Meeting Digital Standards in Northumberland Schools

Summary

There have been a number of updates from the DfE to Keeping Children Safe in Education (KCSIE) and Meeting Digital Technology standards in schools and colleges.

This pack aims to draw together information on how the Broadband service meets DfE requirements and how other associated SLA's provide additional resources, support and guidance to support your school with its online safety provision.

Throughout the pack you will find a QR code and link which will take you to the Northumberland ICT Team website which has a digitised version of these documents.

Schools in SLA3 (Online Safety) should visit the Northumberland Online Safety website for regularly updated, more detailed guidance around online safety as a whole, including filtering and monitoring, your curriculum and staff training opportunities.

At the end of the pack are contact details for colleagues from the Curriculum ICT and Digital and IT teams.

Note:
Schools not in the Local Authority SLA 4 broadband must ensure that their current provider meets the standards prescribed by the DfE.

Standards

Guidance on Digital Technology Standards in Schools

This document contains information covering: **Meeting digital and technology standards in schools and colleges: Broadband Standards and Filtering and Monitoring standards - as signposted by the DfE's Keeping Children Safe In Education.**

This is the first part of the pack and takes each of the DfE Broadband and Filtering and Monitoring standards and adds a Local Authority response which explains how the demands are met. The remainder of the pack are A4 posters which cover:

1. The Northumberland Community of Schools.
2. Commsworld: Our Internet Service Provider.
3. Performance of the Network.
4. Dealing with an incident (Flow Chart).
5. Filtering Overview - managing your access to the internet.
6. Monitoring and Reporting Overview.
7. Online Safety CPD - courses, training and support for staff.
8. The Northumberland Online Safety Audit.
9. The NCC Schools' Broadband SLA: pricing and contract length.
10. Contacts - contact details for technical issues and for

monitoring, reporting and filtering issues.

Broadband Standard One: Schools and colleges should use a full fibre connection for their broadband service

Schools should use a full-fibre connection for their broadband service. Full fibre services provide the capacity and speed needed for the effective use of online learning tools.

Primary schools should have a minimum 100Mbps download speed and a minimum 30Mbps upload speed. Secondary schools, all-through schools and further education colleges should have a connection with the capacity to deliver 1Gbps download and upload speed.

The requirement is fully met by the Broadband SLA. SLA 4 exceeds the standard for primary schools, by providing a 1gb full fibre connection to all First, Primary and Special schools through our partnership with Commsworld. Secondary schools have bespoke arrangements with Digital and IT to ensure standards are met, including greater upload bandwidth.

Contact the Digital and IT help desk If you have any technical enquiries relating to your broadband connection.

phone 01670 627004
https://customer.hornbill.com/northumberland

Dependencies

Actions schools need to take for themselves.
Following your 1Gb upgrade, the speed of the internet may still vary. This can be caused by several factors, outside the control of the Local Authority Broadband service provider. Internal network cabling, switches and old network equipment such as routers and wireless access points, can all have a dramatic effect on the the performance of computers within the school.

This is an important issue and one which is the school's responsibility to address. Technical support contracted by the school should review key *elements, such as internal switches and wireless infrastructure to ensure they are not restricting internal network traffic. Schools need to make arrangements to review their internal network infrastructure, requesting a report from their technical support.*

Broadband Standard Two: Schools and colleges should have a backup broadband connection to ensure resilience and maintain continuity of service

Schools and colleges should have a backup broadband connection to ensure resilience and maintain continuity of service. With increasing reliance on Internet-based services, broadband internet is an essential service. Schools should ensure that appropriate measures are in place to mitigate against a single point of failure.

The Local Authority solution does not rely on BT for connection but rather is connected to a private wide area network owned and managed by Commsworld. This has several features which provide greater resilience. Triangulating additional connection node points, so that if an individual node goes down, it is backed up by the other connection on the node. If the fault cannot quickly be resolved, then the Local authority has a temporary mobile network solution which can be deployed allowing schools to access critical systems while any issues are resolved.

Broadband Standard Three: Schools and colleges should have appropriate IT security and safeguarding systems in place, under both child and data protection legislation

It’s essential that children are safeguarded from potentially harmful and inappropriate online material. An effective whole school and college approach to online safety empowers a school or college to protect and educate students and staff in their use of technology. It establishes ways to identify, intervene in, and escalate any concerns where appropriate.

