Abbey Meads Community Primary School Acceptable Use & E-Safety Policy (Internet)

This Acceptable Use Policy should be read in conjunction with Abbey Meads Primary School's Safeguarding and Child Protection, Prevent, Computing, Relationships and Sex Education, Data Protection, Behaviour and Anti-bullying policies. This policy also reflects the guidance 'Keeping Children Safe in Education'.

What does the 'Acceptable Use & E-Safety Policy' cover?

This policy addresses all rights, privileges and responsibilities associated with the Internet. Examples include: websites, email, chat, Virtual Learning Environment, video, discussion group's bulletin boards, real-time conferencing, and social networking sites.

Rationale

The Internet has become an important aspect of everyday life to which children need to be able to respond safely and responsibly.

At Abbey Meads Community Primary School we believe that the Internet offers a valuable resource for teachers and children providing ways to communicate with others world-wide and initiate cultural exchanges between pupils. Access to the Internet offers both children and teachers vast, diverse, and unique resources and helps to improve educational standards. It supports the professional work of staff as well as enhancing the school's management information and business administrative systems.

Internet access is available to teachers and students to promote efficiency with communication, resource sharing and access to high-quality learning material. Pupils have access to online learning spaces where pupils can access targeted learning, publish their work and track their development on programs such as Accelerated Reader, Mathletics, Purple Mash and Times Tables Rock stars.

Although we use the latest and most advanced filtering systems at Abbey Meads Community Primary School, there is always a small risk inherent with internet use that children may encounter inappropriate material on the Internet. The school will actively take all reasonable precautions to restrict pupil access to both undesirable and illegal material, as well as educate pupils to take appropriate action if they do come across such material. Pupils are only able to access the Internet under the supervision of an adult. This policy sets out measures to be taken that minimise these risks. It is recognised that this policy cannot cover all eventualities: there may be times where professional judgement is required to deal with issues not covered in this document. In these situations, staff will advise the Headteacher and Designated Safeguarding Lead of the justification for these actions.

This document applies to all members of staff and pupils at Abbey Meads Community Primary School, including senior leaders, teachers, support staff, governors and volunteers. Staff should review their practice in terms of the continually changing world of social networking and internet-based software, and ensure they follow the guidance in this document.

Aim

To ensure that children and adults can use the Internet safely and responsibly as an integral part of planning, delivering and resourcing lessons in all subjects of the curriculum, both within and outside school hours.

Guidelines

Internet access is a necessary part of the statutory curriculum. It is an entitlement for pupils who use it responsibly.

➢ In Foundation Stage nearly all of access to the Internet will be through adult demonstration. However, there may be situations when children have supervised access to specific teacher approved on-line materials.

➢ At Key Stage 1 the majority of access to the Internet will also be through adult demonstration. However, there may be situations when children have supervised access to specific teacher approved on-line materials such as Purple Mash.

➢ At Key Stage 2 Internet access will be granted to a whole class as part of a scheme of work, after discussion on responsible Internet use. This will involve the use of recommended search engines. The search engine is accessed through a proxy set up by our technician company, GHS – this proxy enforces the safest settings online so pupils cannot change them.

Children and staff (teaching and non-teaching) must never knowingly seek to view material over the Internet that is illegal, pornographic, exploitative to children, violent, sexist, racist, or in any other way offensive or unsuitable within a school environment.

The school subscribes to a filtered Internet service – RM SafetyNet. This service ensures that access to inappropriate sites is blocked; the content of web pages or searches is dynamically filtered for unsuitable words; web browsers are set to reject inappropriate sites and logs are made of banned internet sites visited by pupils and students. Our Computing Engineers will make regular checks in liaison with our technical support company, GHS, to ensure that the filtering system selected is effective in practice. The school can elect to ban individual websites or search words that it considers inappropriate on top of the RM Unify's level of filtering. The filter protects both staff and children from accidental or deliberate misuses.

