Filtering and Monitoring

1 Safer Use of Technology

1.1 Classroom Use

- Angram Bank Primary School uses a wide range of technology. This includes access to: Computers, laptops and other digital devices
- Internet which may include search engines and educational websites
- Learning platform/intranet
- Email (where appropriate and permitted for use as part of the curriculum)
- Games consoles and other games-based technologies
- Digital devices with cameras (iPads and laptops), web cams and video cameras

All setting owned devices will be used in accordance with our acceptable use policies and with appropriate safety and security measures in place.

Settings should list the specific measures in place e.g. for tablets, if mobile device management software will be used, how access will be recorded and how this will be enforced.

Members of staff will always evaluate websites, tools and apps fully before use in the classroom or recommending for use at home.

The setting will use age-appropriate search tools following an informed risk assessment, to identify which tool best suits the needs of our community.

Settings should list search tools suggested for staff and learners to use. Examples include SWGfL Squiggle, Dorling Kindersley find out, Google Safe Search or CBBC safe search.

Google Safe Search, Youtube Restrict:[Moderate/Strict] Mode and blocking of Youtube from Chrome browsers are implemented by policy through our device management platforms.

We will ensure that the use of internet-derived materials, by staff and learners complies with copyright law and acknowledge the source of information.

Supervision of learners will be appropriate to their age and ability.

Early Years Foundation Stage and Key Stage 1
Access to the internet will be by adult demonstration, with occasional directly supervised access to specific and approved online materials, which supports the learning outcomes planned for the learners age and ability.

Key Stage 2
Learners will use age-appropriate search engines and online tools.

Learners will be directed by the teacher to online materials and resources which support the learning outcomes planned for the learners age and ability.

1.2 Managing Internet Access

We will maintain a record of users who are granted access to our devices and systems.

All staff, learners and visitors will be provided with an acceptable use policy before being given access to our computer system, IT resources or internet.

We will carry our regular audits and review activity reports to help identify pupils/staff attempting to access sites to establish any safeguarding concerns, risks and vulnerabilities and offer advice, support and react accordingly.

1.3 Filtering and Monitoring

Filtering and Monitoring KCSIE 2023 – Paragraph 141-143

DFE digital standards updated 29 March 2023 inform this section: Meeting digital and technology standards in schools and colleges - Filtering and monitoring standards for schools and colleges - Guidance - GOV.UK (www.gov.uk)

Note: A guide for education settings about establishing 'appropriate levels' of filtering and monitoring can be found at: https://www.saferinternet.org.uk/advice-centre/teachers-and-school-staff/appropriate-filtering-and-monitoring

Angram Bank Primary School governors and leaders have ensured that our setting has age and ability appropriate filtering and monitoring in place, to limit learner's exposure to online risks.

The governors and leaders are aware of the need to prevent "over blocking" (KCSIE 2023 paragraph 134), as that may unreasonably restrict what can be taught, with regards to online activities and safeguarding.

Our decision regarding filtering and monitoring has been informed by a risk assessment, considering our specific needs and circumstances.

Changes to the filtering and monitoring approach will be risk assessed by staff with educational and technical experience and, where appropriate, with consent from the leadership team; all changes to the filtering policy are logged and recorded.

The leadership team will ensure that regular checks are made to ensure that the filtering and monitoring methods are effective and appropriate.

All members of staff are aware that they cannot rely on filtering and monitoring alone to safeguard learners; effective classroom management and regular education about safe and responsible use is essential.

1.3.1 Filtering

Education broadband connectivity is provided by Virgin.

We use Smoothwall which blocks sites which can be categorised as: pornography, racial hatred, extremism, gaming and sites of an illegal nature.

The filtering system blocks all sites on the Internet Watch Foundation (IWF) list.

We work with Ekte and Smoothwall to ensure that our filtering policy is reviewed annually. Ekte and Smoothwall reserves the right to charge a consultation or subscription fee for providing support to review filtering policies and provision of training.

If learners discover unsuitable sites, they will be required to:

Children will be taught to turn off monitor/screen and report the concern immediate to a member of staff.

The member of staff will report the concern (including the URL of the site if possible) to the DSL (or deputy) and/or technical staff.

The breach will be recorded and escalated as appropriate.

Parents/carers will be informed of filtering breaches involving their child.

Any material believed to be illegal will be reported immediately to the appropriate agencies, such as the IWF, Police or CEOP.

1.3.2 Monitoring

We will appropriately monitor internet use on all setting owned or provided internet enabled devices. This is achieved by: Smoothwall monitoring.

If a concern is identified via monitoring approaches we will:

Report to DSL or deputy.

