MARIAN VIAN PRIMARY SCHOOL

E-SAFETY POLICY

Marian Vian Primary School is committed to safeguarding and promoting the welfare of children and young people and expects all staff and volunteers to share this commitment.

Staff Responsible:	DSL and Computing Leads
Date of Review:	October 2025
Date of Next Review:	October 2027

VERSION CONTROL

Date	Change
February 2018	New Policy
March 2020	Page 4 – reference changed to “Keeping Children Safe I Education 2019”
	Page 10 – Clarification of the use of USBs in school – no longer permitted for children
	Page 11 – Clarification regarding the issue of pupil e-mail accounts. Previous version implied they were routinely issued
	Page 13 – Section added regarding parents WhatsApp groups
	Page 13 – Bullet point added regarding staff not engaging with parents on social media
	Page 14 – Sentence added regarding parents not allowing children access to non age-appropriate sites
	Page 17 – Section added regarding children not brining mobile phones into school
	Page 22 – Additional link added for Turn IT On filtering information
March 2023	Page 5 – addition and update of key legislation
	Page 6 – addition of smart watches
	Page 6 – roles and responsibilities addition of ICT Leads
	Page 10 - Reducing Online Risks - Addition of statements: ‘Staff will undertake RPA Cyber Training annually.’ and ‘Our website has a direct link to Child Exploitation and Online Protection where concerns about online sexual abuse or the way someone has been communicating with you online can be instantly reported.’
	Page 11 – filtering update
	Page 11 – Dealing with Filtering Breaches Deletion of /or for the point 2 The member of staff will report the concern (including the URL of the site if possible) to the Inclusion Manager and/or technical staff.
	Page 12 - Security and Management of Information Systems Alteration of point 2 from ‘and staff must keep USBs malware-free if on occasion they need to bring them in from home.’ to ‘Staff and children are not allowed to bring work into school on USBs, instead email to the class email account.’
	Page 13 – Pupils Alteration of: ‘If pupils need email accounts for educational purposes, these will be provided by the school.’ to ‘Pupils are provided with email accounts for educational purposes by the school.’ Addition of ‘annually’ to ‘Pupils will sign an AUP annually and will receive education regarding safe and appropriate email etiquette before access is permitted.’
	Page 13 – Change of Virtual Learning Environment to Remote Learning Environment
	Page 14 – Staff use of social media Addition of second sentence to point No member of staff should engage with children or parents through social media. *Where staff members are also parents, they have a responsibility to be professional at all times in their communication with parents via group or individual messaging.*
	Page 16 – Change of wording in point 7 to’ Parents, carers and pupils will have given consent of any official social media use, along with expectations for safe use and action taken to safeguard the community.’
	Page 19 - Pupils’ Use of Personal Devices and Mobile Phones Addition of ‘over the age of 18’ to point 7 ‘Pupils’ Use of Personal Devices and Mobile Phones.’

	Page 19 - Responding to Online Safety Incidents and Concerns Addition of 'up-skirting' to point 1. 'All members of the school community will be made aware of the reporting procedure for online safety concerns, including: breaches of filtering, youth produced sexual imagery (sexting), up-skirting, cyberbullying and illegal content.
	Page 22– Cyberbullying – Addition of 'and Safeguarding Policy' to point Cyberbullying, along with all other forms of bullying, will not be tolerated and will be dealt with in line with the schools' Anti-bullying and Behaviour Policy and Safeguarding Policy.
	Page 23- Links with other policies Addition of Safeguarding Policy, Staff Code of Conduct, Whistleblowing Policy
29.4.24	Addition of Commerce in a main issue area Change from Inclusion Manager to DSL change of IT Lead to Computing Lead Addition of roles for Governors and Headteacher Addition of Cyberbullying and AI Revision of responsibilities
27.11.24	Addition of AI appendices

Contents

Aims

This policy takes into account the Department for Education's (DfE's) statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for schools on:

- Teaching online safety in schools
- Preventing and tackling bullying and cyber-bullying: advice for headteachers and school staff
- Relationships and sex education
- Searching, screening and confiscation

It also refers to the DfE's guidance on protecting children from radicalisation.

