to the same information in the monitoring service used by the provider. • Service Desk SLA and associated performance targets including service credits. • Customer responsibilities. **3. Second and Third Line support** • How calls are escalated if First Line cannot resolve the issue immediately • Further escalation processes including complaints • Access to this level by 3rd Parties acting on behalf of the school and authorised to do so.				
10	**Service management** **Change management** **Capacity management** **Service reporting**	The provider is responsible for the delivery and quality of services up to the router. The provider will ensure that services bought by the school are available as expected. The provider shall follow ITIL and/or FITS best practice for service, change and capacity management processes. The school shall supply all appropriate information to the provider to enable transition of existing services, user accounts, email etc. In any contract the provider to include but not be limited to: • Assurance that the services delivered meet the school's requirements and expectations. • Management of service quality provision to agreed service levels (SLA). • The process to raise, action and record change requests to the current services (e.g. a bandwidth increase) with expected time lines from request to implementation. • Pro-active monitoring of the services with alarms when faults affect services. The provider will ensure that the school receives the bandwidth that it has paid for, and that there are	✔	✔	✔	

		no further charges to restore degraded circuits. • Assurance that the provider has capacity to deliver the agreed levels and availability of services if overall demand for connectivity and services increases during the contract period. • Regular service reports and review (this may be through an on-line portal). • Billing directly to the school for all services chosen with availability of itemised charges.				
11	**Access management**	Some broadband services that schools choose to buy may require user authentication e.g. pupils may be required to login to receive the correct Internet filtering level. A provider must offer a suitable access management solution. The login process must lead to a "landing page" to show the process has completed successfully. The solution must be compatible with other systems with authorised access. The Identity solution should use the Schools Interoperability Framework (SIF) and the Zone Integration Server (ZIS) services for both 3rd party authentication and for user management. A new provider may offer to transfer existing user accounts to their service to ensure continuity, which may be useful if they link to other features such as email addresses. There is usually a charge for this transition.	✔	✔	✔	
12	**Security safeguards (firewalls)**	It is the school's statutory responsibility to make sure that appropriate safeguards are in place, under both child and data protection legislation. Pupils and staff need to be protected from inappropriate content and contact on the Internet. School data, personal data and the ICT system itself need to be protected from attack. In addition to barriers such as a firewall and filtering systems for web access and email, the school must have acceptable use, safeguarding and data protection policies in place. A firewall is commonly assumed to be "what protects computers from the Internet". It's a program or device which controls traffic passing into a network to protect it from unauthorised access. This is usually data passing to or from the Internet. The provider must offer a managed central Internet firewall, or a local firewall on the school network, or enable the school to maintain their own firewall. The firewall must ensure high network security, but be flexible enough at a school level to accept regulated changes to allow some types of traffic. There should be a process to request and manage changes to the firewall. This should include checks to make sure the changes are unlikely to expose the school, pupils or network to risk or	✔	✔	✔	

		harm.				
13	**Internet filtering – managed**	It is the school's statutory responsibility to make sure that appropriate safeguards are in place, under both child and data protection legislation. Pupils and staff need to be protected from inappropriate content and contact on the Internet. School data, personal data and the ICT system itself need to be protected from attack. In addition to barriers such as a firewall and filtering systems for web access and email, the school must have acceptable use, safeguarding and data protection policies in place. **No school should have an unfiltered Internet connection, even if they run their own filtering solution on the school network.** The school must make sure the ISP has **a minimum of the Internet Watch Foundation (IWF) watch list** in place. The IWF watch list is an optional service not a statutory requirement and not all ISPs subscribe. Filtering controls should NOT allow this to be turned off. The filtering solution should protect users, but allow access to appropriate material. It should provide granular levels of access to cater for the developing user and the requirements of different subjects and levels of courses. There may be separate levels of access for teachers and adults. It should use a list of permitted websites built up following review and categorisation including new websites as they occur. The filtering solution should provide records of users' web history for safeguarding purposes. Many schools want to be able to control the web filter directly at a local level. This level of flexibility requires an appropriate technical resource available in school, and is probably more appropriate to a secondary school. A typical primary school is more likely to need a fully managed filter service. The filter system must also take account of proxy anonymisers and proxy bypass. The filter system should filter "https" sites at URL level. The best current guidance on filtering is the Becta accreditation, although this is no longer an actively maintained resource. Advice is available from Child Exploitation and Online Protection (CEOP) at www.ceop.police.uk and the UK Council for Child Internet Safety (UKCCIS) at www.education.gov.uk/ukccis, but neither has yet provided an equivalent to the Becta guidance.	✔	✔	✔	

