Online Safety Policy

ABSTRACT
How we, as an organisation, ensure the safety and wellbeing of pupils and staff with regards to online use and devices

APPOVED	Headteacher
POLICY DATE	Autumn 2022
REVIEW	Autumn 2024

Online Safety Policy

Information and Communications Technology (ICT) covers a wide range of resources including web-based and mobile learning. It is also important to recognise the constant and fast-paced evolution of ICT within our society as a whole. Currently the internet technologies children and young people are using both inside and outside of the classroom include:

- Websites
- Learning Platforms –Google classroom
- Email and Instant Messaging
- Chat Rooms and Social Networking
- Blogs
- Podcasting
- Video Broadcasting
- Downloading from the internet
- Gaming
- Mobile/Smart phones with text, video and/or web functionality
- Other mobile devices with web functionality

Aims and objectives:

- To ensure the safety and wellbeing of children and young people when adults, young people or children are using the internet, social media or mobile devices
- To provide staff and volunteers with the overarching principles that guide our approach to online safety
- To ensure that, as an organisation, we operate in line with our values and within the law in terms of how we use online devices.

We believe that:

- Children and young people should never experience abuse of any kind
- Children should be able to use the internet for education and personal development, but safeguards need to be in place to ensure they are kept safe at all times.

We recognise that:

- The online world provides everyone with many opportunities; however, it can also present risks and challenges
- We have a duty to ensure that all children, young people and adults involved in our organisation are protected from potential harm online
- We have a responsibility to help keep children and young people safe online, whether or not they are using [name of organisation]'s network and devices
- All children, regardless of age, disability, gender reassignment, race, religion or belief, sex or sexual orientation, have the right to equal protection from all types of harm or abuse
- Working in partnership with children, young people, their parents, carers and other agencies is essential in promoting young people's welfare and in helping young people to be responsible in their approach to online safety.

We will seek to keep children and young people safe by:

- appointing Computing Lead - tbc
- providing clear and specific directions to staff and volunteers on how to behave online through our behaviour code for adults
- supporting and encouraging the young people using our service to use the internet, social media and mobile phones in a way that keeps them safe and shows respect for others
- supporting and encouraging parents and carers to do what they can to keep their children safe online. To support this, parents will be given an information sheet giving tips on how to keep their child safe. This will be available in a number of languages.
- developing an online safety agreement for use with young people and their parents/carers
- developing clear and robust procedures to enable us to respond appropriately to any incidents of inappropriate online behaviour, whether by an adult or a child/young person
- reviewing and updating the security of our information systems regularly
- ensuring that user names, logins, email accounts and passwords are used effectively
- ensuring personal information about the adults and children who are involved in our organisation is held securely and shared only as appropriate
- ensuring that images of children, young people and families are used only after their written permission has been obtained, and only for the purpose for which consent has been given
- providing supervision, support and training for staff and volunteers about online safety
- examining and risk assessing any social media platforms and new technologies before they are used within the organisation.

If online abuse occurs, we will respond to it by:

- having clear and robust safeguarding procedures in place for responding to abuse (including online abuse)
- providing support and training for all staff and volunteers on dealing with all forms of abuse, including bullying/cyberbullying, emotional abuse, sexting, sexual abuse and sexual exploitation
- making sure our response takes the needs of the person experiencing abuse, any bystanders and our organisation as a whole into account
- reviewing the plan developed to address online abuse at regular intervals, in order to ensure that any problems have been resolved in the long term.

Online safety (taken from KCSiE 2023)

- It is essential that children be 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 pupils, students, and staff in their use of technology and establishes mechanisms to identify, intervene in, and escalate any concerns where appropriate.
- The breadth of issues classified within online safety is considerable and ever evolving, but can be categorised into four areas of risk:
  Content: being exposed to illegal, inappropriate, or harmful content, for example: pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation, and extremism.

Contact: being subjected to harmful online interaction with other users; for example: peer to peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other persons
Conduct: online behaviour that increases the likelihood of, or causes, harm; for example, making, sending and receiving explicit images (e.g. consensual and nonconsensual sharing of nudes and semi-nudes and/or pornography, sharing other explicit images and online bullying, and
Commerce: risks such as online gambling, inappropriate advertising, phishing and or financial scams. If you feel your pupils, students or staff are at risk, please report it to the Anti-Phishing Working Group (https://apwg.org/).

