Whitepaper

Digital Safety Excellence in an Independent School

The key components every DSL needs to know

Essential reading for:

Headteachers, DSLs and anyone responsible for online safety in an independent school

Whitepaper

Contents

About This Document

Do you know what it takes to implement excellent digital safety standards? Do you know the difference between basic and advanced policies?

To properly keep students safe online goes far beyond minimal compliance. It should never be a tick in a box approach.

Online dangers are not going away and those schools with a child-centred approach to safeguarding understand this, and take great care to ensure students and staff are protected at every digital touch-point.

Creating a standardised model of online safety excellence is vitally important for independent schools. The benefits are far reaching.

- Student safety
- Network and data security
- Ofsted and ISI compliance
- Reputation
- Reassurance to parents
- High academic attainment
- Improved student behaviour.

This guide has been prepared by Smoothwall's online safety experts to help safety leaders in independent schools understand what excellence looks like and the steps needed to raise standards across their school in the most time and cost-efficient way.

It is designed to help your school become a beacon of excellence in online safety.

Essential reading for:

Headteachers, DSLs, Governors and anyone responsible for online safety within an independent school environment.

If you have any questions about your online safety solutions or online safety in general, please do not hesitate to contact the Smoothwall team.

We'd be happy to help.

Tel: +44 (0)870 1999 500
Email: enquiries@smoothwall.com
Web: www.smoothwall.com/contact

smoothwall®

1.0 The Safeguarding Characteristics of an Independent School

Independent schools have several unique factors that make high standards of online safety vitally important.

Data risks

Schools with parents and/or students in the public eye could be at a higher risk of hacking due to the value of personal information held. Data privacy is key, as is effective anti-ransomware and anti-malware functions.

Parental expectations

With fees rising 65% in the last 10 years[1] and with more than one school in any region to choose from parents naturally have high expectations. Facilities, grades and pastoral care are important. But increasingly so too is online safety.

Reputation

The number of incidents in the media relating to online safeguarding in independent schools is increasing. Recent stories have included County Lines, drug dealing within school, peer on peer abuse, cyber-bullying, self-harm and staff/pupil inappropriate relationships. Such issues can be very public for private schools with parents expecting the very best in return for the fees they pay.

Loco parentis and out of hours

Schools with children in loco parentis have a 24/7 responsibility for safeguarding. There is a need to vary safeguarding according to age group, time of day, and location and for this to be manageable by staff when the IT team have gone home.

Bring your own device

Many day schools issue devices for home use. But many students prefer to bring in their own high spec devices. It's important to communicate with parents about the importance of online safety. Devices going off-site could pose a risk to the school network if they are not suitably protected.

Peer pressure

Peer pressure can be very strong especially when students are living and studying together. Effective digital monitoring allows schools to detect early stage situations such as an interest in drugs, before the problem escalates.

1. Higher Education Policy Institute. 2018. https://www.hepi.ac.uk/2018/01/22/lessons-higher-education-private-quasi-private-schools/

2.0 Digital Safety - The Excellence Model

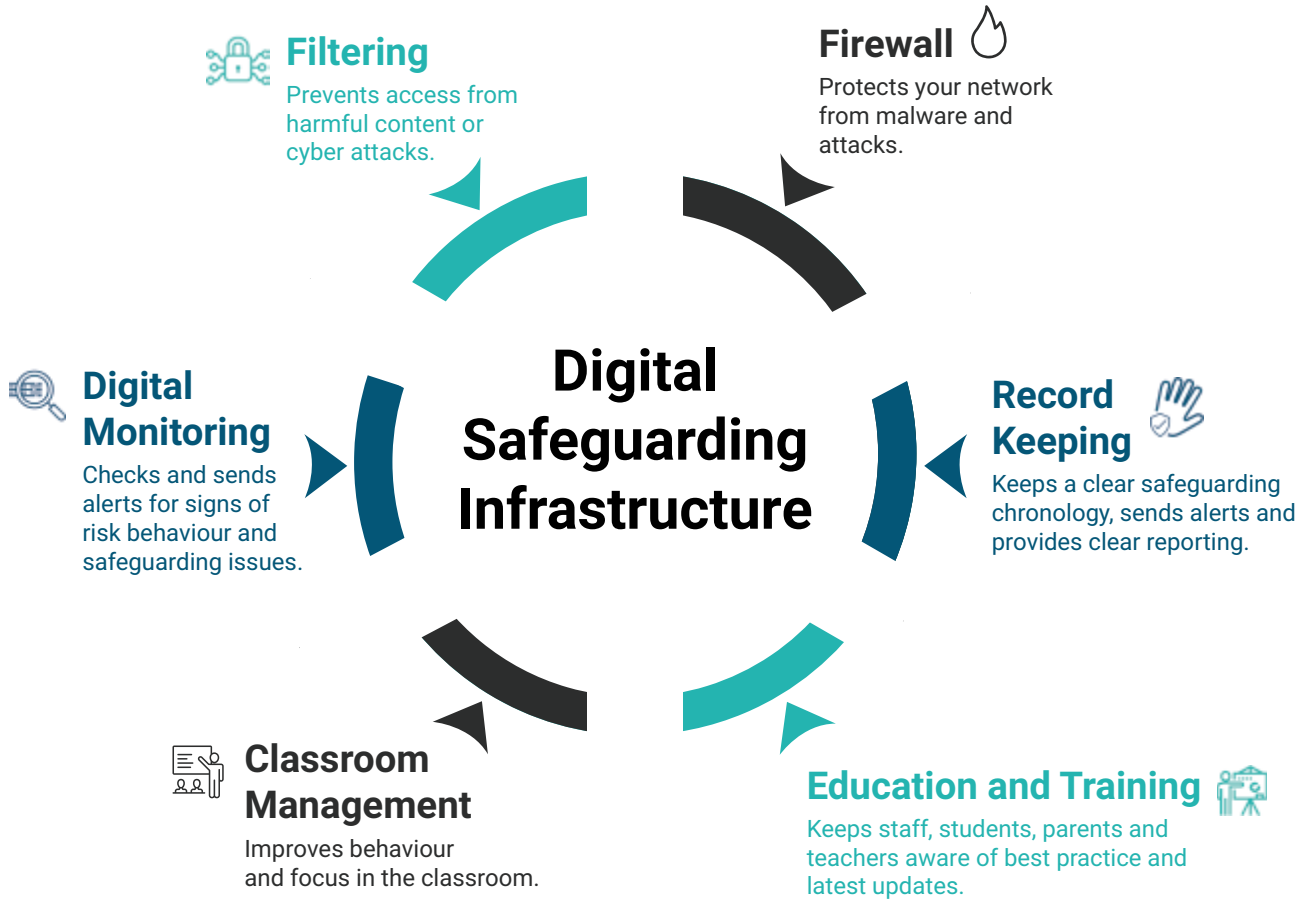
Simply meeting the minimum statutory requirements for safeguarding does not protect an independent school from digital risk in today's climate. It requires a multi-level approach.

