A FAMILY, A FOUNDATION, A FUTURE

Whitminster Endowed Cof E Primary School

On-Line Safety policy

See also Keeping Children Safe in Education policies and Data Protection policies

Written by : A Parry-Jones

Agreed by Curriculum Governors:

Review Date: Summer 2026

Scope of the Policy

This policy applies to **all** members of the school community (including volunteers, parents/carers, visitors and community users) who have access to or use school ICT systems inside and outside school. The Education and Inspections Act 2006 empowers Headteachers, to such extent as is reasonable, to regulate the behaviour of pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is relevant to incidents, including cyber-bullying, which may take place out of school, but are linked to membership of the school. The school will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, inform parents / carers of known incidents of inappropriate online safety behaviour that take place out of school. This policy should be read alongside the acceptable use policies for staff and pupils, the anti-bullying policy and the behaviour policy.

The breadth of issues classified within online safety is considerable, 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 purposes'

- **conduct:** personal online behaviour that increases the likelihood of, or causes, harm; for example, making, sending and receiving explicit images (e.g consensual and non-consensual 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/)

Roles and Responsibilities

These are clearly detailed in Appendix 1 for all members of the school community.

- The governors have overall responsibility for ratifying the policy, ensuring that it is implemented and monitoring it. This action is delegated to the Curriculum Committee.
- The Headteacher is responsible for ensuring the safety (including online safety) of members of the school community, though the day to day responsibility for online safety is delegated to the Analytical team and IT subject leader. The Headteacher is also the designated safeguarding lead and is trained in online safety issues and aware of the potential for serious child protection issues to arise from sharing of personal data, access to illegal / inappropriate materials, inappropriate on-line contact with adults / strangers, potential or actual incidents of grooming and cyber-bullying.

Training and Awareness Raising

There is a planned programme of Online safety training for **all** staff and governors to ensure that they understand their responsibilities, as outlined in this, and the acceptable use policies. The following actions are undertaken to raise awareness:

- The DSL receive regular updates through attendance at relevant training such as SWGfL and SAS training sessions .
- All staff, including support staff, receive an annual safeguarding update in September.

- Any reported incidents and how they are addressed are discussed at staff meetings and used as an opportunity to test our processes and update staff on how to deal with issues.
- The DSL provides advice/guidance and training as required to individuals and seeks LA advice on issues where appropriate.
- A training log is used to record when updates and training are delivered.

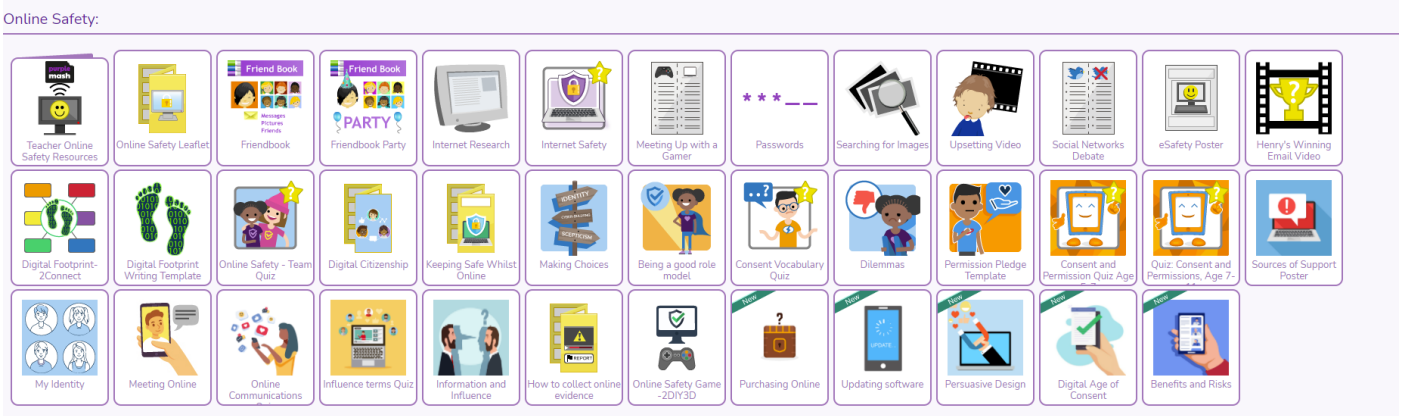
Induction Processes

- All new staff receive safeguarding training as part of their induction programme.
- Parents of new reception children receive a briefing about online safety and processes when their child starts school. There are also updates to this throughout the key stages.
- Parents of children who join school mid-year are made aware of the processes and their children are also introduced to the acceptable use policy.