It reflects existing legislation, including but not limited to the Education Act 1996 (as amended), the Education and Inspections Act 2006 and the Equality Act 2010. In addition, it reflects the Education Act 2011, which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on pupils' electronic devices where they believe there is a 'good reason' to do so.

This policy complies with our funding agreement and articles of association.

The policy also takes into account the National Curriculum computing programmes of study.

The purpose of Marian Vian's online safety policy is to:

- Safeguard and protect all members of Marian Vian Primary School community online.
- Identify approaches to educate and raise awareness of online safety throughout the community.
- Enable all staff to work safely and responsibly, to role model positive behaviour online and to manage professional standards and practice when using technology.
- Identify clear procedures to use when responding to online safety concerns.

Marian Vian primary school recognises that the issues classified within online safety are considerable, but can be broadly categorised into four areas of risk:

- **Content:** being exposed to illegal, inappropriate or harmful content, such as pornography, fake news, racism, misogyny, self-harm, suicide, antisemitism, radicalisation and extremism
- **Contact:** being subjected to harmful online interaction with other users, such as 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, such as 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

Policy Scope

Marian Vian Primary School believes that:

- online safety is an essential part of safeguarding and acknowledge their duty to ensure that all pupils and staff are protected from potential harm online.
- the internet and associated devices, such as computers, tablets, mobile phones, smart watches and games consoles, are an important part of everyday life.
- pupils should be empowered to build resilience and to develop strategies to manage and respond to risk online.

This policy applies to all staff including the governing body, teachers, support staff, external contractors, visitors, volunteers and other individuals who work for, or provide services on behalf of the school (collectively referred to as 'staff 'in this policy) as well as pupils and parents/carers.

This policy applies to all access to the internet and use of technology, including personal devices, or where pupils, staff or other individuals have been provided with school-issued devices for use off-site, such as work laptops, tablets or mobile phones.

Roles and Responsibilities

The governing board

The governing board has overall responsibility for monitoring this policy and holding the headteacher to account for its implementation. The governing board will make sure all staff undergo online safety training as part of child protection and safeguarding training, and ensure staff understand their expectations, roles and responsibilities around filtering and monitoring. The governing board will also make sure all staff receive regular online safety updates (via email, e-bulletins and staff meetings), as required and at least annually, to ensure they are continually provided with the relevant skills and knowledge to effectively safeguard children. The governing board will co-ordinate regular meetings with appropriate staff to discuss online safety, requirements for training, and monitor online safety logs as provided by the designated safeguarding lead (DSL).

The governing board should ensure children are taught how to keep themselves and others safe, including keeping safe online. The governing board must ensure the school has appropriate filtering and monitoring systems in place on school devices and school networks,

and will regularly review their effectiveness. The board will review the DfE filtering and monitoring standards, and discuss with IT staff and service providers what needs to be done to support the school in meeting the standards, which include:

- Identifying and assigning roles and responsibilities to manage filtering and monitoring systems;
- Reviewing filtering and monitoring provisions at least annually;
- Blocking harmful and inappropriate content without unreasonably impacting teaching and learning;
- Having effective monitoring strategies in place that meet their safeguarding needs.

The governor who oversees online safety is .

All governors will:

- Ensure they have read and understand this policy
- Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet (appendix 3)
- Ensure that online safety is a running and interrelated theme while devising and
- implementing their whole-school or college approach to safeguarding and related policies and/or procedures
- Ensure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and some pupils with special educational needs and/or disabilities (SEND). This is because of the importance of recognising that a 'one size fits all' approach may not be appropriate for all children in all situations, and a more personalised or contextualised approach may often be more suitable. The school has appointed the DSL and Computing Leads to be the online safety leads but recognises that all members of the community have important roles and responsibilities to play with regards to online safety.