An effective online safety infrastructure is made up of six harmonising components which combine to support students, staff and network safety - at every touch-point.

While some schools will be ready for a digital safeguarding infrastructure, others may prefer to journey towards it over time, or will only ever require certain elements of it.

Regardless of where you are on your excellence journey understanding each component is fundamental to improving your overall safety provision.

Over the following pages we review each component in turn, comparing basic versus advanced provision and helping DSLs to make more informed decisions relative to each.

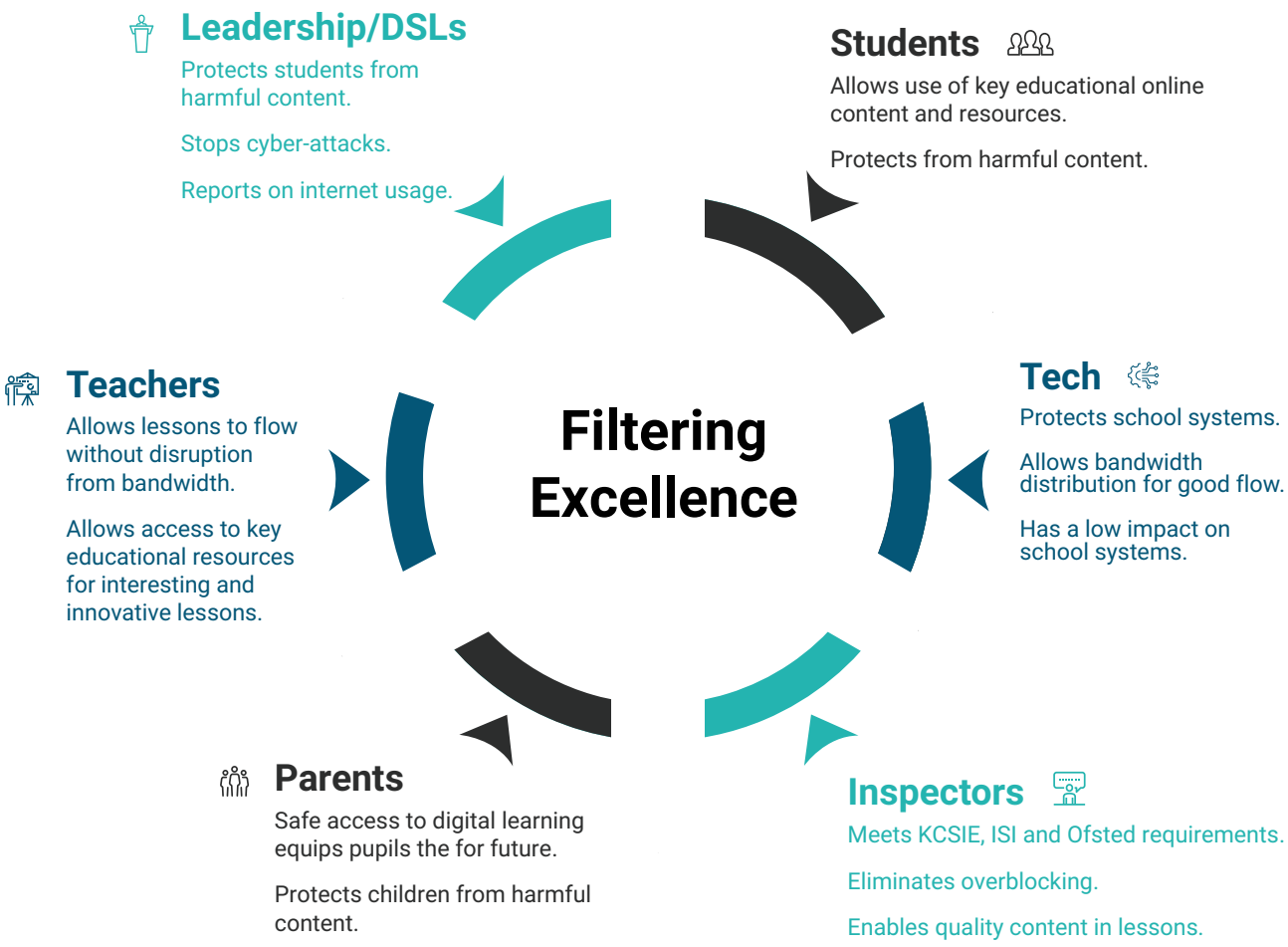


To properly keep students safe online goes far beyond minimal compliance. It should never be a tick in a box approach.

2.1 Web filtering

Although filtering is a statutory requirement, not all filters are alike. A basic web filter can expose independent schools to significant risk, both to student well-being, academic attainment, network protection and reputational damage.

Advanced filtering, on the other hand, has far reaching benefits that impact on the whole school community.



Basic vs advanced filtering

The following table explains the common differences between basic and advanced filtering.
Do you know if your school's web filter is giving you the protection you need?

Basic filtering	Advanced filtering
Blocklist filtering Blocklists can be out of date leading to harmful content being accessed. Can also cause over-blocking as the system cannot see beyond the URL.	**Dynamic filtering** Sees beyond the URL to analyse web page content, context and construction, in real-time. Avoids over-blocking, prevents harmful content and promotes learning.
Circumvention Basic systems can be circumvented by capable students via VPNs and proxy filters.	**No circumvention** Advanced filters cannot be circumvented.
Device coverage May not cover all devices or have only limited function.	**Device coverage** Will usually cover all device requirements including iOS and tablets.
Bandwidth limitation Can be demanding on network bandwidth leading to slow or crashing machines during lessons. Lessons involving media content or high content file exchange are especially vulnerable.	**Real-time bandwidth allocation** Bandwidth allocation minimises slow service. More bandwidth can be given dynamically to those classes who need it.