The teaching of the acceptable and responsible use of the Internet is an integral part of all Computing lessons. E-safety modules are planned into both the Computing and the PSHE curriculum and are taught in conjunction with Safer Internet Day. Children are also educated on what to do if they come across inappropriate material in school - the expectation is that they will minimise the application window and inform an adult immediately if they encounter any material that makes them feel uncomfortable. The adult must then report this the Computing Co-ordinator and/or the DSL (subject to the content of material viewed) who will then contact the computing engineers who will filter the website.

As well as teaching children about e-safety through Computing or PSHE lessons, we also promote safe internet usage across the school with e-safety displays and posters. Parents receive an e-safety document on a yearly basis, linked to Safer Internet Day, informing them of websites to visit to find out more information regarding helping their children stay safe online.

Whilst in school, children do not have access to public or un-moderated chat-rooms – only regulated and teacher approved educational online discussions or forums (such as commenting on Purple Mash) will be permitted.

Pupils do not use mobile phones during the school day and on school grounds (unless for medical reasons) – any mobile phones brought to school must be handed in to the Class Teacher. It is forbidden to send abusive or otherwise inappropriate messages using the facilities provided by the school network or using personal devices of any kind.

The school's computer network security systems are reviewed regularly and all user files, temporary Internet files and history files will be monitored by our technical support company, GHS.

Virus protection software is installed and updated regularly by GHS.

Data on the school server is backed up remotely by GHS.

All access to the school network requires entry of a recognised User ID – pupils and staff must log out after every network session.

Pupils and staff must NOT: upload or download non-approved application software on the school network without permission from an admin password holder, use any form of personal storage devices (USB memory sticks, hard drives, etc.) without a virus check or break copyright and intellectual property rights rules.

Staff must ensure that the pages of any personal social networking sites (e.g. Facebook / Instagram / Twitter / YouTube / TikTok, Twitch, etc.) of which they are a member, are of an appropriate nature and that the pages of any 'friends' that they are linked to are also appropriate. Comments posted on social networking sites must not in any way bring the school, staff or pupils of the school into disrepute. General and positive comments about work are acceptable, but negative comments or negative references to specific members of staff, pupils, parents or governors are not. If inappropriate comments are seen, staff have an obligation to report this to the Senior Management Team. Staff must NOT agree to become 'friends' with or 'follow' any pupil currently at Abbey Meads Community Primary School. Staff must not access personal social networking sites on their school computer whilst on school premises. Staff personal social networking site accounts may be accessed but only outside of the school network. Content may not be downloaded from these sites onto or using school equipment.

Staff and pupils should consider carefully the implication of what they publish to social media, such as video sharing sites, e.g. YouTube, and blogging sites, e.g. Twitter, both in a personal and school capacity. Staff should ensure that their conduct befits their professional role in school. All adults working at Abbey Meads Community Primary School have a responsibility to maintain public confidence in their ability to safeguard the welfare and best interests of pupils. Staff, particularly in the case of new staff, should review their social networking site content to ensure that information publicly viewable is accurate and appropriate, and does not contain any confidential information about the school, its parents, pupils or staff.

The school recognises the value of using social media for school purposes to enhance learning and enrich communication and engagement of parents. Staff must follow the guidelines of this document when using social media: recognisable images of children may only be used with the parents' permission; when using social media in the classroom, content must be checked carefully by staff before use.

Staff should not communicate with parents or pupils using their personal mobile telephones. In the infrequent scenario where multiple school phones are needed by staff (Parent consultations evenings, etc.), staff may choose to use their personal mobile phones to communicate with parents if there is no extra charge. **Staff must ensure that their number is hidden from the caller**. **This can**

be amended in your phone's settings by turning off 'Caller ID'. Always check by calling a trusted party before making a call to a parent /carer, to ensure that your number is hidden when calling.

Staff are able to access work email and the Internet at home using the school laptops but must ensure that they do not open emails that could contain viruses when at home. Downloading software or programs from the Internet is not possible without an Admin Username and Password allocated by GHS.

Cyberbullying (using technology to embarrass, humiliate, threaten or intimidate) is dealt with in the same way as bullying at Abbey Meads Community Primary School – please see Abbey Meads Community Primary's Anti-bullying policy: records should be kept, and teacher/SMT informed of the incidences so they can be recorded and dealt with appropriately. Abbey Meads Community Primary School's Behaviour Policy is also followed. In any cases of misuse of social media by children where members of staff are misrepresented and police investigation will be considered. Pupils are taught about cyberbullying through PSHE lessons.