Guidelines

1. **Pupils' online access**

Owing to the international scale and linked nature of information available via the Internet, it is not possible to guarantee that unsuitable material will never appear. **Supervision is the key strategy.** Whatever systems are in place, something could go wrong which places pupils in an embarrassing or potentially dangerous situation. Children and staff should immediately report any inappropriate images or see below 'Reporting Incidents'.

Responsible usage of the Internet for all pupils should be taught routinely through Computing. It is good practice to teach pupils to use the Internet in response to an articulated need – e.g. a question arising from work in class. Children should be able to answer the question "What is the purpose?"

Children will be taught use search technologies effectively, appreciate how results are selected and ranked, and be discerning in evaluating digital content.

Sharing websites via J2e and Google are a useful way to present this choice to pupils.

2. **Filters**

Grange Primary School has the educational filtered secure broadband connectivity through the LGfL and so connects to the 'private' National Education Network. We use the LGfL filtering system which blocks sites that fall into categories such as pornography, race hatred, gaming, sites of an illegal nature, and prevents access to extremist websites and materials etc. All changes to the filtering policy are logged and only available to staff with the approved 'web filtering management' status. We use user-level filtering where relevant, thereby closing down or opening up options appropriate to the age / stage of the students. Our SBT (school based technician) ensures the network is healthy through use of anti-virus software (from LGfL) etc. and the network is set up so staff and pupils cannot download executable files. All chat rooms and social networking sites are blocked except those that are part of an educational network or approved Learning Platform. Any sites which the school wants unblocking needs authorising through the head teacher, and a written request needs to be raised on the Adept Support website which will be processed by a member of the RM Remote Support team.

3. **Monitoring**

- The appropriateness of any filtering and monitoring systems are a matter for individual schools and colleges and will be informed in part, by the risk assessment required by the Prevent Duty.39
- To support schools and colleges to meet this duty, the Department for Education has published filtering and monitoring standards which set out that schools and colleges should:
  • identify and assign roles and responsibilities to manage filtering and monitoring systems.
  • review filtering and monitoring provision at least annually.
  • block harmful and inappropriate content without unreasonably impacting teaching and learning.
  • have effective monitoring strategies in place that meet their safeguarding needs

Governing bodies and proprietors should review the standards and discuss with IT staff and service providers what more needs to be done to support schools and colleges in meeting this standard.

4. **Online Safety**

All teachers are responsible for promoting and supporting safe behaviour in their classroom and following school Online Safety procedures. Central to this is fostering a 'No Blame' culture where pupils feel able to report any bullying, abuse or inappropriate materials. Children will receive Online-Safety education once an academic year, **and will be reminded at the start of each lesson** to teach them the importance of being safe online and highlighting the potential dangers that they can be exposed to.

Online safety is taught in every year group.

Social Networking Sites - These are a popular aspect online for young people. Sites such as: Facebook, Instagram, Snapchat, WhatsApp, YouTube and Ticktock allow users to share information and communicate with each other. It is important for children to understand that most social networking sites carry an age restriction of 13 and that this space is used by the vast majority of the population; these are environments that should be used with caution.

Prevent Duty

As a school we aim to ensure that children are safe from terrorist and extremist material when accessing online at school. As outlined above, suitable filtering is in place to protect pupils. All teachers are aware of the risks posed by the online activity of extremist and terrorist groups, and by communication with parents and sharing guidance on safe internet access at home and supervision by an adult, we aim to ensure that pupils are protected from the threat of radicalisation. In the case of any member of staff or pupil attempting to access inappropriate material online, the school would make a referral to the Channel programme in accordance with government and Local Authority guidelines, See the school's Prevent Duty Document.