User settings May not allow the variable settings needed to accommodate different age ranges and settings.	**Variable settings/reports** Allows for variable filtering provision for different ages, groups or physical settings such as boarding houses.

Continued.

Basic filtering	Advanced filtering
Social media Has a single option to block or unblock social media.	**Social media controls** Has multiple options for social media control e.g. by age group, by type of access as well as read-only mode.
Deployment May only provide cloud deployment which is insufficient for on-premise IT environments.	**Deployment** Will have different deployment options including cloud, hybrid and on-premise. Schools can choose according to their needs.

Illustrative case scenarios

What does this mean in practice? The following scenarios show what basic versus advanced filtering means in an everyday context.

Basic filtering

Example 1
A student accesses a far-right extremist page advertising an event. This is a new page and isn't currently on the blocklist.

Example 2
A Media Studies A-Level lesson using animation can't run because of lack of bandwidth. The whole school system slows down.

Example 3
A student circumvents the filter through VPN and accesses social media. They make a "bait out" page with a doctored image of a female pupil in the school who is subsequently bullied.

Example 4
A teacher opens a phishing email and exposes the whole school network. Hackers retrieve personal information of the child of a celebrity parent.

Advanced filtering

Example 1
A student is blocked from accessing a far-right extremist page as the real-time content analysis sees it includes extremist content.

Example 2
A student tries to circumvent the filter using VPN but is unable to. They access social media but are unable to create a page or write anything negative. A cyberbullying incident is avoided.

Example 3
Bandwidth is allocated to the A-Level Media Studies lesson allowing them to see animation smoothly without impacting on other classes.

Example 4
A phishing email is identified and blocked. The school network remains safe and no information is gained.

2.2 Digital monitoring

Monitoring is essential for identifying students at risk of online harm and is part of statutory safeguarding guidance.