14	**Website hosting**	If your school has a website, where is it currently hosted? Most schools now have a web presence, which range in complexity from very simple sites to complex database solutions. If your current provider hosts your website, the new provider needs to offer an equivalent, appropriate service. Generally, the web hosting service must support both Microsoft and Linux operating systems with either Microsoft SQL and MySQL backend databases and support for at least following: C#, .NET, Java, PHP, Python, and Ruby. There will be charges to host the site, which may be linked to amount of data stored and/or traffic to the site. There may be additional support costs. If you are moving to a new provider they must offer to transfer the existing site. There is usually a charge for this transition.	✔	✔	✔	
15	**Email relaying for accounts**	An email relay service passes all outgoing email to its destination regardless of the sender's email address. To ensure that local email solutions operate as intended, including the Northamptonshire County Council provided email service (Head@, Bursar@ and Senco@ accounts), the service provider needs to offer the ability to relay emails from inside the school network.	✔	✔	✔	
16	**Email for pupils and staff**	It is the school's statutory responsibility to make sure that appropriate safeguards are in place, under both child and data protection legislation. Pupils and staff need to be protected from inappropriate content and contact on the Internet. In addition to email filtering the school must have acceptable use, safeguarding and data protection policies in place. Some schools' email systems are part of a bundle of services from their ISP or Learning Platform provider. Other schools have their own email server. Some use a web-based email solution, which can be accessed anywhere with an Internet connection and is maintained entirely by the provider. Web based systems ideally operates on a secure "https" address. All school email services must be subject to email filtering as described in 17. An email solution for pupils and staff should offer: • An individual email address for each user with an agreed format. • A number of generic email addresses for the school to use e.g. Information@. • Different mail-box sizes for pupils and staff e.g. in line with Microsoft's live@EDU product a minimum of 500Mb for pupils and 10Gb for staff. • Address lists or contacts. • Distribution Lists. • Allowance for attachments for type and size.		✔	✔	

		• Personal and shared Calendars. • Appropriate screens and tools for different user groups e.g. pupils and staff • The ability to send emails with different disclaimers based on the user. • Aliases. • Backup and recovery of email in the event of a fault. • Support from the provider. Email services are often charged on a per user basis. If you are moving to a new provider they must offer to transfer existing email, calendars and contacts to their service to ensure continuity. There is usually a charge for this transition.				
17	**Email filtering – managed**	It is the school's statutory responsibility to make sure that appropriate safeguards are in place, under both child and data protection legislation. Pupils and staff need to be protected from inappropriate content and contact on the Internet. In addition to email filtering the school must have acceptable use, safeguarding and data protection policies in place. All school email services including locally hosted email must have a filtering solution to protect both the user and the network from attack. The email filtering solution should offer: • Content filtering rules for all in-coming and out-going emails. The rules should be customised for different user groups e.g. pupils and staff. • The ability for the school to apply local filtering rules, for curriculum or other purposes. • The ability for the user to customise additional content filtering rules. • Filtering and validation of attachments including those that are password protected, to prevent spoofing. • Lexical (key word), anti-virus, malware, adware and SPAM analysis of all incoming emails • An alert to the recipient that an email has been identified as a threat e.g. SPAM. • The facility to suspend inbound email or quarantine potentially harmful email and store it for a defined period. • The facility to manage quarantined emails at school/site level. The best current guidance on filtering is the Becta accreditation, although this is no longer an actively maintained resource. Advice is available from Child Exploitation and Online Protection (CEOP) at www.ceop.police.uk and the UK Council for Child Internet Safety (UKCCIS) at www.education.gov.uk/ukccis, but neither has yet provided an equivalent to the Becta guidance.		✔	✔	