Pupils:

We use J2e and Google with the pupils and lock this down where appropriate using LGfL filtering. Pupils' USO and Google accounts are not visible to others and handed out to that person only. Pupils are introduced to the cloud and working collaboratively on a document and communicating online as part of the Computing scheme of work. Pupils are taught about the

safety of communicating online both in school and at home i.e. they are taught:

- not to give out their username and password unless it is part of a school managed project or to someone they know and trust and is approved by their teacher or parent/carer;
- they must not reveal private details of themselves or others in an online, such as an address, telephone number, etc.;
- to 'Stop and Think Before They Click' and not to open a link unless they are sure the source is safe;
- that they should think carefully before uploading any attachments as this will remain online forever;
- that they must immediately tell a teacher / responsible adult if they receive a document online which makes them feel uncomfortable, is offensive or of a bullying nature;
- not to respond to malicious or threatening messages.
  Additional in relation to SMART
  Not to meet 'friends' or strangers encountered online
  Ensure reliability of information by checking additional sources

5. **Use of email**

We do not publish personal e-mail addresses of pupils or staff on the school website. We use anonymous or group e-mail addresses, for example info@grange for communication with the wider public. The school will contact the police if one of our staff or pupils receives an e-mail that we consider is particularly disturbing or breaks the law. The school manages accounts effectively with up to date account details of users. We are aware that spam, phishing and virus attachments can make emails dangerous. We use a number of LGfL-provided technologies to help protect users and systems in the school, including desktop anti-virus product, plus direct email filtering for viruses, Trojans, pornography, phishing and inappropriate language. Finally, LGfL WebScreen2 filtering monitors and protects our internet access to the World Wide Web.

6. **Web publishing**

The school has its own website, and the school is registered with the ICO under the Data Protection Act. Parental consent is gained upon admission to the school. This is required before any text, audio, pictorial or photographic reference to a child or children being published. Records are kept of parents or carers who decline permission. Individual pupils will not be identifiable by name, and names will not be linked to any photographs. Personal information will never be published without prior consent.

7. **Reporting incidents**

If one or more pupils discover (view) inappropriate material, the first priority is to provide them with support. Children should report any unsuitable sites to the class teacher. The class teacher is then responsible to report the inappropriate material to the Safeguarding Lead. From there the Computing coordinator should inform the head teacher.to the upgraded LGFL filters there are a lot more restrictions placed upon the internet.

Incidents which occur due to non-compliance with the school Online Safety policy and issues relating to staff misuse must be referred to the head teacher. Any incidents which refer to

children protection must be reported to the Designated Safeguarding Lead.

8. **Parents and the community**

   Pupils' online access at home is increasing rapidly, encouraged by low cost access and developments in mobile technology. Unless parents are aware of the dangers, pupils may have unrestricted and unsupervised access to the Internet in the home. The school may be able to help parents plan appropriate, supervised use of the Internet at home and educate them about the risks. Parents should also be advised to check whether their child's use elsewhere in the community is covered by an appropriate use policy. Parents' attention will be drawn to the school Online Safety Policy in newsletters, the school prospectus and on the school website.

9. **Safeguarding**

   Staff must refrain from giving their personal contact details to parents/carers or pupils, including connecting through social media and messaging apps.

   Staff must avoid publicising their contact details on any social media platform or website, to avoid unwanted contact by parents/carers or pupils.

   Staff must not use their mobile phones to take photographs or recordings of pupils, their work, or anything else which could identify a pupil. If it's necessary to take photos or recordings as part of a lesson/school trip/activity, this must be done using school equipment.

10. **Roles and responsibilities**

    Online Safety is recognised as an essential aspect of strategic leadership in this school and the Head, with the support of Governors, aims to embed safe practices into the culture of the school. The Headteacher ensures that the policy is implemented and compliance with the policy monitored. The responsibility for Online Safety has been designated to a member of the senior management team.

    Our school Online Safety Coordinator is Ms. Charles.

    Our Online Safety Coordinator ensures that they are up to date with Online Safety issues and guidance through the Local Authority Online Safety Officer and through organizations such as Becta, LGFL, NSPCC and CEOP. The school's Online Safety Coordinator ensures the Head, senior management and the Governors are updated as necessary.

Strategic and operational practices

At this school:

- The Head Teacher is the Senior Information Risk Officer (SIRO).
- The Education Space are our appointed Data Protection Officer (DPO), with responsibility for data protection compliance.
- We have listed the information and information asset owners in our Information Asset Register.