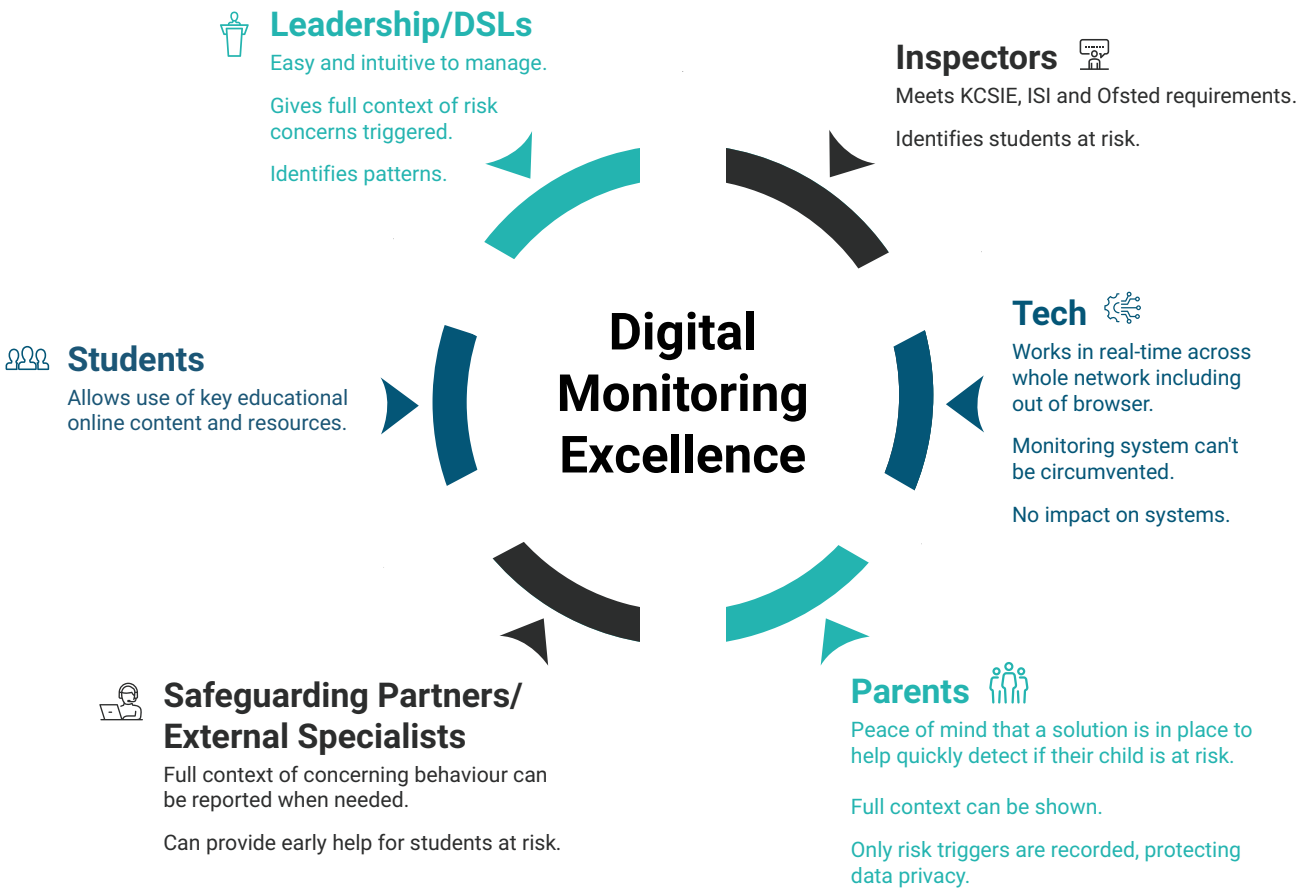
By identifying issues at an early stage, schools can tackle a concern before it escalates into a more significant problem.

The types of issues digital monitoring can help safeguard against include: bullying, mental health issues, substance abuse, exploitation and abuse, self-harm, radicalisation and others.

It can also help reduce the number of students who do not reach their maximum potential or even have to exit the school altogether.

Digital monitoring solutions commonly fall into two categories: self-service and managed-service. A self-service solution requires daily attention from the DSL whereas a managed-service solution has a safety expert assessing risk on their behalf.

A good digital monitoring solution benefits the whole school community, as shown below.



Basic vs. advanced digital monitoring

Basic monitoring	Advanced monitoring
School management Requires manually review of usage logs. This is time consuming and risks missed incidents.	**Third party management** Safety specialists check all logs and alert DSLs to high risks by phone and email.
Delayed function May not report alerts in real-time, putting the student and school at risk if an urgent concern is triggered.	**Real-time** Often works in real-time and reports on urgent concerns immediately.
No pre-grading Does not provide pre-grading. It's difficult to know which alerts need immediate attention. Often results in false positives.	**Pre-grading** Filters out false positives. Pre-graded risk alerts include immediate notification of high risks.
Basic reporting Provide limited contextual evidence of incidents making follow up difficult.	**Full context reporting** Shows the full context of a capture including a screenshot. Makes intervention and follow up actions more effective.
Circumvention Can be circumvented via a VPN and anonymous proxy server, leaving students unprotected.	**Circumvention** Identifies all risk activity and cannot be circumvented via VPNs or proxy servers.
In browser Often only monitors inside browsers and precludes web-chat, private chat windows, Word or other documents.	**Switch on to switch off** Captures any concern that takes place on a computer from log-on to log-off, including files opened from a USB, text chat or chatting in a private chat window.

Illustrative case scenarios

The following scenarios show what basic versus advanced monitoring means in practice.

Basic digital monitoring

Example 1
A student types in an offline Word document about going for a 'joint' after lessons to another student. The student agrees and deletes the words. This occurs offline and monitoring fails to see it.

Example 2
A student looks for a good place to have a hair cut. The monitoring system triggers an alert as it can't differentiate between a haircut and a violent action. Precious DSL time is wasted.