Teaching and learning

Internet access will be planned to enrich and extend learning activities - access levels will be reviewed to reflect curriculum requirements.

Staff will select sites which will support learning outcomes planned for pupil's age and maturity. Children in Key Stage 2 will be required to use search engines to locate websites and information, but this will be carried out with adult supervision. Where possible direct links to sites will be provided rather than a search (where internet search is not the main focus of learning).

Teachers are responsible for guiding pupils in their online activities, by providing clear objectives for Internet use - teaching staff will also ensure that pupils are aware of what is regarded as acceptable and responsible use of the Internet.

Pupils (at an appropriate level) will be made fully aware of the risks to which they may be exposed while on the Internet - they will be shown how to recognise and avoid the negative aspects of the Internet such as pornography, violence, racism and exploitation of children, through PSHE and e-safety lessons.

Specific e-safety lessons are taught at least once a year in every year group through Jigsaw, our PSHE scheme of learning alongside reminders and recaps of e-safety measures at the start of each session.

Planned seating and computer monitor positions will allow teachers to observe, trace and monitor pupil access and usage of the Internet. Internet 'History' checks can be used to monitor Internet activity of pupils whilst using the Internet.

All Internet access is filtered through a proxy server to screen out undesirable sites.

Tablets e.g. iPads

iPads are available across the school – exactly the same 'acceptable use' rules apply to these devices.

As it is easier to use these devices inappropriately without being detected, pupils are encouraged to be vigilant and responsible, and alert an adult immediately if any inappropriate use takes place.

Pupils must ask permission before using a tablet to photograph another pupil or staff member.

Tapestry

At Abbey Meads Community Primary School we use software applications that allow pupils and teachers to publish learning online.

Content uploaded to Tapestry is monitored, checked and accepted by class teachers. Teachers can refuse to accept the uploading of work, pupil's comments and parent comments if it is not deemed appropriate.

Letters are sent home to parents at the beginning of the year, outlining the purpose of Tapestry, how to connect to their child's portfolios and appropriate use. This is also discussed in Curriculum Meetings at the start of the year.

School Website & TV Screens

The copyright of all material on the school's web pages belongs to the school – permission to reproduce any material must be sought and obtained.

Contact details for the school will include only the school's postal address, e-mail address and telephone number – no information about teachers', governors' or pupils' home addresses or the like will be published.

The school will not publish any material produced by individual or groups of pupils to the website or TV screens without the agreed permission of their parents in line with the school's photographic permissions policy.

Identifiable photographs of pupils whose parents have not provided written permission will not be published to the website.

Video footage of pupils published to the website or TV screens will not be published if parents' written permission has not been provided.

Zoom / Microsoft Teams / Other video calling services

Video calling can be used to communicate effectively with other members of staff within the school or BKAT. The main purpose of using video calling should be for: staff training, staff meetings, collaboration with other members of staff, planning and assessment.

When on a video call, ensure that no other parties are present. If unknown parties are present and cannot be identified, simply end the call as soon as possible and report this to your Headteacher.

Video calling with the school approved PCE Virtual platform (Teachers2Parents) can be used for parental consultations. **If teachers are conducting these meetings from outside of the school, they must ensure that their background is neutral and/or blurred.**

Communicating e-safety

'Rules for responsible Internet use' posters will be displayed near all networked fixed position computer systems.

E-Safety lessons will be provided throughout each Computing module and will include references to Acceptable Use of the Internet. Reconsolidation lessons will also be used to affirm and address e-safety when an issue arises.

Pupils will be informed that their Internet use is monitored and be given instructions on safe and responsible use of the Internet.

All staff will be provided with a copy of the School's Acceptable Use & e-Safety Policy – teachers are aware that Internet traffic can be monitored and traced to an individual user. Each year, staff are issued with the latest policy and a signature is required to confirm it has been read and understood.