18	**Access to NEN services**	The provider should allow access to the National Education Network (NEN) services with its pool of free resources for schools. These include the Pathe library, audio material and safeguarding and online teaching and learning resources for all areas of the curriculum.		✔	✔	
19	**Learning Platform access or hosting**	Access to the school's Learning Platform or Virtual Learning Environment (VLE) can potentially lead to increased traffic on the broadband connection. You will need to consider the bandwidth requirement. If the VLE is hosted externally, users in school need to upload and download content, which may include large multimedia files. If the VLE is hosted internally users will need equivalent access from outside school. The bandwidth required may increase rapidly as users begin to take full advantage of the Learning Platform on the school network or from home. An internally hosted VLE will also need the provider to manage an external, public-facing IP address through which it can be accessed, and the host's DNS.		✔	✔	
20	**Videoconferencing**	VC provides a live multi-way audio and video connection with the scope to include shared documents, whiteboards and web pages to enable multi-location meetings, presentations and lessons to be held without having to leave your school. It is likely that schools will also begin to use high definition (HD) video conferencing services. Schools will need to purchase the appropriate equipment to work with the provider's solution. The provider should offer a solution to support the Janet Video Conferencing Service (JVCS) based H323 service and other video conferencing facilities. When the video conferencing solution is being used it should not have a detrimental effect on the bandwidth available for other users. This is managed through Quality of Service (QoS), where bandwidth to operate the service without degrading its quality is maintained and should be part of the solution provided.		✔	✔	
21	**Security safeguards (eCAF compliance)**	Data protection and other legislation, and standards such as ISO 27001, mean it is the school's responsibility to take reasonable measures to protect their systems, their own data, and data on other systems they may access e.g. the electronic Common Assessment Framework (eCAF). There may also be requirements from other parties based at, or making use of, the school. In addition to barriers such as a firewall and filtering systems for web access and email the school must have acceptable use, safeguarding and data protection policies in place. Schools need to abide by relevant standards to connect to external systems, as well as ensuring that any existing security analyses for systems such as eCAF are still met.		✔	✔	

22	**Cloud-based services**	Schools and service providers are looking at the developments in "cloud-based" services hosted remotely on the Internet, like email, office applications and remote back up. This will change the way we think about software and resources traditionally installed on computers or on-site, and will affect the cost of such applications and services. Access to cloud services requires the appropriate bandwidth, and schools are expected to use more cloud based services over the next few years. Any contract must be flexible enough to meet demand for future cloud-based services. It should also guarantee the initial bandwidth will be maintained in respect of factors like circuit degradation.			✔	
23	**Remote access**	Do your pupils and staff need remote access to the school network and applications? This may be provided using a Virtual Private Network (VPN). The provider should offer a range of authentication mechanisms from username and password to multi-factor authentication. The service must utilise remote access products that are certified and configured in line with FIPS140-2 and compliance with encryption requirements as specified in CESG Manual V and T guidance or their replacement Good Practice Guides.			✔	
24	**Single Sign On (SSO)**	Single Sign On means the user signs on to the network once but then has access to all the resources bought by the school that otherwise need a separate login, including third party resources. This should include admin access to web filter, email filter and network monitoring control systems. The provider should offer a range of authentication mechanisms from username and password to multi-factor authentication. The provider should also offer options including standards from UK Access Management Federation, as well as integration of directory services.			✔	
25	**Access for other groups – Health, Police etc**	Schools may have other organisations on the same site such as Police and Health. These third party organisations will require access to their own networks through the school network. The provider must offer a service enabling authorised end user organisations to access their own networks in a secure manner without affecting the school network. These organisations will require the capability of meeting all relevant GCSx and PSN standards and a single site may consist of VLANs for multiple organisations with differing PSN security requirements.			✔	
26	**Mobile services**	Some schools may wish to give access to the school network via a 3G dongle. The provider must offer a secure solution.			✔	