You should talk to your supplier or in-house support team to ensure that you have a content filtering system in place which meets the requirements outlined in the online safety section of keeping children safe in education, paragraphs 123-135.

You should also ensure that you have a firewall as part of your internet and network system. This could be an on-premises device directly protecting your network and directly managed by the school or college. It also might be an ‘edge’ service provided and managed by your supplier or in-house support team.

The Northumberland Broadband SLA, in conjunction with the online safety SLA (SLA 3) supports and promotes the whole school approach to online safety. For the protection of pupils, staff, equipment and data, the Northumberland Broadband service provides a high-speed secure network which provides sophisticated filtering of the Internet, coupled with monitoring software which provides reports of Internet usage.

The ICT and e-learning team provide training on the filtering, monitoring and reporting system. Alongside this, we provide additional training for all staff and governors on online safety, including courses introducing AI, Teaching Online Safety, Cyber Essentials and an annual online safety update. We provide a variety of software for the school to effectively audit and monitor their whole school online safety provision and an online safety website providing guidance and resources to support schools as they develop their whole school approach.

The multi-layered approach to online safety and security involves
all sites being provided with the following, via the broadband sla and online safety SLA.

- *School’s own firewall*
- *Fortiguard filtering and monitoring software*
- *Senso monitoring and reporting software*
- *Lightspeed MDM (Mobile Device Manager)to manage iOS devices.*
- *The set up of Apple Classroom to monitor iPad activity in the classroom.*

- *A three-fold approach to monitoring and reporting including a monthly internet activity report, email notifications and the facility to request further investigation into internet traffic for a specific user or device.*

Please contact the ICT and eLearning Team at: onlinesafety@northumberland.gov.uk to ensure these systems are set up for the relevant persons at your school.

Associated training is provided for all schools in SLAs 3 and 4.

Filtering and Monitoring Standard One: Identify and assign roles and responsibilities to manage your filtering and monitoring systems

Schools and colleges should provide a safe environment to learn and work, including when online. Filtering and monitoring are both important parts of safeguarding students and staff from illegal, inappropriate and potentially harmful online material.

Clear roles, responsibilities and strategies are vital for delivering and maintaining effective filtering and monitoring systems. It’s important that your designated safeguarding lead (DSL) and IT support work together, using their professional expertise to make informed decisions. Governors and your senior leadership team (SLT) should provide support as required.

The Northumberland ICT and eLearning team advise forming an online safety group comprising of any individuals playing a role in the development of your online safety provision. Including your DSL, technical support, policy makers and the member of staff overseeing your online safety curriculum. You will find a template on the online safety website. This will help you outline roles and responsibilities clearly and create a schedule and itinerary for group meetings.

Filtering and Monitoring Standard Two: Review your filtering and monitoring provision at least annually

For filtering and monitoring to be effective it should meet the needs of your students and staff. It should reflect your specific use of technology while minimising potential harms.

To understand and evaluate the changing needs and potential risks of your school or college, you should review your filtering and monitoring provision at least once every academic year.

Schools should carry out a risk assessment to ensure filtering and monitoring meets the needs of your staff and pupils. Template available via the online safety website.

The Northumberland Online Safety Audit is available to all schools in SLA3. One of the six categories is dedicated to auditing your network, devices and software. If you don't yet have access to this tool please contact a member of the Northumberland ICT and eLearning team.

It is vital that you test filtering and monitoring systems are working as expected at least annually. testfiltering.com will help you to verify that your internet filter is blocking illegal, harmful and inappropriate content.

Filtering and Monitoring Standard Three: Filtering systems should block harmful and inappropriate content, without unreasonably impacting teaching and learning

An active and well-managed filtering system is an important part of providing a safe environment for students to learn. No filtering system can be 100% effective. You need to understand:

- your filtering system’s coverage
- any limitations

You should mitigate against these limitations to minimise harm and meet your statutory duties in the filtering and monitoring section of Keeping children safe in education and the Prevent duty guidance: England and Wales (2023)

An effective filtering system needs to block internet access to harmful sites and inappropriate content. It should not:

- unreasonably impact teaching and learning or school or college administration
- restrict students from learning how to assess and manage risk themselves

The filtering solution employed by the Northumberland broadband service is provided by Fortinet.