- We ensure staff know to immediately report, and who to report to, any incidents where data protection may have been compromised, such as when passwords for sensitive systems or devices are lost or stolen, so that relevant action(s) can be taken.
- All staff are DBS checked and records are held in one central record.

  We ensure ALL staff are sent an Acceptable Use Agreement * (updated September 2022) and keep a register of signatures to confirm that this has been received and read.

  This makes clear all responsibilities and expectations with regard to data security.
- We have approved educational web filtering across our wired and wireless networks. We monitor school e-mails / online platforms, etc. to ensure compliance with the Acceptable Use Agreement. As well as monitoring usage, we may also monitor content of e-mails.
- We follow LA guidelines for the transfer of any data, such as MIS data or reports of children, to professionals working in the Local Authority or their partners in Children's Services / Family Services, Health, Welfare and Social Services.
- All staff have their own unique username and private passwords to access school systems. Staff are responsible for keeping their passwords private.
- Relevant Admin / SLT staff access confidential school information via the MyUSO portal which uses 2 factor authentication.
- School staff who set up usernames and passwords for e-mail, network access, or other online services work within the approved system and follow the security processes required by those systems.
- We ask staff to undertake house-keeping checks at least annually to review, remove and destroy any digital materials and documents which need no longer be stored.
- Any new technologies which require the sharing of personal data first are subject to a DPIA (Data Processing Impact Assessment) by our Data Protection Officer to assess the level of risk. Any companies, apps or websites that we use have fully transparent Data Protection Policies. We keep the sharing of personal data to a minimum outside of what is required by the DfE, Newham etc. This is outlined in our Privacy Notice and Data Policy.

Technical or manual solutions

- Staff have secure area(s) on the network to store sensitive documents or photographs.
- We require staff to log out of systems when leaving their computer, but also enforce lock-out after 10 mins. idle time.
- We use the DfE S2S site to securely transfer CTF pupil data files to DfE / other schools.
- We use the Pan-London Admissions system to transfer admissions data. Staff with access to the Admissions system also use a LGfL OTP tag as an extra precaution.
- We use LGfL Auto Update for creation of online user accounts for access to services and online resources.
- We use LGfL's USO-FX2 to transfer documents to schools in London, such as references, reports of children.

- We store any sensitive/special category written material in lockable storage cabinets in a locked room
- All servers are in lockable locations and managed by DBS-checked staff.
- We use LGfL's Grid Store remote secure back-up for disaster recovery on our network / admin, curriculum server(s).
- For ICT disposal, we delete all data from hard drives and memory and dispose of the equipment via Newham Council
- Portable equipment loaned by the school for use by staff at home, where used for any protected data, is disposed of through the same procedure.
- Paper based sensitive information is shredded.
- Visitor log on have restricted access to curriculum drives.

Users, both pupils and staff, need to know how to keep their personal information private and set-up and use these environments safely. As part of the LGFL filtering these sites are blocked within school, however as a duty of care to both students and adults it is our responsibility to educate about the potential dangers.

Information and support:
There is a wealth of information available to support schools and parents to keep children safe online. The following list is not exhaustive but should provide a useful starting point:

Organisation/Resource	What it does/provides
Think u Know	NCA CEOPs advice on online safety
Disrespect Nobody	Home Office advice on healthy relationships, including sexting ar pornography
Parent Zone	Help for parents on how to keep their children safe online
Childnet.cyberbullying	Guidance for schools on cyberbullying
Educate Against Hate	Practical advice for parents, teachers and governors on protectir children from extremism and radicalisation.
UKCIS	The UK Council for Internet Safety's website provides: • Sexting advice • Online safety: Questions for Governing Bodies • Education for a connected world framework
NSPCC	NSPCC advice for schools and colleges
NSPCC	NSPCC advice for parents
Common sense Media	Independent reviews, age ratings, & other information about all types of media for children and their parents
Searching, Screening and Confiscatio	Guidance to schools on searching children in schools and confiscating items such as mobile phones
LGFL	Advice and resources from the London Grid for Learning

Related policies and procedures
This policy statement should be read alongside our organisational policies and procedures, including:

- Safeguarding, Early Help & Child Protection policy
- Behaviour Policy
- Whistleblowing Policy
- Staff Handbook
- Data Policy
- Acceptable Use Agreement

    - I may have identified an aspect of the AUG that should be discussed to enable clarification.