Example 3
While in their boarding house, a student sends a threat of violence to another student on social media. The digital monitoring software doesn't cover encrypted sites and doesn't pick it up.

Example 4
A student searches on the internet for ways to be violent towards teachers. Later that day they attack a teacher. The monitoring system doesn't work in real-time and the DSL sees the alert the next day.

Advanced digital monitoring

Example 1
A student types in offline notes about going for a 'joint' after lessons to another student. The monitoring software picks it up in real-time, the DSL is alerted and meets the student at the end of lesson to discuss.

Example 2
A student looks for a good place to have a 'hair cut'. The monitoring system understands this is a safe search and no alert is created, saving the DSL time.

Example 3
While in their boarding house, a student sends a threat of violence to another student on social media. It is picked up in real-time and the DSL can implement an appropriate bullying follow-up.

Example 4
A student searches on the internet for ways to be violent towards teachers. It is picked up in real-time and the DSL can alert staff to a possible risk and follow up with the student straight away.

2.3 Digital safeguard record keeping

Ofsted and ISI look for evidence that all concerns are recorded in a timely and secure way. KCSIE refers to the importance of this too.

Having a clear chronology of a student's history is an important aspect of record keeping. It enables schools to keep safeguarding records as secure, living digital documents that can be shared with appropriate parties, as needed.

Insufficient record keeping puts students at risk and has been mentioned in serious case reviews after child deaths.

"Deficiencies in record keeping have been identified by several child death enquiries as a problem area that requires attention from all agencies".[2]

2. Oxfordshire County Council. 2016. Guidance on record keeping for educational and early years settings.

Basic vs. advanced record keeping

Basic record keeping	Advanced record keeping
Difficult to update Records are physical and difficult to update. Key information and details may be lost.	**Easy and fast to update** Software allows staff members to add concerns to records immediately. Appropriate members of staff are alerted in real-time.
Creating chronology and reports Sharing information about a student to relevant parties is essential for keeping track and tackling student issues. Physical records are often unable to show clear reports and a clear time-line of what has happened and what interventions have ensued.	**Creating chronology and reports** Information can be easily and safely shared. Evidence is saved and correct information for referrals is always available.
Tracking referrals Key concerns or referrals can easily be lost.	**Tracking referrals** Ensures concerns are tracked and makes it easy to see if concerns have been acted upon.
Insecure access to records Physically-held records can limit access to records. Online spreadsheets or other files may not be secure risking inappropriate access.	**Secure access to records** Ensures safe and secure access by the right people on any device, anywhere.
Weak group tracking Limited record keeping may mean that it is difficult to track specific areas such as 'CP Plans' and 'Child in need'.	**Strong group tracking** Allow tagging of students in particular areas such as 'CP plans' and 'child in need'.
Minimal information gathering May lack detail in records from other systems such as online incidents that have taken place and body maps may not be able to link without manual interpretation.	**Appropriate information gathering** Allows a full student picture. Body maps can be combined to look for emerging patterns of self-harm or bullying.

Illustrative case scenarios

The following scenarios show what basic versus advanced record keeping means in practice.

Basic record keeping

Example 1
A teacher is concerned about a student but does not have time to see a DSL. They are urgently called away and forget to report the incident. The student concerned takes an overdose later that week.

Example 2
A DSL sees a concern raised about another student taking drugs but is busy at the time. With many concerns raised on a daily basis, the concern is not followed up. The student ends up in hospital after taking a class A drug.

Example 3
A student is referred to an outside agency for possible child abuse. The school have not recorded enough information for a threshold to be reached for a child to be referred even though enough has occurred. The child remains unnecessarily at risk for longer.

Example 4
Online monitoring has found a student interacting with a known drug dealer on social media. The information is not fed into their child protection record even though it is a vital part of the student's time-line of being at risk of drug issues.

Advanced record keeping

Example 1
A teacher is concerned about a student and can record a concern immediately securely online. Even though they are urgently called away, they have been able to raise the alarm and the concern can be followed up.

Example 2
A DSL sees a concern raised about another student taking drugs. They are very busy at the time but set a review schedule prompt to ensure they follow it up.

Example 3
A student is referred to an outside agency for possible child abuse. The secure system enables the school to print a clear report detailing every aspect of a concern of child abuse. Enough information is provided to reach the threshold for a referral.

Example 4
Online monitoring has found a student interacting with a local drug dealer on social media. The information is automatically linked to the pupil's record keeping file which can then be shown on their full chronology.