Fortinet:

- *Are Internet Watch Foundation (IWF) members*
- *Block access to illegal content including child sexual abuse material (CSAM) using the IWF url list.*
- *Use the counter-Terrorism Internet Referral Unit list (CTIRU)*
- *Are one of the leading providers of filtering for both business and education sectors.*
- *Fortinet uses physical devices called Fortigates on each school site to filter and provide a firewall for all of the web traffic into the school.*
- *Sites are automatically categorised, if the site falls into a blocked category, that site will automatically be blocked.*
- *Main blocked categories for inappropriate content include: Discrimination, Drugs / Substance abuse, Extremism, Gambling, Malware / Hacking, Pornography, Piracy and copyright theft , Self Harm, Violence.*

It is important to point out that no filtering system is 100% effective. Schools should ensure that staff and pupils understand what to do in the event of *accessing material deemed inappropriate for the school network. This should be embedded in your online safety curriculum. Teachers should also know how to request that a site is reviewed and potentially allowed in school if they feel it has been blocked in error.*

In both cases a designated member of staff can contact Digital and IT to request that a site be allowed or blocked in school. The school should keep a record of these amendments.

phone 01670 627004
https://customer.hornbill.com/northumberland

Filtering and Monitoring Standard Four: Have effective monitoring strategies that meet the safeguarding needs of your school or college

Monitoring user activity on school and college devices is an important part of providing a safe environment for students and staff. Unlike filtering, it does not stop users from accessing material through internet searches or software.

Monitoring allows you to review user activity on school and college devices. There are both technical and manual solutions. Which solution your school or college uses will depend on your educational setting, including:

- student age
- student risk profile
- whether screens are easy to see
- number of devices in use
- whether devices are used off-site, for example, at home

For monitoring to be effective it must pick up incidents that are of concern urgently, usually through alerts or observations, allowing you to take prompt action and record the outcome.

The Northumberland ICT and eLearning team provide a multi layered approach to monitoring and reporting.

Schools receive a monthly web usage report. These reports provide an overview of your network activity, they are a good place to start in identifying trends and anomalies that you may decide require further investigation.

Senso is a cloud based remote monitoring and management tool developed specifically for schools. Senso monitors Chrome and Windows devices. Key members of staff in each school have a Senso Safeguarding account, this allows them to receive regular reports outlining internet activity for their school as well as notifications relating to activity that requires urgent attention.

Fortinet email alerts: While your PCs and Chromebooks are monitored by Senso, this is not currently the case for iPads. Tablets operate differently to windows and chrome devices, iPads in particular have security and privacy settings that are fantastic for personal security, but have made developing a usable monitoring solution challenging. We are able to set up alerts that generate an email in the event that a user attempts to access a website belonging to a blocked category. We can also set up alerts that are triggered when a key word is entered, however, this is only possible if the school has deep packet inspection enabled on their network. DPI is only suitable in certain cases as it can impact other systems. Please contact us if you have any questions about this.

We strongly recommend schools also set up Apple Classroom to aid the monitoring of pupil online activity. With this in place, classroom teachers are able to monitor pupil screens from their designated teacher iPad.

Please ensure that these monitoring and reporting methods are set up and are working correctly in your school.

Contact onlinesafety@northumberland.gov.uk if you have any queries.

Please note that while this document outlines the ways in which the Northumberland Schools' Broadband Service meets the Broadband Standards and Filtering and Monitoring Standards, schools should review **'Meeting digital and technology standards in schools and colleges'** in its entirety with support from the organisation that manages their school network.

At the time this NCC guide was printed, the DfE document had last been updated on the 6th November 2024 and included the following:

- Broadband internet standards for schools and colleges
- Cloud solution standards for schools and colleges
- Cyber security standards for schools and colleges
- Digital accessibility standards
- Digital leadership and governance standards
- Filtering and monitoring standards for schools and colleges
- Laptop, desktop and tablet standards
- Network cabling standards for schools and colleges
- Network switching standards for schools and colleges
- Servers and storage standards for schools and colleges
- Wireless network standards for schools and colleges

Please visit the Northumberland Online Safety website to access regularly updated information to help you develop your whole school approach to online safety.

Notes

Northumberland ICT & eLearning

Northumberland County Council