The attached Monitoring and Filtering Appendix forms part of the Safeguarding Policy

Appendix A

Filtering and monitoring standards for schools and colleges

Find out what standards your school or college should meet on filtering and Monitoring.

You should identify and assign roles and responsibilities to manage your filtering and monitoring systems

The Importance of Meeting the Standard

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

Clear roles, responsibilities and strategies are vital for delivering and maintaining effective filtering and monitoring systems. It's important that the right people are working together and using their professional expertise to make informed decisions.

How to meet the Standard?

Governing bodies and proprietors have overall strategic responsibility for filtering and monitoring and need assurance that the standards are being met.

To do this, they should identify and assign:

- a member of the senior leadership team and a governor, to be responsible for ensuring these standards are met
- the roles and responsibilities of staff and third parties, for example, external service providers

We are aware that there may not be full-time staff for each of these roles and responsibility may lie as part of a wider role within the school, college, or trust. However, it must be clear who is responsible and it must be possible to make prompt changes to your provision.

Technical Requirements to Meet the Standard

The senior leadership team are responsible for:

- procuring filtering and monitoring systems
- documenting decisions on what is blocked or allowed and why
- reviewing the effectiveness of your provision
- overseeing reports

They are also responsible for making sure that all staff:

- understand their role
- are appropriately trained
- follow policies, processes and procedures
- act on reports and concerns

Senior leaders should work closely with governors or proprietors, the designated safeguarding lead (DSL) and IT service providers in all aspects of filtering and monitoring. Your IT service provider may be a staff technician or an external service provider.

Day to day management of filtering and monitoring systems requires the specialist knowledge of both safeguarding and IT staff to be effective. The DSL should work closely together with IT service providers to meet the needs of your setting. You may need to ask filtering or monitoring providers for system specific training and support.

The DSL should take lead responsibility for safeguarding and online safety, which could include overseeing and acting on:

- filtering and monitoring reports
- safeguarding concerns
- checks to filtering and monitoring systems

The IT service provider should have technical responsibility for:

- maintaining filtering and monitoring systems
- providing filtering and monitoring reports
- completing actions following concerns or checks to systems

The IT service provider should work with the senior leadership team and DSL to:

- procure systems
- identify risk
- carry out reviews
- carry out checks

When to Meet the Standard

You should already be meeting this standard.

You should review your filtering and monitoring provision at least annually

The importance of meeting the standard

For filtering and monitoring to be effective it should meet the needs of your pupils and staff, and 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 annually.

Additional checks to filtering and monitoring need to be informed by the review process so that governing bodies and proprietors have assurance that systems are working effectively and meeting safeguarding obligations.

How to Meet the Standard?

Governing bodies and proprietors have overall strategic responsibility for meeting this standard. They should make sure that filtering and monitoring provision is reviewed, which can be part of a wider online safety review, at least annually.

The review should be conducted by members of the senior leadership team, the designated safeguarding lead (DSL), and the IT service provider and involve the responsible governor. The results of the online safety review should be recorded for reference and made available to those entitled to inspect that information.

Your IT service provider may be a staff technician or an external service provider.

Technical requirements to meet the standard

A review of filtering and monitoring should be carried out to identify your current provision, any gaps, and the specific needs of your pupils and staff.

You need to understand:

- the risk profile of your pupils, including their age range, pupils with special educational needs and disability (SEND), pupils with English as an additional language (EAL)
- what your filtering system currently blocks or allows and why
- any outside safeguarding influences, such as county lines
- any relevant safeguarding reports
- the digital resilience of your pupils

- teaching requirements, for example, your RHSE and PSHE curriculum
- the specific use of your chosen technologies, including Bring Your Own Device (BYOD)
- what related safeguarding or technology policies you have in place
- what checks are currently taking place and how resulting actions are handled

To make your filtering and monitoring provision effective, your review should inform:

- related safeguarding or technology policies and procedures
- roles and responsibilities
- training of staff
- curriculum and learning opportunities
- procurement decisions
- how often and what is checked
- monitoring strategies

The review should be done as a minimum annually, or when:

- a safeguarding risk is identified
- there is a change in working practice, like remote access or BYOD
- new technology is introduced

There are templates and advice in the reviewing online safety section of Keeping children safe in education.