27	**Support for cluster working**	Your school may wish to work as part of a cluster of schools in order to work closely together to and share resources. Schools in this position should consider using the same service provider, or buying from the same procurement framework. The provider's solution must enable collaboration to happen securely and without affecting each school's independent services, filtering levels and access.			✔	
28	**Support for campus working**	A campus site is where more than one school shares a single broadband circuit. The router permits each school to have its own completely separate Local Area Network (LAN). The provider must offer a solution to enable suitable separation between each organisations LAN environment.			✔	
29	**Community Broadband**	Some schools may wish to be part of the local broadband community and offer a broadband community hub. Such provision will bring an extra demand on bandwidth requirements. Can the provider offer such support for a community option?			✔	

Glossary

Asymmetrical Bandwidth		The upload speed is lower than the download speed.	
Bandwidth		Rate of data transfer (speed) of a broadband circuit.	
Broadband carrier		Telecoms service which provides “wires in the ground”.	
Broadband provider		Company which sells Internet connection and other related services.	
Campus sites		One physical site where more than one school share a single broadband circuit.	
Child Exploitation and Online Protection	CEOP		www.ceop.police.uk
Cloud-based services		Services hosted remotely and accessed via the Internet.	
Contention ratio		The number of users sharing a connection.	
Domain Name System	DNS	What translates the words in Internet addresses like www.myschool.northants.sch.uk into IP network addresses.	
Dongle		A USB device which connects the PC or laptop to a wireless or mobile network.	
electronic Common Assessment Framework	eCAF		
Email relay		A service which passes all outgoing email to its destination regardless of the sender’s email address.	
Firewall		A program or device which controls traffic passing into a network to protect it from unauthorised access, usually between computers and the Internet.	
Framework for ICT Technical Support	FITS	A framework for best practice for service, change and capacity management processes in schools ICT support.	
Government	HMG		
High definition	HD		
Hypertext transfer protocol	http	The basis of data communication on the world wide web.	
Secure Hypertext transfer protocol	https	Web sites handling secure data e.g banks.	
Internet Protocol	IP		
Internet Service Provider	ISP		
Internet Watch Foundation	IWF	In independent, un- legislated, non-statutory body which provides a “watch list” used as a minimum filtering level by voluntary participating ISPs.	

IT Information Library	ITIL	A framework for best practice for service, change and capacity management processes in the IT support industry.	
Janet Video Conferencing Service	JVCS		
Latency		The round-trip time for a request for data on the Internet to return.	
Local Authority	LA		
Management Information System	MIS		
Mega bits per second	Mbps	Measurement of bandwidth.	
National Education Network	NEN		
Quality of Service	QoS	The graded levels of priority given to different types of Internet data.	
Router		A device that connects two networks, usually the device which connects a PC or network to the Internet.	
Schools Interoperability Framework	SIF	Standard for user authentication between systems.	
Service Level Agreement	SLA		
Single Sign On	SSO	The user only signs on to the network once but then has access to all the resources, including an increasing list of third party resources bought by schools, that otherwise need a separate login.	
Symmetrical Bandwidth		The upload speed is the same as the download speed.	
Simple Mail Transfer Protocol	SMPT	The standard protocol for email over the internet.	
UK Council for Child Internet Safety	UKCCIS		www.education.gov.uk/ukccis
Uniform or universal resource locator	URL	A web address.	
Videoconferencing	VC	A live multi-way video and audio link to enable meetings, presentations and lessons to be held without having to leave your school.	
Virtual Learning Environment	VLE	An online environment containing, but not limited to, file storage space and learning resources.	
Virtual Private Network	VPN	Devices on a network are grouped together and act as if they are on a separate, self-contained network.	
Web 2.0	Web 2.0	The “second generation” of web sites and applications which allow user participation and collaboration.	
Zone Integration Server	ZIS	Standard for user authentication between systems.	