Teaching and Learning

Online safety is now a statutory part of the programme of study for all key stages. Rules and technical solutions are are not infallible and we are aware that outside school children will be using unfiltered internet provision. We believe it is crucial to educate children about how to behave responsibly online and how to keep themselves and others safe. Children and young people need the help and support of the school and parents to recognise and avoid online safety risks. There is a planned and progressive scheme of work for online safety which is taught at every year group. This is based around the Purple Mash scheme and, across the key stages, covers:

- Internet safety
- Privacy and security
- Relationships and communication
- Cyberbullying
- Information literacy
- Self image and identity
- Digital footprint and reputation
- Creative credit and copyright



The scheme of work is delivered as part of computing, PSHE and other lessons.
Regular opportunities are taken to reinforce online safety messages in all lessons and to teach pupils to be critically aware and consider the accuracy of the information they access online. Online safety messages are also reinforced through other subjects and through a planned programme of other activities such as assemblies and events. Older pupils are taught to acknowledge the source of information and respect copyright. Pupils are helped to understand the AUP, recognise online safety risks, adopt safe practices, report any issues and keep evidence to support reporting (for older children). Staff model safe practice in use of technologies and mobile devices and guide students to appropriate sites and follow practices for dealing with unsuitable material found in internet searches. Where pupils undertake searching of the internet staff monitor the content of the websites they are visiting. If they identify pupils who may be vulnerable, for example, who are not adopting safe practices or completing inappropriate searches this should be logged and appropriate support given to those pupils to help them understand the risks and what to do to keep safe.

The following aspects also contribute to our curriculum provision:

- Coverage of learning experiences is recorded and staff check understanding when teaching about online safety.
- Annual online safety events such as Safer Internet Day are also used to raise awareness.

Rules for Keeping Safe

These are reinforced through the following:

- Pupils sign an acceptable use agreement and this is also communicated to parents who we hope will reinforce the messages at home.
- Pupils are helped to understand the student acceptable use policy and school rules for online safety and encouraged to act accordingly.
- All classes have online safety rules displayed in their classroom and staff regularly refer to these, for example, during activities where children are searching the internet for information.
- Staff act as good role models in their own use of IT.
- Staff are aware that there may be some children that are more vulnerable than others to being approached online and endeavour to ensure that these children understand the issues involved.
- Online behaviour is dealt with in accordance with our behaviour policy. There are sanctions and rewards in place for this.

Education – parents / carers and the community

Parents and carers have an essential role in educating their children and monitoring their behaviour online, however they may have a limited understanding of the risks and issues and underestimate the dangers or be unsure how to deal with them. The school aims to raise awareness and support parents through:

- Curriculum activities
- Letters and newsletters including information on any online safety issues that have been raised in school (anonymously recorded) and how to address these
- Parents / carers information afternoons (before homework showcases)
- Events such as Safer Internet Day
- Providing information and weblinks about where to access support on the website

Education – staff and volunteers

All staff receive regular online safety training so that they understand the risks and their responsibilities. This includes:

- A planned programme of online safety training which is regularly updated and reinforced and linked to the expectations outlined in this policy, Keeping Children Safe in Education and in the Ofsted framework.
- All new staff receive online safety training and training on relevant policies and expectations as part of their induction programme.
- The DSL receive regular updates and external training to support them to do their role.
- Policies relevant to online safety and their updates are discussed in staff meetings.

Self-evaluation and Improvement

The school undertakes self-evaluation in order to inform actions to continually improve online safety provision through the following:

- Local authority safeguarding audit
- 360 degree safer online self-evaluation tool which is also used to benchmark our provision against other schools.
- Surveys with pupils and staff

Internet Provider and Filtering

The school internet service is provided by SWGFL and this includes a filtering service to limit access to unacceptable material for all users.
Internet access is filtered for all users by SWGFL. See appendix 2
Technical staff monitor internet traffic and report any issues to schools.