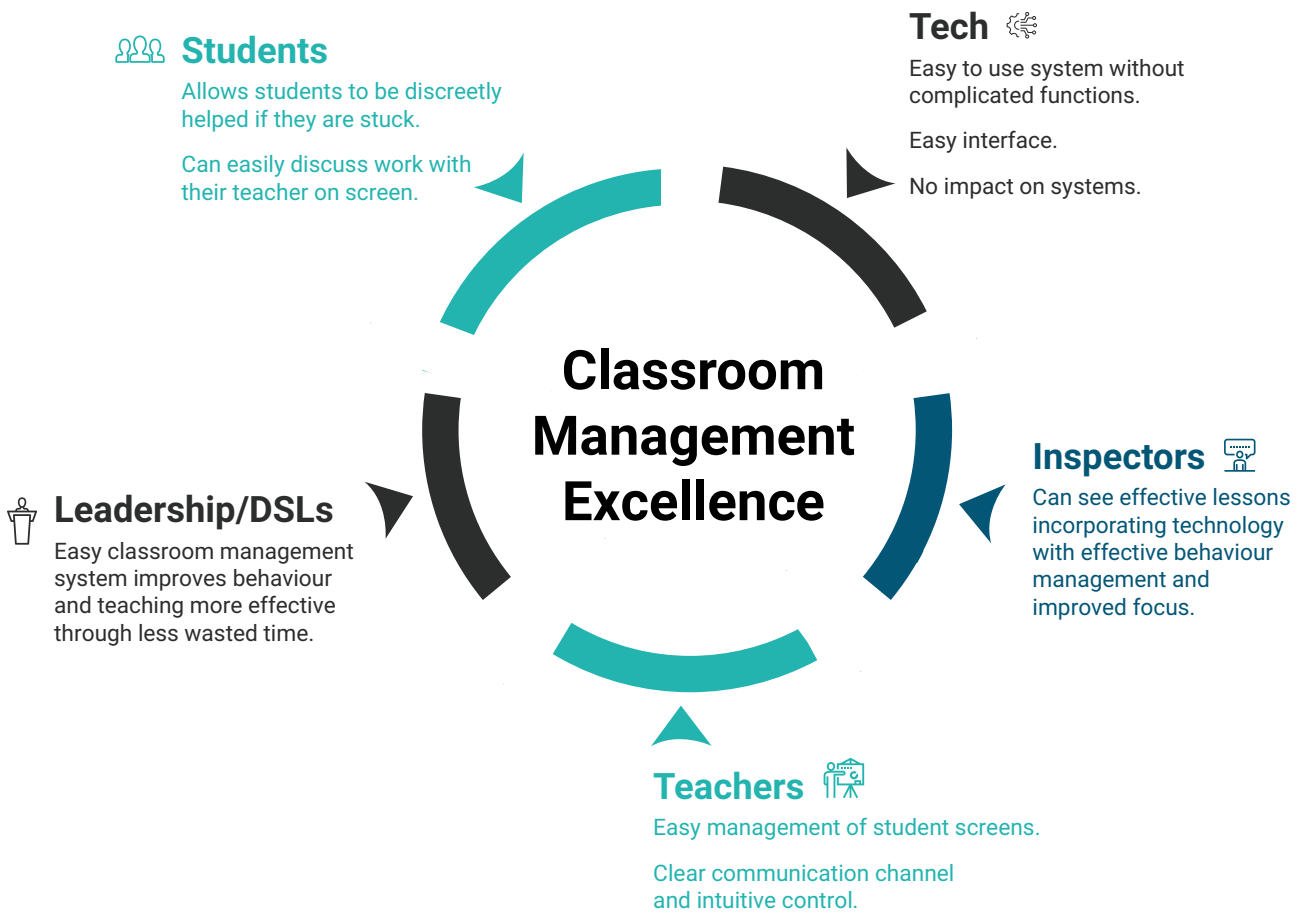
2.4 Classroom management

No matter how focussed and motivated, a classroom of students all simultaneously working on computers can be a challenge for even the most competent of teachers. Making sure that every individual is on task and concentrating can be difficult.

An effective classroom management system enables teachers to maintain a dynamic, focussed, and productive learning environment at all times.

They can instantly disable screen access, as a group or individually; they can see if anyone has jumped off task, and can quickly see and address any misbehaviours, without disrupting anyone else.

Classroom management systems are only effective when they are intuitive. Teachers prefer systems that are easy to use and do not, in any way, detract from the role of teaching.



Basic vs advanced classroom management

Basic classroom management	Advanced classroom management
Complicated operation Can be complicated to set up and use.	**Easy operation** Is intuitive and easy to use. Lessons run smoothly without becoming stuck in operational issues. A simple grid shows all students' screens at once.
General screen view May only give an overview of screens with no ability to drill down to individual screens.	**Individual screen view** Teachers can drill down to a single screen and intervene when needed.
Limitation of device control Limited ability to control students' devices.	**Device control** Staff can easily control student devices. This could be whole class or individual. For instance, if a teacher wants to lock all screens to regain attention or if an individual student needs limited internet use during an exam, the teacher has full control.
Bandwidth limitation Some solutions may impact on bandwidth. For instance chromebooks can be limited by RAM space.	**Bandwidth limitation** Uses peer to peer architecture which enables low impact on bandwidth.
All focus limitation Some solutions are not able to load a specific URL on all devices at once. This can hold up classes while all pupils find the URL.	**Full session control** Teachers can easily set session times or add and remove students without needing to involve IT. Teachers can also open up a url on all devices, saving valuable teaching time.
Limited monitoring Monitoring may not occur in real-time and so a teacher could miss a student being off-track.	**Real-time monitoring and evidencing** Allows staff to monitor in real-time and take screenshots of activity when needed.