Staff will be consulted regularly about the developments of the school's Acceptable Use Policy and given instructions on safe and responsible use of the Internet.

To avoid misunderstandings teachers will contact the Computing Co-ordinator regarding any doubts that arise concerning the legitimacy of any given instance of Internet use.

All parents / guardians will be provided with a copy of this policy, (via a link on the website), informing them how we use the Internet at Abbey Meads Community Primary School and how we share the responsibility.

Equal Opportunities

When writing and reviewing this policy staff have completed an Equality and Diversity Impact Assessment in order to ensure it complies with equality obligations outlined in anti-discrimination legislation.

Policy Review

This policy will be reviewed annually.

This policy may be reviewed earlier at the discretion of the Governors or in the event of changes in policy or legislation at either governmental or LA level.

Policy Version Control

Date	Reason for update (and staff reviewing)	Next Review date
7th December 2022	Curriculum Policy Review – updating policy on handover from previous Computing Lead (TSt/SSh)	December 2023
13th March 2023	SMT review of policies and Website – Preparation for PCEs. (BB/MC)	April 2024
1st May 2024	Temporary review in lieu of Trust Policy being developed and Appendix added below.	September 2024

Appendix 1 - Filtering and **Monitoring** Policy and Procedures

1.1 Introduction

Schools in England (and Wales) are required *"to ensure children are safe from terrorist and extremist material when accessing the internet in school, including by establishing appropriate levels of filtering"* Furthermore, the Department for Education's statutory guidance 'Keeping Children Safe in Education' obliges schools and colleges in England to *"ensure appropriate filters and appropriate monitoring systems are in place and regularly review their effectiveness" and they "should be doing all that they reasonably can to limit children's exposure to the above risks from the school's or college's IT"* however, schools will need to "*be careful that "over blocking" does not lead to unreasonable restrictions as to what children can be taught with regards to online teaching and safeguarding*."

Ofsted concluded as far back as 2010 that "Pupils in the schools that had 'managed' systems had better knowledge and understanding of how to stay safe than those in schools with 'locked down' systems. Pupils were more vulnerable overall when schools used locked down systems because they were not given enough opportunities to learn how to assess and manage risk for themselves."

To further support schools and colleges in England, the Department for Education published Digital and Technology standards.

1.2 Roles and Responsibilities

The school works in partnership with **Securly and GHS** to ensure that the school infrastructure/network is as safe and secure as is reasonably possible. DfE Filtering Standards require that schools and colleges identify and assign roles and responsibilities to manage filtering and monitoring systems.

Role	**Responsibility**	**Name / Position**
Responsible Governor	Strategic responsibility for filtering and monitoring and need assurance that the standards are being met.	Claire Huckerby-Brown (Coopted Governor)
Senior Leadership	Team Member Responsible for ensuring these standards are met and: • procuring filtering and monitoring systems • documenting decisions on what is blocked or allowed and why • reviewing the effectiveness of your provision • overseeing reports Ensure that all staff: • understand their role • are appropriately trained • follow policies, processes and procedures • act on reports and concerns	Bob Buckley Headteacher Supported by Tim Smith Computing Leadership
Designated Safeguarding Lead	Lead responsibility for safeguarding and online safety, which includes overseeing and acting on: • filtering and monitoring reports • safeguarding concerns • checks to filtering and monitoring systems	Bob Buckley Headteacher
IT Service Provider	Technical responsibility for: • maintaining filtering and monitoring systems	Securly *(School processes*

	• providing filtering and monitoring reports • completing actions following concerns or checks to systems	*supported by GHS)*
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	ALL STAFF / VOLUNTEERS working on site and using school devices or observing children using devices.

1.3 Policy statement

- There is a filtering and monitoring system in place that safeguards staff and learners by blocking harmful, illegal and inappropriate content.
- There is a monitoring system that enables the prompt investigation of a potential safeguarding incident and outcomes are logged.
- Roles and responsibilities for the management of filtering and monitoring systems have been defined and allocated.
- There is a defined and agreed process for making changes to the filtering or monitoring system that involves a senior leader in the agreement of the change.
- Mobile devices that access the school's internet connection (whether school or personal devices) will be subject to the same filtering standards as other devices on the school systems.
- The school has provided enhanced/differentiated user-level filtering through the use of the **Securly** filtering system. (allowing different filtering levels for different ages/stages and different groups of users – staff/learners etc.)