Filtering and Monitoring

We aim to 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. The governing body has overall strategic responsibility for filtering and monitoring and need assurance that the standards are being met.
To do this, they identify and assign:
• a member of the senior leadership team (DSL) 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
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 will work closely with governors, the designated safeguarding lead (DSL) and IT service providers in all aspects of filtering and monitoring.

Technical Staff - Roles and Responsibilities

The school ensures, when working with our technical support provider that the following guidelines are adhered to.

- There are regular reviews and audits of the safety and security of school ICT systems.
- Servers, wireless systems and cabling are securely located and physical access is restricted.
- All users have clearly defined access rights to school ICT systems and are provided with a username and password by the technical support provider.
- School ICT technical staff regularly monitor and record the activity of users on the school ICT systems and users are made aware of this in the Acceptable Use Policy.
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations etc from accidental or malicious attempts which might threaten the security of the school systems and data.
- The school infrastructure and individual workstations are protected by up to date virus software.
- An agreed policy is in place (AUP) regarding the downloading of executable files by users
- An agreed policy is in place (AUP) regarding the extent of personal use that users (staff / students / pupils / community users) are allowed on laptops and other portable devices that may be used out of school.
- An agreed policy is detailed regarding the use of removable media (e.g. memory sticks / CDs / DVDs) by users on school workstations / portable devices in our acceptable use agreement.

Use of Digital Images and Video

Ease of access to technologies which take digital images and video has many benefits for learning. Taking and sharing images and video are much easier and, if not managed, this could increase the potential risk of misuse and has the potential to be used for cyberbullying. The school informs and educates users about the risks associated with digital images and these are outlined in the acceptable use policies:

- When using digital images, staff educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images including publishing their own images on social networking sites.
- Pupils should not take, use, share, publish or distribute images / video of others without their permission and staff reinforce this when appropriate.
- Written permission is obtained from parents or carers before photographs of pupils are taken. These photographs are only taken to be used for educational purposes or to promote achievements or the school.
- Staff are allowed to take digital / video images to support educational aims, but follow guidance in the acceptable use policy concerning the sharing, distribution and publication of those images.

- Images are only taken and used of individuals where there is a signed permission form in place.
- Pupils full names are not published on any online platform or school communication including the web site, newsletter or twitter feed. Photographs published anywhere that include pupils are carefully selected and not used in association with pupils' full names or other information that could identify them.
- Care is always taken to ensure that pupils are appropriately dressed if images are taken and that they are not participating in any activity which might bring individuals or the school into disrepute.
- In accordance with guidance from the Information Commissioner's Office, parents / carers are welcome to take videos and digital images of their children at school events for their own personal use as this is not covered by the General Data Protection Regulation. However in order to protect other children and respect privacy these images should not be published or made publicly available on social networking sites. Parents / carers should also not comment on any activities involving other pupils in the digital / video images. This is clearly detailed in our acceptable use policy for parents.

Mobile Technologies

These might include mobile phones, tablets or any other device that has the capability of accessing the school's wireless network. The primary use of these in school is to support learning, teaching and management.

Staff and governors can gain access to wifi on personal devices through guest wifi access. This provides limited access to the internet only and not to the school network.
Children are not allowed to use their personal devices in school as the school provides access to the technologies to be used for learning.
Staff are not allowed to use their personal mobile phones in school while they are teaching and any use should be restricted to times when children are not present. The only exception to this is in case of emergency during a school trip.
Photos taken for educational reasons or celebrations may as necessary be taken on a personal device but are immediately deleted permanently after upload to social media or school website.

Communications Technologies and Social Media

A wide range of communications technologies have the potential to enhance learning and management. The acceptable use agreements outline how these systems should be used.