DSL or deputy will respond in line with the child protection policy.

All users are informed that use of our systems can be monitored and that all monitoring will be in line with data protection, human rights and privacy legislation.

2 Roles and Responsibilities

The school's Designated Safeguarding Lead (DSL) has lead responsibility for online safety. Whilst activities of the designated safeguarding lead may be delegated to an appropriately trained deputy, overall the ultimate lead responsibility for safeguarding and child protection, including online safety remains with the DSL.

Angram Bank Primary School recognises that all members of the community have important roles and responsibilities to play with regards to online safety.

2.1 The leadership and management team

The leadership management team will:

- Ensure that online safety is viewed as a safeguarding issue and that practice is in line with national and local recommendations and requirements.

- Ensure there are appropriate and up-to-date policies regarding online safety; including a staff code of conduct/behaviour policy and/or acceptable use policy, which covers acceptable use of technology.
- Ensure that suitable and appropriate filtering and monitoring systems are in place and work with technical staff to monitor the safety and security of our systems and networks.
- Ensure that online safety is embedded within a progressive curriculum, which enables all learners to develop an age-appropriate understanding of online safety.
- Support the DSL and any deputies by ensuring they have sufficient time and resources to fulfil their online safety responsibilities.
- Ensure parents are directed to online safety advice and information
- Provide information on a school's website for parents and the community
- Ensure there are robust reporting channels for the community to access regarding online safety concerns, including internal, local and national support.
- Ensure that appropriate risk assessments are undertaken regarding the safe use of technology.
- Audit and evaluate online safety practice to identify strengths and areas for improvement.
- As recommended by the DFE's Meeting digital and technology standards in schools and colleges guidance - Meeting digital and technology standards in schools and colleges - Filtering and monitoring standards for schools and colleges - Guidance - GOV.UK (www.gov.uk)
    - Identify and assign roles and responsibilities to manage your filtering and monitoring systems
    - 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 someone with technical knowledge of the filtering and/or monitoring solution 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.
        - The filtering and monitoring solution provider(s) may not be provider of Onsite IT Support Services and it is important to understand roles and responsibilities of providers and those with technical knowledge of the filtering and/or monitoring solution within the school.

2.2 The Designated Safeguarding Lead (DSL)

The Designated Safeguarding Lead (DSL) will:

- Act as a named point of contact on all online safeguarding issues and liaise with other members of staff or other agencies, as appropriate.
- Work alongside deputy DSLs to ensure online safety is recognised as part of the settings safeguarding responsibilities and that a coordinated approach is implemented.
- Ensure all members of staff receive regular, up-to-date, and appropriate online safety training.
- Access regular and appropriate training and support to ensure they understand the unique risks associated with online safety and have the relevant knowledge and up to date required to keep learners safe online.
- Access regular and appropriate training and support to ensure they recognise the additional risks that learners with SEN and disabilities (SEND) face online.
- Keep up to date with current research, legislation and trends regarding online safety and communicate this with the community, as appropriate.
- Work with staff to coordinate participation in local and national events to promote positive online behaviour, such as Safer Internet Day.
- Ensure that online safety is promoted to parents, carers and the wider community, through a variety of channels and approaches.
- Maintain records of online safety concerns, as well as actions taken, as part of the settings safeguarding recording mechanisms.
- Monitor online safety incidents to identify gaps and trends, and use this data to update the education response, policies and procedures.
- Report online safety concerns, as appropriate, to the setting management team and Governing Body.
- Work with the leadership team to review and update online safety policies on a regular basis (at least annually) with stakeholder input.
- DFE's Meeting digital and technology standards in schools and colleges guidance - Meeting digital and technology standards in schools and colleges - Filtering and monitoring standards for schools and colleges - Guidance - GOV.UK (www.gov.uk)
    - The designated safeguarding lead (DSL) should take lead responsibility for any safeguarding and child protection matters that are picked up through monitoring.
    - 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.
    - The designated safeguarding lead (DSL) should take lead responsibility for any safeguarding and child protection matters that are picked up through monitoring.

2.3 Members of Staff

It is the responsibility of all members of staff to:

- Contribute to the development of online safety policies.
- Read and adhere to the online safety policy and acceptable use policies.
- Take responsibility for the security of setting systems and the data they use or have access to.
- Model good practice when using technology and maintain a professional level of conduct in their personal use of technology, both on and off site.
- Embed online safety education in curriculum delivery, wherever possible.
- Have an awareness of a range of online safety issues and how they may be experienced by the children in their care.
- Identify online safety concerns and take appropriate action by following the settings safeguarding policies and procedures.
- Know when and how to escalate online safety issues, including signposting to appropriate support, internally and externally.
- Take personal responsibility for professional development in this area.
- Identify students who are involved in cybercrime, or those who are technically gifted and talented and are at risk of becoming involved in cybercrime, and make a Cyber Choices referral.