The headteacher

The headteacher is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the school.

The leadership and 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 Code of Conduct and/or an Acceptable Use Policy (AUP) that covers acceptable use of technology.
- Ensure that suitable and appropriate filtering and monitoring systems are in place.

- Ensure that online safety is embedded within a progressive whole school curriculum, which enables all pupils to develop an age-appropriate understanding of online safety.

The DSL (and safeguarding team in the DSLs absence) will:

- Supporting the headteacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Work with the headteacher and governing board to review this policy annually and ensure the procedures and implementation are updated and reviewed regularly
  Work with the headteacher, management team, ICT manager and other staff, as necessary, to address any online safety issues or incidents.
- Take the lead on understanding the filtering and monitoring systems and processes in place on school devices and school networks
- Work with the computing lead to make sure the appropriate systems and processes are in place
- Manage all online safety issues and incidents in line with the school's child protection policy
- Ensure that any online safety incidents are logged (see appendix 5) and dealt with appropriately in line with this policy
- Ensure that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school behaviour policy
- Update and deliver staff training on online safety (appendix 4 contains a self-audit for staff on online safety training needs)
- Liaise with other agencies and/or external services if necessary
- Providing regular reports on online safety in school to the headteacher and/or governing board
- Undertake annual risk assessments that consider and reflect the risks children face
- Provide regular safeguarding and child protection updates, including online safety, to all staff, at least annually, in order to continue to provide them with relevant skills and knowledge to safeguard effectively

This list is not intended to be exhaustive.

Details of our DSL and the safeguarding team are on the schools' website and the Child Protection and Safeguarding Policy.

The Computing Lead

It is the responsibility of the Computing Lead to:

- Ensure all staff and volunteers read and understand this policy.

- Have responsibility for the day-to-day running of this policy.
- Train Governors, staff and parents on the potential risks and benefits relating to online safety.
- Oversee the online safety curriculum teaching.
- Be aware that any photos of staff or adults and children on the website and/or social media have a potential AI risk.
- Work with the DSL to ensure that current legislation and guidelines is reflected in daily practice.
- Update the APUs annually and share with pupils, families and staff.

This list is not intended to be exhaustive.

It is the responsibility of all members of staff and volunteers to:

All staff, including contractors and agency staff, and volunteers are responsible for:

- Maintaining an understanding of this policy
- Implementing this policy consistently
- Agreeing and adhering to the terms on acceptable use of the school's systems and the internet (appendix 3), and ensuring that pupils follow the school's terms on acceptable use (appendices 1 and 2)
- Knowing that the DSL and safeguarding team are responsible for the filtering and monitoring systems and processes, and being aware of how to report any incidents of those systems or processes failing by contacting Eduthing
- Following the correct procedures outlined by Eduthing if they need to bypass the filtering and monitoring systems for educational purposes
- Working with the DSL to ensure that any online safety incidents are logged (see appendix 5) and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy
- Responding appropriately to all reports and concerns about sexual violence and/or harassment, both online and offline, and maintaining an attitude of 'it could happen here'.

This list is not intended to be exhaustive.

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

- Provide technical support and perspective to the DSL and leadership team, especially in the development and implementation of appropriate online safety policies and procedures.

- Implement appropriate security measures *(including password policies and encryption)* to ensure that the school's IT infrastructure/system is secure and not open to misuse or malicious attack, whilst allowing learning opportunities to be maximised.
- Ensure that the school filtering and monitoring procedures are applied and updated on a regular basis on school devices and school networks, to assess effectiveness and ensure pupils are kept safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material; responsibility for its implementation is shared with the leadership team.
- Report any filtering breaches to the DSL and leadership team, as well as, the school's Internet Service Provider or other services, as appropriate.
- Ensure that any safeguarding concerns, identified through monitoring or filtering breaches are reported to the DSL, in accordance with the school's safeguarding procedures.
- Put in place an appropriate level of security protection procedures, such as filtering and monitoring systems on school devices and school networks, which are reviewed and updated at least annually to assess effectiveness and ensure pupils are kept safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material
- Ensure that the school's systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
- Conduct a full security check and monitoring the school's systems on a monthly basis
- Block access to potentially dangerous sites and, where possible, prevent the downloading of potentially dangerous files
- Ensure that any online safety incidents are logged (see appendix 5) and dealt with appropriately in line with this policy
- Ensure that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy

This list is not intended to be exhaustive.

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

- Engage in age appropriate online safety education opportunities.
- Read and adhere to the school AUPs.
- 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.

It is the responsibility of parents and carers to:

- Ensure their child has read, understood, agreed and adhere to the terms on acceptable use of the school's IT systems and internet (appendices 1 and 2)
- Support the school in their online safety approaches by discussing online safety issues with their children and reinforce appropriate, safe online behaviours at home.
- Role model safe and appropriate use of technology and social media.
- Notify a member of staff or the headteacher of any concerns or queries regarding this policy
- Abide by the schools' home-school agreement and/or AUPs. Identify changes in behaviour that could indicate that their child is at risk of harm online.
- Seek help and support from the school, or other appropriate agencies, if they or their child encounter risk or concerns online.
- Use school systems, such as learning platforms, and other network resources, safely and appropriately.
- Take responsibility for their own awareness in relation to the risks and opportunities posed by new and emerging technologies.

Parents/carers can seek further guidance on keeping children safe online from the following organisations and websites:

- What are the issues? – UK Safer Internet Centre
- Hot topics – Childnet
- Parent resource sheet – Childnet

Visitors and members of the community

Visitors and members of the community who use the school's IT systems or internet will be made aware of this policy, when relevant, and expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use (appendix 3).

Education and Engagement Approaches

Education and engagement with pupils

The school will establish and embed a progressive online safety curriculum throughout the whole school, to raise awareness and promote safe and responsible internet use amongst pupils by:

- Ensuring education regarding safe and responsible use precedes internet access.
- Including online safety in the PSHE, SRE and Computing programmes of study, covering use both at home school and home.
- Reinforcing online safety messages whenever technology or the internet is in use.

- Educating pupils in the effective use of the internet to research; including the skills of knowledge location, retrieval and evaluation.
- Teaching pupils to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.

The school will support pupils to read and understand the AUP in a way which suits their age and ability by:

- Informing pupils that network and internet use will be monitored for safety and security purposes and in accordance with legislation.
- Using support, such as external visitors, where appropriate, to complement and support the schools' internal online safety education approaches.

Pupils will be taught to:

- Use technology safely and respectfully, keeping personal information private
- Identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies
- Use technology safely, respectfully and responsibly
- Recognise acceptable and unacceptable behaviour
- Identify a range of ways to report concerns about content and contact

By the end of primary school, pupils will know:

- That people sometimes behave differently online, including by pretending to be someone they are not
- That the same principles apply to online relationships as to face-to-face relationships, including the importance of respect for others online, including when we are anonymous
- The rules and principles for keeping safe online, how to recognise risks, harmful content and contact, and how to report them
- How to critically consider their online friendships and sources of information including awareness of the risks associated with people they have never met
- How information and data is shared and used online
- What sorts of boundaries are appropriate in friendships with peers and others (including in a digital context)
- How to respond safely and appropriately to adults they may encounter (in all contexts, including online) whom they do not know.

The safe use of social media and the internet will also be covered in other subjects where relevant.

Where necessary, teaching about safeguarding, including online safety, will be adapted for vulnerable children, victims of abuse and some pupils with SEND.