- The official school email service is used for communications between staff, and with parents/carers and students as it provides an effective audit trail. Communications are always professional in tone and content.
- Users are made aware that email communications may be monitored and what to do if they receive an email that makes them feel uncomfortable, is offensive, threatening or bullying in nature through the acceptable use policies.
- Governor communications take place through governor school e-mail accounts.
- Personal email addresses, text messaging, public chat and social networking programmes are not be used for communications with parents/carers and children.
- The school uses Twitter / Facebook to update parents on news and events and this is managed and monitored by a named member of staff who approves content and monitors use of the account.
- Personal information is also not posted on the school website and only official email addresses are listed for members of staff.
- Guidance on personal use of social media and mobile devices is included in the staff, parent and pupil acceptable use policies including clear reporting mechanisms. Training is provided for staff and risks, reporting and issues around social networking forms part of the learning for pupils.
- Staff ensure that no reference is made in social media to pupils, parents or other staff and do not engage in online discussions on personal matters about any member of the school community
- Personal opinions are not attributed to the school
- Security settings on personal social media profiles are regularly checked to minimise risk
- Staff personal use of social media where it does not relate to the school is outside the scope of the policy but is should be made clear that the member of staff is not communicating on behalf of the school. If staff come across communications that might bring the school into disrepute in their personal communications they should not get involved, refer the publisher to relevant complaints procedures and report the issue.

Copyright

School office manager is responsible for making sure that software licence audit is regularly updated and also making regular checks to ensure the number of software installations matches the licences held. Where there are insufficient licences this could breach the Copyright Act which may lead to fines or unexpected additional license costs.

Data Protection

Personal Data is defined as any data which relate to a living individual who can be identified from the data. This includes opinion about the individual. Sensitive Personal Data about a person includes information about their racial or ethnic origin, political opinions, their religious beliefs or other beliefs of a similar nature, whether they are a member of a trade union and their physical or mental health or condition.

Personal data is recorded, processed, transferred and made available according to the General Data Protection Regulation and is:

- Fairly and lawfully processed
- Processed for limited purposes
- Adequate, relevant and not excessive
- Accurate
- Kept no longer than is necessary
- Processed in accordance with the data subject's rights
- Secure and only transferred to others with adequate protection

Transfer of Data

Whenever possible secure online storage is used to ensure that documents do not need to be transferred to limit the risk. We ensure that data is stored in accordance with the requirements laid down by the Information Commissioner's Office and within the EU. This also applies to cloud storage used.

The school ensures that:

- It holds the minimum personal data necessary to enable it to perform its function and does not hold it for longer than necessary for the purposes it was collected for.
- The data held is accurate, up to date and inaccuracies are corrected as quickly as possible.
- All personal data is fairly obtained in accordance with our "Privacy Notice" and lawfully processed. Personal and sensitive data relating to pupils or staff is not e-mailed as this is not secure.
- Personal data including assessment data is transferred using secure file transfer.
- Where information does need to be transferred between devices then encrypted memory sticks are used.
- It has clear and understood arrangements for the security, storage and transfer of personal data
- It is registered as a Data Controller for the purposes of the General Data Protection Regulation (GDPR)
- Risk assessments are regularly carried out.
- Data subjects have a right to access their data and there are clear procedures for this.
- There are clear and understood policies and routines for the deletion and disposal of data.
- There is a policy for reporting, logging, managing and recovering from information risk incidents.
- The staff acceptable use policy clearly defines the data protection measures that staff should take and how data can be securely stored and deleted.

Staff ensure that they

- Take care to ensure safe keeping of personal data and minimise the risk or loss or misuse
- Use personal data only on secure password protected website and devices and log off at the end of every session
- Transfer data using encryption and secure password protected devices

Where personal data is stored on removable media:

- The data is encrypted and password protected
- The device is password protected
- The device has approved virus and malware checking software
- The data is securely deleted from the device once finished with.

Reporting and Recording

There are clear reporting mechanisms in place for online safety incidents and all staff are regularly reminded of these and fully aware of their responsibilities to follow up any reported issues.

Staff should report online safety issues are reported to the DSL. If these include allegations of bullying then the anti-bullying policy is followed. Issues which may impact on the well-being and safety of a child are reported directly to the DSL and Child Protection procedures are followed. Issues impacting on staff or to the detriment of the school should be reported to the headteacher or to the Chair of Governors if the headteacher is absent or the accusation involves the headteacher.
Pupils are encouraged to report any incidents to an adult whether it relates to themselves or a friend. We encourage children to take responsibility for protecting each other.