Checks to your filtering provision need to be completed and recorded as part of your filtering and monitoring review process. How often the checks take place should be based on your context, the risks highlighted in your filtering and monitoring review, and any other risk assessments. Checks should be undertaken from both a safeguarding and IT perspective.

When checking filtering and monitoring systems you should make sure that the system setup has not changed or been deactivated. The checks should include a range of:

- school owned devices and services, including those used off site
- geographical areas across the site
- user groups, for example, teachers, pupils and guests

You should keep a log of your checks so they can be reviewed. You should record:

- when the checks took place
- who did the check
- what they tested or checked
- resulting actions

You should make sure that:

- all staff know how to report and record concerns
- filtering and monitoring systems work on new devices and services before releasing them to staff and pupils
- block lists are reviewed and they can be modified in line with changes to safeguarding risks

You can use South West Grid for Learning's (SWGfL) testing tool to check that your filtering system is blocking access to:

- illegal child sexual abuse material
- unlawful terrorist content
- adult content

When to Meet the Standard

You should already be meeting this standard.

Your filtering system should block harmful and inappropriate content, without unreasonably impacting teaching and learning

The Importance of Meeting the Standard

An active and well managed filtering system is an important part of providing a safe environment for pupils to learn.

No filtering system can be 100% effective. You need to understand the coverage of your filtering system, any limitations it has, and mitigate accordingly to minimise harm and meet your statutory requirements in Keeping children safe in education (KCSIE) and the Prevent duty.

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 administration
- restrict students from learning how to assess and manage risk themselves

How to Meet the Standard?

Governing bodies and proprietors need to support the senior leadership team to procure and set up systems which meet this standard and the risk profile of the school or college.

Management of filtering systems requires the specialist knowledge of both safeguarding and IT staff to be effective. You may need to ask your filtering provider for system specific training and support.

Technical Requirements to Meet the Standard

Make sure your filtering provider is: check compliance

- a member of Internet Watch Foundation (IWF)
- signed up to Counter-Terrorism Internet Referral Unit list (CTIRU)
- blocking access to illegal content including child sexual abuse material (CSAM)

If the filtering provision is procured with a broadband service, make sure it meets the needs of your school or college.

Your filtering system should be operational, up to date and applied to all:

- users, including guest accounts
- school owned devices
- devices using the school broadband connection

Your filtering system should:

- filter all internet feeds, including any backup connections
- be age and ability appropriate for the users, and be suitable for educational settings
- handle multilingual web content, images, common misspellings and abbreviations
- identify technologies and techniques that allow users to get around the filtering such as VPNs and proxy services and block them
- provide alerts when any web content has been blocked

Mobile and app content is often presented in a different way to web browser content. If your users access content in this way, you should get confirmation from your provider as to whether they can provide filtering on mobile or app technologies. A technical monitoring system should be applied to devices using mobile or app content to reduce the risk of harm.

It is important to be able to identify individuals who might be trying to access unsuitable or illegal material so they can be supported by appropriate staff, such as the senior leadership team or the designated safeguarding lead.

Your filtering systems should allow you to identify:

- device name or ID, IP address, and where possible, the individual
- the time and date of attempted access
- the search term or content being blocked

Schools and colleges will need to conduct their own data protection impact assessment (DPIA) and review the privacy notices of third party providers. A DPIA template is available from the ICO.

The DfE data protection toolkit includes guidance on privacy notices and DPIAs.

The UK Safer Internet Centre has guidance on establishing appropriate filtering.

Your senior leadership team may decide to enforce Safe Search, or a child friendly search engine or tools, to provide an additional level of protection for your users on top of the filtering service.