2.4 Staff who manage the technical environment

It is the responsibility of staff managing the technical environment to:

- Implement appropriate security measures as directed by the DSL and leadership team, these include password policies and encryption; but not exclusive, to ensure that the settings IT infrastructure/system is secure and not open to misuse or malicious attack, whilst allowing learning opportunities to be maximised.
- Ensure appropriate access and technical support is given to the DSL (and/or deputy) to filtering and monitoring systems, to enable them to take appropriate safeguarding action if/when required.
- Understand the DFE's Meeting digital and technology standards in schools and colleges guidance - Meeting digital and technology standards in schools and colleges - Filtering and monitoring standards for schools and colleges - Guidance - GOV.UK (www.gov.uk) to ensure filtering system should block harmful and inappropriate content, without unreasonably impacting teaching and learning
- Ensure that our filtering policy is applied, and SSL certificates deployed to devices are updated on a regular basis; responsibility for its implementation is shared with the leadership team.
- Support the DSL or leadership team with the review of the school's filtering and monitoring provision
- Provide technical support and perspective to the DSL and leadership team, especially in the development and implementation of appropriate online safety policies and procedures

If staff managing the technical environment are outsourced the managed service provider reserves the right to charge a consultation or subscription fee for providing support to review filtering policies, development, implementation of policies and provision of training.

2.5 Learners

It is the responsibility of learners (at a level that is appropriate to their individual age and ability) to:

- Engage in age-appropriate online safety education opportunities.
- Contribute to the development of online safety policies.
- Read and adhere to the acceptable use policies.
- Respect the feelings and rights of others both on and offline.
- Take responsibility for keeping themselves and others safe online.
- Seek help from a trusted adult, if there is a concern online, and support others that may be experiencing online safety issues.

2.6 Parents and Carers

It is the responsibility of parents and carers to:

- Read the acceptable use policies and encourage their children to adhere to them.
- Support our online safety approaches by discussing online safety issues with their children and reinforcing appropriate and safe online behaviours at home.
- Role model safe and appropriate use of technology and social media.
- Abide by the home-school agreement and/or acceptable use policies.
- Identify changes in behaviour that could indicate that their child is at risk of harm online.
- Seek help and support from the setting, or other appropriate agencies, if they or their child encounter risk or concerns online.
- Use our systems, such as learning platforms, and other network resources, safely and appropriately. These include Seesaw, Times Table Rock Stars, Spelling Shed, Google Classroom and Nessy.
- Take responsibility for their own awareness in relation to the risks and opportunities posed by new and emerging technologies.

2.7 Governing Body

The Governing Body will:

- 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
- 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.

- 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.
- KCSIE 2023 paragraph 124 - Governing bodies and proprietors should ensure that all staff undergo safeguarding and child protection training (including online safety which, amongst other things, includes an understanding of the expectations, applicable roles and responsibilities in relation to filtering and monitoring – see para 141 for further information) at induction. The training should be regularly updated. Induction and training should be in line with any advice from local safeguarding partners
- 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.
- Ensure effective monitoring strategies that meet the safeguarding needs of the school.

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. DFE's Meeting digital and technology standards in schools and colleges guidance - Meeting digital and technology standards in schools and colleges - Filtering and monitoring standards for schools and colleges - Guidance - GOV.UK (www.gov.uk)

Appendix [number here]

1 Filtering Provision

The filtering service is:

Filtering service and provider	**Please tick for the procured filtering provision**
iBoss / ekte	
Netsweeper / ekte (emPSN)	
Smoothwall / Local Authority	✓
Other (please note here):	

The filtering service is accessible and onsite/remote support provided to the school by:

Managed IT Support	**Please tick for where appropriate**
Ekte	✓
Local Authority	
Other (please note here):	

Monitoring Provision

The monitoring service is:

Monitoring service and provider	Please tick for the procured filtering provision
No monitoring service procured (NA)	✓
Senso Safeguard Cloud Bundle / ekte	
Netsweeper Onguard	
Smoothwall Monitor	
Impero Safeguard	
Netsupport Classroom.Cloud	
Other (please note here):	

The monitoring service (where procured) is accessible and onsite/remote support of the solution is provided to the school by:

Managed IT Support	Please tick for where appropriate
Ekte	
Local Authority	
Other (please note here):	N/A