Managing Incidents

In the event of suspicion of an infringement of policy then all the following steps should happen.

- More than one senior member of staff should be involved in investigating to protect possible future accusations.
- Use a computer that will not be used by young people which could be taken off site by the police if required.
- Ensure staff have internet access to investigate but that sites and content are closely monitored and recorded.
- Record the URL of any site containing alleged misuse and the nature of the content causing concern. It may be useful to record and store screenshots of the content by printing them, signing them and attaching them to the record. Except for child abuse images as this would constitute an offence.
- Once the investigation is complete the investigating group should identify the appropriate response in line with policies which may internal procedures, involvement of LA or police.

Reporting to the police

- If the content being reviewed includes images of child abuse then monitoring should be stopped and the police informed immediately. Other incidents to be referred to the police are
    - incidents of 'grooming' behaviour
    - the sending of obscene materials to a child
    - adult material which potentially breaches the Obscene Publications Act
    - criminally racist material
    - promotion of terrorism or extremism
    - other criminal conduct, activity or materials

  In any of the above isolate the computer involved as any change to its stage may hamper a police investigation.

Sanctions and Disciplinary proceedings

Sanctions and disciplinary procedures may be taken where users visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to (unless this is part of an investigation:

- Child Sexual abuse images
- Grooming, incitement, arrangement or facilitation of sexual acts against children Contrary to the Sexual Offences Act 2003.
- pornography, adult or mature content
- promotion of any kind of discrimination, racial or religious hatred
- personal gambling or betting
- personal use of auction sites
- any site engaging in or encouraging illegal activity
- threatening behaviour, including promotion of physical violence or mental harm
- any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute

- using school systems to run a private business
- use systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school
- uploading, downloading or transmitting commercial software or any copyrighted materials belonging to third parties, without the necessary licensing permissions
- revealing or publicising confidential or proprietary information (e.g. financial or personal information, databases, computer or network access codes and passwords)
- creating or propagating computer viruses or other harmful files
- carrying out sustained or instantaneous high volume network traffic (downloading or uploading files) that causes network congestion and hinders others in their use of the Internet

In addition the following indicates school policy on these uses of the Internet:

	Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable
Online gaming (educational)		✓		
Online gaming (non-educational)				✓
Online gambling				✓
Online shopping / commerce			✓	
File sharing (using p2p networks)			✓	

Sanctions: Pupils

The 2011 Education Act increased powers with regard to the searching for and of electronic devices and the deletion of data. These are applied through the school's Behaviour Policy.

Incidents	Refer to class teacher / tutor	Refer to Headteacher	Refer to Police	Refer to technical support staff for action re filtering / security etc	Inform parents / carers	Removal of network / Internet acce rights	Warning	Further sanction eg detention / exclusion

Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).			✓		✓			
Unauthorised use of non-educational sites during lessons	✓	✓		✓			✓	
Unauthorised use of mobile phone / digital camera / other handheld device	✓							
Unauthorised use of social networking / instant messaging / personal email	✓			✓				
Unauthorised downloading or uploading of files	✓			✓			✓	
Allowing others to access school network by sharing username and passwords		✓		✓	✓	✓	✓	✓
Attempting to access or accessing the school network, using another pupil's account		✓		✓	✓	✓	✓	✓
Attempting to access or accessing the school network, using the account of a member of staff		✓		✓	✓	✓	✓	✓
Corrupting or destroying the data of other users	✓			✓	✓	✓		✓
Sending an email, text, instant message, tweet or post that is regarded as offensive, harassment or of a bullying nature		✓		✓		✓		✓
Continued infringements of the above, following previous warnings or sanctions		✓		✓	✓	✓		✓
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school		✓				✓		✓
Using proxy sites or other means to subvert the school's filtering system		✓		✓			✓	
Accidentally accessing offensive or pornographic material and failing to report the incident		✓			✓		✓	
Deliberately accessing or trying to access offensive or pornographic material			✓		✓	✓		✓
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act		✓			✓	✓		✓