Illustrative case scenarios

The following scenarios show what basic versus advanced classroom management means in practice.

Basic level classroom management

Example 1
The start of the lesson is held up while a teacher works out how to launch a URL to all students.

Example 2
The teacher takes a screenshot of a student on a games site but forgets to save it.

Example 3
A pupil becomes stuck and off-task because the teacher can't see an overview of all screens in real-time and can't scan the whole class easily.

Example 4
The teacher can't see the content on every students' screen because the classroom manager software is complicated to navigate around.

Advanced classroom management

Example 1
A teacher spots a student off-task in their full grid view and quickly puts the student back on task by closing the irrelevant window.

Example 2
A student goes to a TV programme website. The teacher takes an evidence screenshot and passes the information on to the student's pastoral tutor.

Example 3
A teacher sets a time limit on a session so that there is no hold up for the class plenary.

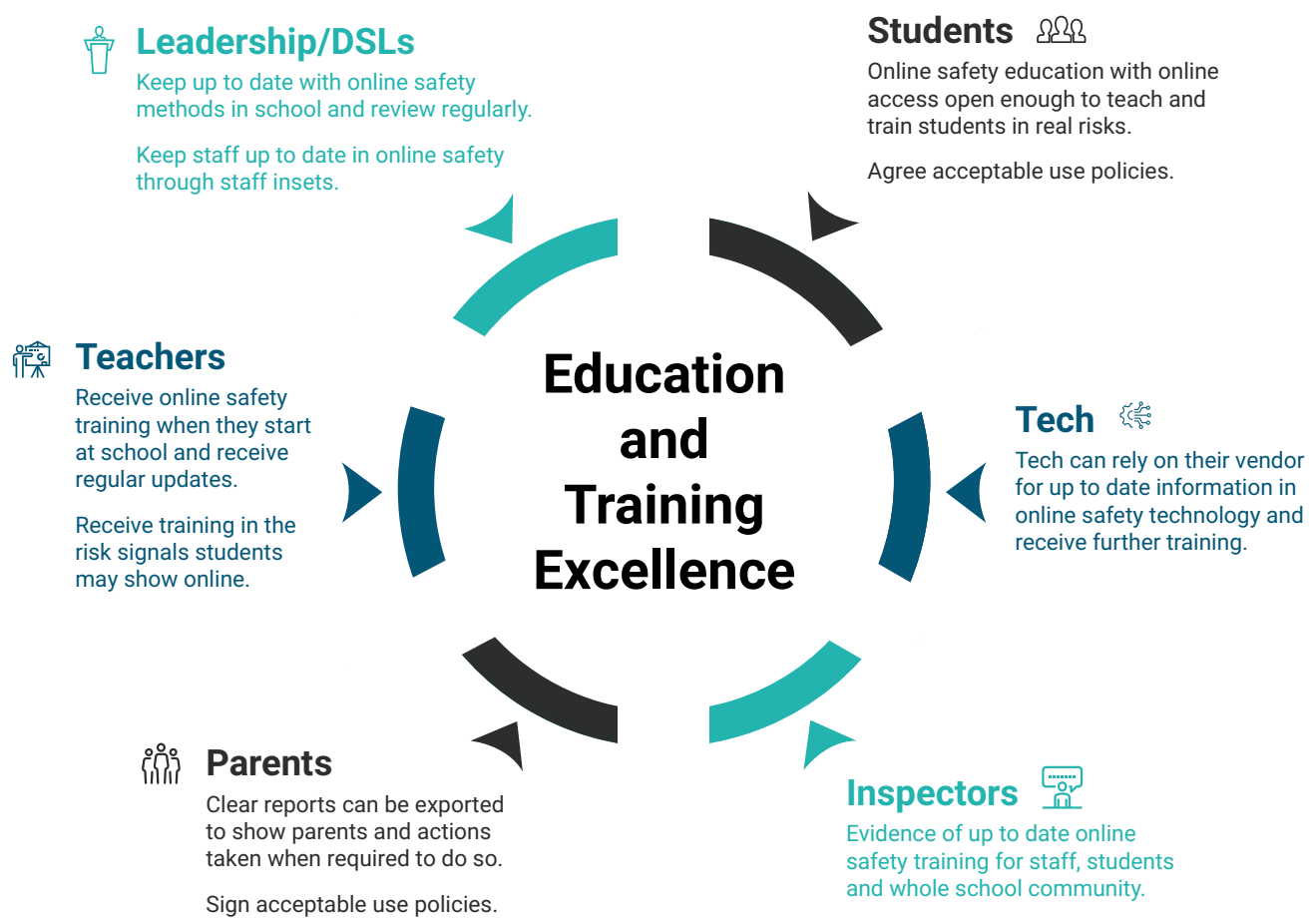
Example 4
A teacher has assigned their classes on Google Classroom. As the classroom management software integrates, they are able to use the resources without rebuilding the lessons.

2.5 Education and training

Roles and responsibilities

Education and awareness of online dangers is a crucial component in keeping children safe online. A DSL is expected to ensure every member of staff is appropriately trained from the moment they arrive at the school.