D - What do providers offer

	Requirement	Potential Providers					Services from which provider
		A	B	C	D	E	
1	Bandwidth (rate of data transfer or speed)						
2	Contention ratio						
3	Symmetrical or asymmetrical bandwidth?						
4	Latency						
5	Router						
6	IP Management						
7	DNS						
8	Agreed and guaranteed levels of reliability and resilience						
9	Service desk support						
10	Service, Change, Capacity management Service reporting						
11	Access management						
12	Security safeguards (firewalls)						
13	Internet filtering – managed						
14	Website hosting						
15	Email relying for accounts						
16	Email for pupils and staff						
17	Email filtering – managed						
18	Access to NEN services						
19	Learning Platform access or hosting						

20	Videoconferencing (VC) facility						
21	Security safeguards (eCAF compliance)						
22	Cloud based services						
23	Remote access						
24	Single Sign On (SSO)						
25	Access for other groups – Health, Police etc						
26	Mobile services						
27	Support for cluster working						
28	Support for campus working						
29	Community Broadband						

E - Becta - Accreditation of Internet Services requirements

The purpose of this accreditation is to identify Internet services and products that offer functionality which meets or exceeds a set of published minimum requirements related to Internet safety. These are currently under review by the Department for Education.

Managed Internet service requirements

A managed Internet service must meet or exceed the following requirements as a minimum under the Becta Accreditation of Internet Services.

Internet Watch Foundation Child Sexual Abuse Images and Content (CAIC) list

It is a requirement of this accreditation that the Internet Watch Foundation CAIC list is implemented in all accredited products and services.

Illegal content blocked

The product or service must block 100% of illegal material identified by the Internet Watch Foundation.

Inappropriate content blocked

The product or service must be capable of blocking at least 90% of inappropriate Internet content in each the following categories:

- **Adult**: content containing sexually explicit images, video or text, the depiction of actual or realistic sexual activity
- **Violence**: content containing graphically violent images, video or text
- **Race hate material**: content which promotes violence or attack on individuals or institutions on the basis of religious, racial or gender grounds
- **Illegal drug taking and the promotion of illegal drug use**: content relating to the use or promotion of illegal drugs or misuse of prescription drugs
- **Criminal skill/activity**: content relating to the promotion of criminal and other activities
- **Gambling**: content relating to the use of online gambling websites or information relating to the promotion of gambling and gambling advice.

Change requests to the filtered content

- There must be a mechanism for an **authorised** member of a customer organisation to request amendments to the web content filtering service
- The appropriate procedures must be in place to authenticate personnel that request changes to any part of the service.

Availability

- Internet connectivity must have a high degree of availability, eg. 98% or no more than 31.5 hours downtime per year. (This figure is calculated as 98% of the hours from 196 term days)
- The connection to the Internet must be capable of sustaining a bandwidth of at least 75% of its stated bandwidth.

Web hosting

- The Internet provision must also make available a web site hosting service for those customers who require it.

Email requirements

- Applicants must provide, if required, sufficient email accounts to allow each person within the end user organisation to have at least one email account
- The email service must be capable of providing each user with a mailbox that can hold at least 20MB of email
- The service or product must provide end user organisations with the ability to allow the use of email addresses that protect the anonymity of individuals, if requested.
- External and internal, incoming and outgoing email messages with inappropriate words in either the subject or message body must be filtered or blocked.

Security and virus protection

The service or product should include adequate protection against the following:

- External malicious attacks
- Viruses and trojans
- Denial of service attacks
- Email bombs and spam.