1.4 Filtering Procedures

The filtering of internet content provides an important means of preventing users from accessing material that is illegal or is inappropriate in an educational context. The filtering system cannot, however, provide a 100% guarantee that it will do so, as online content changes dynamically and new technologies are constantly being developed. It is important, therefore, to understand that filtering is only one element in a larger strategy for online safety and acceptable use.

Internet access is filtered for all users. Differentiated internet access is available for staff and customised filtering changes are managed by the school. Illegal content is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation URL list and other illegal content lists. There is a clear route for reporting and managing changes to the filtering system. Where personal mobile devices are allowed internet access through the school network, filtering will be applied that is consistent with school practice.

The filtering system used in our school is up to date and applied to all:

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

This system:-

- filters all internet feeds, including any backup connections
- is age and ability appropriate for the users and is suitable for educational settings
- handles multilingual web content, images, common misspellings and abbreviations
- identifies technologies and techniques that allow users to get around the filtering such as VPNs and proxy services and block them
- provides alerts when any web content has been blocked
- is regularly updated

1.5 Monitoring Procedures

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 review of user activity on school devices. For monitoring to be effective it must pick up incidents urgently, usually through alerts or observations, allowing prompt action to be taken.

Our monitoring strategy includes:

- physical monitoring by staff watching screens of users
- network monitoring using log files of internet traffic and web access
- individual device monitoring through software or third-party services

The monitoring process alerts the school to breaches of the filtering policy, which are then acted upon.

1.6 Filtering and Monitoring Review and Checks

Strategic review

The filtering and monitoring provision is reviewed at least annually, as part of a wider online safety annual review, using either the SWGfL or LGfL 360-degree tools:

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

The review is conducted by members of the senior leadership team, the designated safeguarding lead (DSL), and the IT service provider.

Operational review

In addition to the annual review of filtering and monitoring, checks to filtering and monitoring systems are completed and recorded as part of the filtering and monitoring review process. How often the checks take place

will be based on the context, the risks highlighted in the filtering and monitoring review, and any other risk assessments.

Checks will be undertaken from both a safeguarding and IT perspective.