Education starts with children themselves but it extends to the whole school community, including governors, headteachers, teachers, house heads, staff and parents. When everyone understands and follows safe practices, safety online becomes the norm, not the exception.



3.0 Revising Your School's Online Safety Infrastructure

Steps to improvement

It is vital to regularly review your online safety infrastructure.

Use the template below to make notes for each component. Write any limitations you have and the improvements you want to make. Use the basic/ advanced tables from section 2 to help you.

Think about how your current software is working in school and any issues any staff have mentioned in its operation that you could look to resolve.

If you would like help in reviewing your current system and planning change, Smoothwall can provide online safety experts to help you. We offer a wide range of options in online safety components and can provide a complete online safety infrastructure to create a level of excellence in protection within your school.

Online safety infrastructure school review

Current solution	Where does it fall short?	Improvements needed
Filtering:		
Digital monitoring:		

Current solution	Where does it fall short?	Improvements needed
Record keeping:		
Classroom management:		
Education:		

Appendices

Book a demo

Smoothwall is the UK's leading authority on safeguarding technology for education.

Our expertise and pioneering solutions make us the ideal choice for independent schools requiring a credible and an education focussed safeguard provider.

If you have a question about any aspect of online safety in your school please contact us. We'd love to help.

We can arrange online demonstration for any solution at a day and time convenient to you or meet in person.

Contact us on:

Tel: +44 (0)870 1999 500
Email: enquiries@smoothwall.com

smoothwall.com

smoothwall®

Further reading

Safeguard Monitoring: A Complete Guide to Active Monitoring for Schools

What is monitoring, why do Ofsted require it, and how can you integrate it into a busy safeguarding strategy.

Available at: https://smoothwall.com/active-monitoring-schools

Safeguard Monitoring: How to Prepare Your Case for Funding

A step by step guide for DSLs, Head Teachers, Principals and anyone responsible for ensuring a compliant digital monitoring provision within their School.

Available at: https://smoothwall.com/how-to-create-a-case-for-funding

More papers and articles

To see more papers and articles on digital safeguarding in independent schools, please visit https://smoothwall.com/education/about-you/independent-digital-safety-leaders/

About Smoothwall

Smoothwall is the leading digital safeguarding solutions provider in UK Education. 10,000 schools, colleges and academies depend on our filtering and monitoring technologies to keep their students safe and their education organisations compliant.

Since our humble beginnings in 2000 we have been dedicated to empowering educational organisations to digitally safeguard the young people in their care.

Our solutions are innovative and pioneering and developed from the ground up to meet and exceed the legislative requirements set out by the Department for Education, as outlined in the Prevent duty and Keeping Children Safe in Education.

Digital safeguarding solutions were historically seen as security products to be selected, deployed and managed by a school/college's ICT department. And while the ownership remains generally true, the meteoric rise in the use of the internet as a vital tool for learning has firmly placed digital safeguarding on the agenda of most educational stakeholders.

Web filters today are not tools for blocking content.

They are a means of improving learning outcomes by enabling students to freely access rich internet content, protected by granular filtering, controls and alerts to ensure any risks and safeguarding issues are quickly and accurately identified.

Schools/colleges favour Smoothwall because of our understanding of this core concept and our pioneering solutions that support it.

Where Smoothwall Filter dynamically analyses content and intelligently blocks harmful content, Smoothwall Monitor is installed onto the school/college's computers where it analyses on-screen content and any keystrokes made. Words or phrases indicating the user may be at risk of harming or being harmed are captured in a screen shot and sent to the DSL for analysis (or the Smoothwall team if it's a managed service).

Behavioural profiling by monitoring words over time provides an added level of vigilance to enable an early stage help intervention.

As digital learning becomes more commonplace in the classroom, so does safeguarding issues such as mental health, cyberbullying, radicalisation, child sexual exploitation and others.

The demands placed on the physical eyes and ears of teachers far exceed their ability to identify all but the most obvious risks, and puts the organisation at odds with both student needs and statutory guidelines.

Smoothwall's robust filtering, firewall, monitoring, classroom management and record keeping provision work in tandem to keep young people safe and your organisation compliant with the legislation, guidelines and recommendations placed upon it.

Our Partners

IWF

Smoothwall are members of the Internet Watch Foundation (IWF) and implement the Child Abuse Image Content list of domains and URLs.

Home Office

Smoothwall also implements the police assessed list of unlawful terrorist content, produced on behalf of the Home Office.

UK Safer Internet Centre

Smoothwall submits details of how our solutions comply with UK legislation. These documents can be accessed on the UK Safer Internet Centre website.

EduGeek

We partner with EduGeek and actively promote the communication platform and information sharing they provide to IT leaders across UK Education.

National Online Safety

Smoothwall exclusively partners with National Online Safety to offer customers their award-winning e-safety training for the whole school community.

Smoothwall

Avalon House
1 Savannah Way
Leeds
West Yorkshire
LS10 1AB

Tel: 44(0) 870 1999 500
Email: enquiries@smoothwall.com

smoothwall.com

Smoothwall
Smoothwall
Smoothwall-ltd
SmoothwallTV

smoothwall®