Support requirements

- Single point of contact for the entire service is required
- Support must be available through two channels: telephone and e-support (e-support includes email and or web-based contact methods)
- All support requests must be acknowledged within two working hours and assigned a unique reference number
- A first attempt to resolve the support request takes place within the first four hours.

Other areas that require compliance include system availability and capacity, service continuity, service management, customer service and requirements for Becta to have the appropriate access to any given service or product to enable monitoring evaluations to take place at any time during the accreditation period.

Web content filtering products and services requirements

A web content filtering product or service must meet or exceed the following requirements as a minimum under the Becta Accreditation of Internet Services.

Internet Watch Foundation Child Sexual Abuse Images and Content (CAIC) list

It is a requirement of this accreditation that the Internet Watch Foundation CAIC list is implemented in all accredited products and services.

Illegal content blocked

The product or service must block 100% of illegal material identified by the Internet Watch Foundation.

Inappropriate content blocked

The product or service must be capable of blocking at least 90% of inappropriate Internet content in each the following categories:

- **Adult**: content containing sexually explicit images, video or text, the depiction of actual or realistic sexual activity
- **Violence:** content containing graphically violent images, video or text
- **Race hate material:** content which promotes violence or attack on individuals or institutions on the basis of religious, racial or gender grounds
- **Illegal drug taking and the promotion of illegal drug use:** content relating to the use or promotion of illegal drugs or misuse of prescription drugs
- **Criminal skill/activity:** content relating to the promotion of criminal and other activities
- **Gambling:** content relating to the use of online gambling websites or information relating to the promotion of gambling and gambling advice.

Changes requests to the filtered content

- The must be a mechanism for an authorised member of a customer organisation to request amendments to the web content filtering service
- The appropriate procedures must be in place to authenticate personnel that request changes to any part of the service.

Security and virus protection

The service or product should include adequate protection against the following:

- External malicious attacks
- Viruses and trojans
- Denial of service attacks
- Email bombs and spam.

Support requirements

- Support must be available through two channels: telephone and e-support (e-support includes email and or web based contact methods)
- All support requests must be acknowledged within two working hours and assigned a unique reference number
- A first attempt to resolve the support request takes place within the first four hours.

Other areas that require compliance include system availability and capacity, service continuity, service management, customer service and requirements for Becta to have the appropriate access to any given service or product to enable monitoring evaluations to take place at any time during the accreditation period.

Email filtering products and services requirements

An email filtering product or service must meet or exceed the following requirements as a minimum under the Becta Accreditation of Internet Services.

Email filtering

- Incoming and outgoing email messages with inappropriate words in either the subject or message body must be filtered or blocked
- Messages passed from user to user within the same organisation that contain inappropriate words in either subject or message body must be filtered or blocked
- Keyword list is maintained and updated regularly.

Email capacity

- The email service must be capable of providing each user with a mailbox that can hold at least 20MB of email
- The email service must allow its users to send and receive email messages with attachments which are at least 5MB in size.

Support email address anonymity

The service or product must provide end user organisations with the ability to allow the use of email addresses that protect the anonymity of individuals, if requested.

Security and virus protection

The service or product should include adequate protection against the following:

- External malicious attacks
- Viruses and trojans
- Denial of service attacks
- Email bombs and spam.

Incoming and outgoing email messages infected with a virus, or with a virus infected attachment, must either have the infected file removed or the entire email must be blocked.

Support requirements

- Support must be available through two channels: telephone and e-support (e-support includes email and or web based contact methods)
- All support requests must be acknowledged within two working hours and assigned a unique reference number
- A first attempt to resolve the support request takes place within the first four hours.

Other areas that require compliance include system availability and capacity, service continuity, service management, customer service and requirements for Becta to have the appropriate access to any given service or product to enable monitoring evaluations to take place at any time during the accreditation period.