In our school, we complete the following checks:-

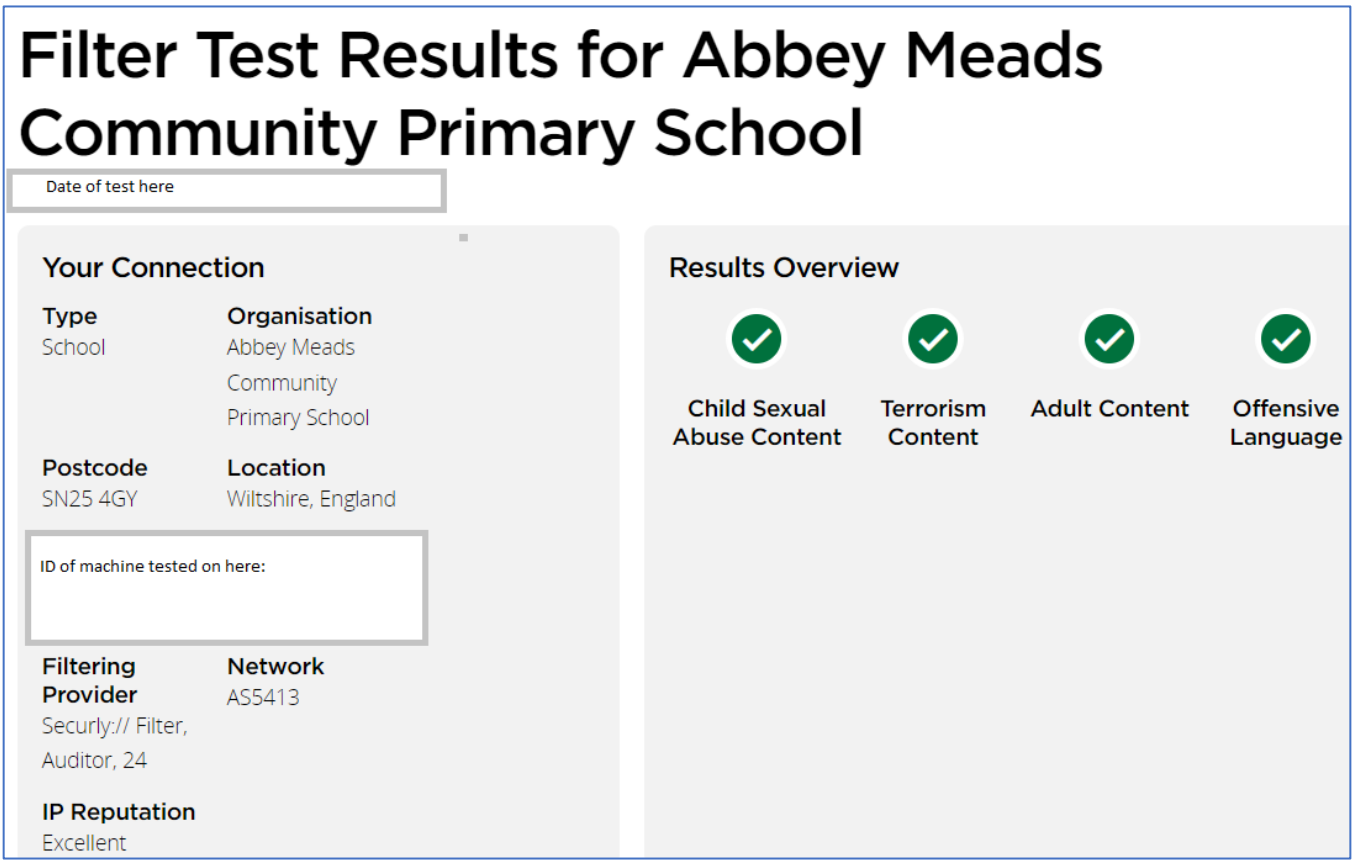
1. a review of the monitoring logs to check for patterns and themes which may arise from user access and cause concern. These are completed weekly via the Monday morning Securly reports.

2. Checks of the filtering systems are performed on 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

Logs of checks are kept so they can be reviewed. These record:

- when the checks took place
- who did the check
- what was tested or checked *(test accounts using staff, guest and pupil permissions)*
- resulting actions

A check using the SWGfL Test Filtering website is also completed termly or when alerted to a possible breach.



1.7 Changes to Filtering and Monitoring Systems

There should be a clear process for requests to change the filtering and monitoring systems and who makes the decision to alter the filtering system.

In this school:

- users may request changes to the filtering and monitoring systems only via the Headteacher and Head of Computing Curriculum
- these two responsible people will consult with GHS for advice on both cyber security and child safety, using their wider base of knowledge implementing this service across many schools and local authorities.
- Only when both HT and Computing Lead are in agreement will a change be made and this will be a school decision based on advice, but remains the responsibility of the school not that of GHS.

1.8 Training/Awareness

It is a statutory requirement in England that staff receive training, at least annually, about safeguarding, child protection, online safety and filtering and monitoring.

Governors, Senior Leaders and staff are made aware of the expectations of them:

- at induction
- at whole-staff/governor training
- through the awareness of policy requirements
- through the acceptable use agreements
- in regular updates throughout the year

Those with specific responsibilities for filtering and monitoring receive enhanced training to help them understand filtering and monitoring systems and their implementation and review.

Learners are made aware of the expectations of them:

- in lessons both in discrete lessons on e-safety and as an integral part of all lessons using technology before starting a session.
- through the acceptable use agreements

Parents are informed of the school's filtering policy through the acceptable use agreement and through online safety awareness sessions/newsletter etc.

This appendix is informed by the Department for Education (DfE) guidance, Keeping Children Safe in Education, and the Digital and Technology Standards and is based on a template from the South West Grid For Learning (SWGfL).

Date: May 2024