Sanctions: Staff

Incidents:	Refer to line manager	Refer to Head teacher	Refer to Local Authority / HR	Refer to LADO(L)/Police(P)	Refer to Technical Support Staff fc action re filtering etc	Warning	Suspension	Disciplinary action
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).				L,P				
Excessive or inappropriate personal use of the Internet / social networking sites / instant messaging / personal email		✓				✓		
Unauthorised downloading or uploading of files		✓			✓	✓		
Allowing others to access school network by sharing username and passwords or attempting to access or accessing the school network, using another person's account		✓						
Careless use of personal data e.g. holding or transferring data in an insecure manner		✓						
Deliberate actions to breach data protection or network security rules		✓		L				✓
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software		✓						✓
Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature staff		✓	✓					✓
Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature to learners		✓		L				✓
Breech of the school e-safety policies in relation to communication with learners		✓		L				✓
Using personal email / social networking / instant messaging / text messaging to carry out digital communications with pupils?		✓		L				✓
Actions which could compromise the staff member's professional standing		✓	✓					
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school		✓	✓					
Using proxy sites or other means to subvert the school's filtering system		✓		P	✓			✓
Accidentally accessing offensive or pornographic material and failing to report the incident		✓		L	✓	✓		
Deliberately accessing or trying to access offensive or pornographic material		✓		L,P				✓
Breaching copyright or licensing regulations		✓						
Continued infringements of the above, following previous warnings or sanctions		✓		L				✓

Monitoring

The school will monitor the impact of the policy through an analysis of:

- Logs of reported incidents and responses
- Monitoring logs of internet activity and any network monitoring data
- Surveys / questionnaires of students, parents / carers, and staff including non-teaching staff
- Monitoring information about the teaching programme and coverage within the curriculum
- Regularly checking that pupils and staff are clear about how to report incidents and respond to them
- The content of the web site and twitter account is regularly monitored by governors and senior leaders to ensure that it complies with this policy and the acceptable use policies.
- Any other web site, such as the school friends, that is linked to the school name is also regularly monitored to ensure that the school is always presented accurately and professionally.

Appendix 1: Roles and Responsibilities

Role	Responsibility
Governors	Approve and review the effectiveness of the online safety policy and acceptable use policies
Head teacher and Senior Leaders:	Duty of care to ensure the safety (and online safety) of the school community. The Headteacher and at least one other member of SLT should know the procedure to be followed in the event of a serious online safety allegation being made against a member of staff. Ensure that all staff receive suitable CPD to carry out their Online safety roles. Ensure that there is a system in place for monitoring and support of those who carry out the internal online safety role. Inform the local authority about any serious Online safety issues including filtering Ensure that the school infrastructure / network is safe and secure and that policies and procedures approved within this policy are implemented. Develop an online safety teaching programme to deliver the statutory programme of study. Monitor online safety teaching to ensure this is being delivered and is having an impact on pupils' understanding.
Child Protection Safeguarding Lead	Have received training in online safety issues and know the potential for child protection and safeguarding issues to arise from sharing personal data, access to illegal // inappropriate materials, inappropriate online contact with strangers, potential or actual incidents of grooming and cyber-bullying.
Curriculum Leaders	Ensure online safety is appropriately reflected in teaching programmes where relevant eg anti bullying, English publishing and copyright and is reflected in relevant policies.
Teaching and Support Staff	Ensure they have an up to date awareness of school online safety issues, policies and practices. Have read, understood and signed the Staff Acceptable Use Agreement (AUP) Act in accordance with the AUP and Online safety policy Report any suspected misuse or problem to the Headteacher. In the event that the incident involves the Headteacher report to the governor responsible for safeguarding. Only communicate with pupils / parents / carers professionally through official school systems Ensure online safety issues are embedded in the curriculum and other activities Ensure pupils follow the online safety rules Ensure that the school programme of study for online safety is delivered through their teaching Monitor ICT activity in lessons, extra-curricular and extended school activities Deliver the scheme of work for online safety and ensure children have a good understanding of what they are being taught. Monitor use of digital technologies (mobile devices and cameras etc) in lessons and other school activities where their use if allowed and implement policies about their use. Ensure that students are guided to appropriate sites in pre-planned internet use, that they are aware of how to search more safely and that any unsuitable material that is accessed is dealt with according to school policy. Immediately report any issues in accordance with school policy.
Students / pupils	Use schools systems in accordance with the pupil acceptable use policy Practice age-appropriate safe searching in order to reduce access to unsafe material Understand how to report online safety issues and do this immediately when an issue arises Know and follow the policies on use of mobile devices and cameras including taking images. Understand the importance of using technologies safely outside school and know that the policy covers actions out of school that are related to their membership of the school Help their friends to keep safe by pointing out any risks and what they could do about them
Parents and carers	Read the school guidance about online safety in the newsletter and on the website and take appropriate action if required to keep their child safe. Endorse (by signature) the Pupil Acceptable Use Policy Ensure that their child / children follow appropriate acceptable use rules at home Discuss online safety issues with their child / children and monitor their home use of ICT systems (including mobile phones and games devices) and the internet