All staff need to be aware of reporting mechanisms for safeguarding and technical concerns. They should report if:

- they witness or suspect unsuitable material has been accessed
- they can access unsuitable material
- they are teaching topics which could create unusual activity on the filtering logs
- there is failure in the software or abuse of the system
- there are perceived unreasonable restrictions that affect teaching and learning or administrative tasks
- they notice abbreviations or misspellings that allow access to restricted material

Dependencies to the Standard

Check that you meet:

- Broadband internet standards
- Cyber security standards

When to Meet the Standard

You should already be meeting this standard.

You should have effective monitoring strategies that meet the safeguarding needs of your school or college

The Importance of Meeting the Standard

Monitoring user activity on school and college devices is an important part of providing a safe environment for children 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. For monitoring to be effective it must pick up incidents urgently, usually through alerts or observations, allowing you to take prompt action and record the outcome.

Your monitoring strategy should be informed by the filtering and monitoring review. A variety of monitoring strategies may be required to minimise safeguarding risks on internet connected devices and may include:

- physically monitoring by staff watching screens of users
- live supervision by staff on a console with device management software
- network monitoring using log files of internet traffic and web access
- individual device monitoring through software or third-party services

How to Meet the Standard?

Governing bodies and proprietors should support the senior leadership team to make sure effective device monitoring is in place which meets this standard and the risk profile of the school or college.

The designated safeguarding lead (DSL) should take lead responsibility for any safeguarding and child protection matters that are picked up through monitoring.

The management of technical monitoring systems require the specialist knowledge of both safeguarding and IT staff to be effective. Training should be provided to make sure their knowledge is current. You may need to ask your monitoring system provider for system specific training and support.

Technical Requirements to Meet the Standard

Governing bodies and proprietors should support the senior leadership team to review the effectiveness of your monitoring strategies and reporting process. Make sure that incidents are urgently picked up, acted on and outcomes are recorded. Incidents could be of a malicious, technical, or safeguarding nature. It should be clear to all staff how to deal with these incidents and who should lead on any actions.

The UK Safer Internet Centre has guidance for schools and colleges on establishing appropriate monitoring.

Device monitoring can be managed by IT staff or third party providers, who need to:

- make sure monitoring systems are working as expected
- provide reporting on pupil device activity
- receive safeguarding training including online safety
- record and report safeguarding concerns to the DSL

Make sure that:

- monitoring data is received in a format that your staff can understand
- users are identifiable to the school or college, so concerns can be traced back to an individual, including guest accounts

If mobile or app technologies are used then you should apply a technical monitoring system to the devices, as your filtering system might not pick up mobile or app content.

In the online safety section of Keeping children safe in education there is guidance on the 4 areas of risk that users may experience when online. Your monitoring provision should identify and alert you to behaviours associated with them.

Technical monitoring systems do not stop unsafe activities on a device or online. Staff should:

- provide effective supervision
- take steps to maintain awareness of how devices are being used by pupils
- report any safeguarding concerns to the DSL

School and college monitoring procedures need to be reflected in your Acceptable Use Policy and integrated into relevant online safety, safeguarding and organisational policies, such as privacy notices.

Schools and colleges that have a technical monitoring system will need to conduct their own data protection impact assessment (DPIA) and review the privacy notices of third party providers. A DPIA template is available from the ICO.

The DfE data protection toolkit includes guidance on privacy notices and DPIAs.

Dependencies to the Standard

Check that you meet:

- Cyber security standards

When to Meet the Standard

You should already be meeting this standard.

This policy is linked to the Safeguarding & CP Policy

Curriculum Policy

RSHE Policy

Behaviour Policy

Mobile Phone Policy

Acceptable Use Agreement

Reporting an online incident

Online Safety – Reporting an Online Incident Form

Date:	
Name of Person Reporting:	
When did the incident occur:	
Where did the incident occur:	
Description of the incident:	
Name of Person(s)/Organisation Reported to:	**DSL/DDSL/IT Technician**
Signed: (person reporting)	
Summary of actions taken:	**(To be completed by DSL/DDSL(s)/IT Technician)**
Signed: (person above)	
Date:	

GRANGE PRIMARY SCHOOL
Growing the seeds for lifelong learning