	Access the school website in accordance with the relevant school Acceptable Use Policy. Keep up to date with issues through school updates and attendance at events Ensure they follow the school policy on taking digital and video images at school events Ensure their children following rules on appropriate use of childrens' own devices in school Report any online safety issues that could impact on safeguarding of any children or learning in school so that the school can put in place appropriate measures and use these to inform any changes to teaching
IT Technician	Ensure the school's ICT infrastructure is secure and is not open to misuse or malicious attack Ensure that the school meets Online safety technical requirements of the LA Ensure users may only access the school network through an enforced password protection policy, where passwords are regularly changed Ensure that filtering is robust is blocking but does not inhibit learning and teaching Keep up to date with online safety technical information and update others as relevant Ensure use of the network is regularly monitored in order that any misuse / attempted misuse can be reported to the Headteacher / online safety leader for investigation / action / sanction. Ensure monitoring software / systems are implemented and updated Ensure all security updates / patches are applied (including up to date anti-virus definitions, windows updates) and take action to prevent spyware and malware.
Community Users	Sign and follow the AUP before being provided with access to school systems.

Appropriate FILTERING

In May 2016, the UK Safer Internet Centre issued advice on 'appropriate filtering'. This was based on reforms in the Keeping Children Safe in Education statutory guidance.

The changes outline that by having the appropriate filters and monitoring systems in place, children should not be able to access harmful or inappropriate material from the school or colleges IT system.

The UK Safer Internet Centre have aimed to outline what Education providers should consider to be appropriate filtering.

Here we outline the questions you should be asking your current filtering provider and how our solution RM SafetyNet meets these standards.

Essential QUESTIONS...

Q: Do you have the ability to block access to illegal child abuse images and content (CAIC)?

A: Yes, this content is part of the IWF (Internet Watch Foundation) list, which has been implemented as part of the RM block list since 2004 and cannot be de-activated.

Q: Do you have the ability to provide age appropriate filtering?

A: User-based filtering gives schools greater flexibility and control over Internet filtering.

Filter by individual, year group, after-school club or by tailoring your own user groups. You can also choose to allocate specific times at which websites can be accessed.

Q: Can we get a rich filtering system that is easy to use regardless of experience and gives us control to permit or deny access to specific content?

A: Yes, RM SafetyNet provides the school administrator full control via a web portal. The administrator portal provides a modern, clean and simple workspace. You will have the ability to create multiple groups of users, with the relevant rules and time frames. For example, an after school journalism club can be given more access than during the school day.

Q: Are you able to offer keyword/search term blocking?

A: RM SafetyNet gives schools greater flexibility and control, allowing administrators to block certain words and phrases from being searched.

RM SafetyNet will use SafeSearch to help block inappropriate or explicit images from search results, including but not limited to Google and Bing and cannot be turned off or altered by any user.

URL blocklists are included as standard, incorporating RM's own UK developed definitions along with content from the Internet Watch Foundation database, this is updated on an hourly basis.

Q: Are you able to integrate the "police assessed list of unlawful terrorist content, produced on behalf of the Home Office?

A: Yes, this is integrated in the RM SafetyNet blocklist and cannot be de-activated.

Q: Do you have the ability to publish a rationale that details your approach to filtering with classification and categorisation as well as over blocking?

A: We categorise our filter lists based on customer feedback and software 'scanning' of the Internet for new and updated web pages:

- IWF child abuse images database
- Extremist content
- Active adapt content filtering
- Pornography & illegal or age-restricted activity
- Drugs & substance abuse
- Violence
- Intolerance
- Web-based chat
- Social networking
- Proxy bypass
- Web-based mail
- Non-educational games
- MP3 & .exe files

We publish all of our filtering policies on our website.

Q: Do you have the ability to identify individual users?

A: RM SafetyNet integrates with Active Directory and soon, different MIS' and Google Apps for Education.

Q: Will we have the ability to apply filtering centrally from our school network?

A: Yes, RM SafetyNet is a network level filter. It allows you to push appropriate filtering out to all of your users that are accessing the Internet via network devices.

Q: Do you offer a reporting mechanism to report inappropriate websites visited by your users?

A: RM SafetyNet reporting is tailored to school requirements. It provides access to data on user activity as well as trends across the school community. User logs include detail including date, time, username and group, along with the URL's.

- Top search terms across the school
- Top bandwidth users
- Analysis of user activity

Q: Do you have the ability to block content via mobile and app technologies?

A: For apps that load content from web based cloud services these can typically be permitted or denied using standard filter rules within the SafetyNet administration interface, and we offer guidance on common URLs to block.

For mobile applications that communicate on non-standard web ports these can typically be denied by firewall policy, which can be modified via the standard change request process rather than the RM SafetyNet administration interface.

To find out more call us free on **0808 172 9532** or email **escafety@rm.com**

Appendix 3 COVID On-line Safety (taken from Remote Learning Policy)

Remote Learning On-line Safety (COVID 19 Restrictions)

Where possible, all interactions will be textual and public.

Using video communication

All staff and pupils using video communication must:

- Communicate in groups – one-to-one sessions are not permitted unless parents are also in the room.
- Wear suitable clothing – this includes others in their household.
- Be situated in a suitable 'public' living area within the home with an appropriate background – 'private' living areas within the home, such as bedrooms, are not permitted during video communication.
- Use appropriate language – this includes others in their household.
- Maintain the standard of behaviour expected in school.
- Use the necessary equipment and computer programs as intended.
- Not record, store, or distribute video material without permission.
- Ensure they have a stable connection to avoid disruption to lessons.
- Always remain aware that they are visible.

Using audio communication

All staff and pupils using audio communication must:

- Use appropriate language – this includes others in their household.
- Maintain the standard of behaviour expected in school.
- Use the necessary equipment and computer programs as intended.
- Not record, store, or distribute audio material without permission.
- Ensure they have a stable connection to avoid disruption to lessons.
- Always remain aware that they can be heard.

The school will consider whether one-to-one sessions are appropriate in some circumstances, e.g. to provide support for pupils with SEND. This will be decided and approved by the Head Teacher in collaboration with the SENDCO.

Pupils not using devices or software as intended will be disciplined in line with the behaviour policy.

The school will risk assess the technology used for remote learning prior to use and ensure that there are no privacy issues or scope for inappropriate use.

The school will ensure that all school-owned equipment and technology used for remote learning has suitable anti-virus software installed, can establish secure connections, can recover lost work, and allows for audio and visual material to be recorded or downloaded, where required.

The school will communicate to parents via newsletter about any precautionary measures that need to be put in place if their child is learning remotely using their own/family-owned equipment and technology, e.g. ensuring that their internet connection is secure. This will be at regular intervals throughout the year.
During the period of remote learning, the school will maintain regular contact with parents to:

- Reinforce the importance of children staying safe online.
- Ensure parents are aware of what their children are being asked to do, e.g. sites they have been asked to use and staff they will interact with.
- Encourage them to set age-appropriate parental controls on devices and internet filters to block malicious websites.
- Direct parents to useful resources to help them keep their children safe online.

The school will not be responsible for providing access to the internet off the school premises and will not be responsible for providing online safety software, e.g. anti-virus software, on devices not owned by the school.