Training and engagement with staff

The school will:

- Provide all new staff members of staff with training, as part of their induction, on safe internet use and online safeguarding issues, including cyber-bullying and the risks of online radicalisation.
- All staff members will receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates as required (for example through emails, e-bulletins and staff meetings). This will cover the potential risks posed to pupils (Content, Contact, Conduct and Commerce) as well as our professional practice expectations.
- Make staff aware that school systems are monitored and activity can be traced to individual users; staff will be reminded to behave professionally and in accordance with school's policies when accessing school systems and devices.
- Make staff aware that their online conduct out of school, including personal use of social media, could have an impact on their professional role and reputation within school.
- Highlight useful educational resources and tools which staff should use, according to the age and ability of the pupils.
- Ensure all members of staff are aware of the procedures to follow regarding online safety concerns affecting pupils, colleagues or other members of the school community.

By way of this training, all staff will be made aware that:

Technology is a significant component in many safeguarding and wellbeing issues, and that children are at risk of online abuse Cyber-bullying.

Awareness and engagement with parents and carers

Marian Vian Primary School recognises that parents and carers have an essential role to play in enabling children to become safe and responsible users of the internet and associated technologies.

The school will build a partnership approach to online safety with parents and carers by:

- Providing information and guidance on online safety in a variety of formats. This will include offering specific online safety awareness training and highlighting online safety at other events such as parent evenings and transition events.
- Drawing their attention to the school online safety policy and expectations in newsletters, letters, our prospectus and on our website.

- Requesting that they read online safety information as part of joining our school, for example, within our home school agreement.
- Requiring them to read the school AUP and discuss its implications with their children.
- Be aware of what systems the school uses to filter and monitor online use.
- Be aware of what their children are being asked to do online, including the sites they will be asked to access and who from the school (if anyone) their child will be interacting with online.

If parents/carers have any queries or concerns in relation to online safety, these should be raised in the first instance with the headteacher and/or the DSL.

Reducing Online Risks

We recognise that the internet is a constantly changing environment with new apps, devices, websites and material emerging at a rapid pace therefore we will:

- Regularly review the methods used to identify, assess and minimise online risks.
- Examine emerging technologies for educational benefit and undertake appropriate risk assessments before use in school is permitted.
- Ensure that appropriate filtering and monitoring is in place and take all reasonable precautions to ensure that users can only access appropriate material.
- Due to the global and connected nature of the internet, it is not possible to guarantee that unsuitable material cannot be accessed via a school computer or device.
- All members of the school community are made aware of the school's expectations regarding safe and appropriate behaviour online and the importance of not posting any content, comments, images or videos which could cause harm, distress or offence to members of the community.
- Staff will undertake RPA Cyber Training annually.
- Our website has a direct link to Child Exploitation and Online Protection where concerns about online sexual abuse or the way someone has been communicating with you online can be instantly reported.
- Be aware of the use of AI and challenges in this area.

Safer Use of Technology

Classroom Use

- Marian Vian 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
    - School learning platform
    - Email
    - Digital cameras, web cams and video cameras
- All school owned devices will be used in accordance with the school's AUP and with appropriate safety and security measures in place.
- Members of staff will always evaluate websites, tools and apps fully before use in the classroom or recommending for use at home.
- Children will engage in research and will use age appropriate search tools

Filtering and Monitoring

Decision Making

- Marian Vian Primary School has ensured that the school has age and ability appropriate filtering and monitoring in place, to limit children's exposure to online risks.
- The governors and leaders are aware of the need to prevent "over blocking", as that may unreasonably restrict what children can be taught, with regards to online activities and safeguarding.
- The school's decisions regarding filtering and monitoring have been informed by a risk assessment, taking into account our school's specific needs and circumstances.
- All members of staff are aware that they cannot rely on filtering and monitoring alone to safeguard pupils; effective classroom management and regular education about safe and responsible use is essential.

Filtering

- The school uses London Grid for Learning (LGFL), which blocks sites which can be categorised as: pornography, racial hatred, extremism, gaming and sites of an illegal nature. A weekly report is sent to the Headteacher and DSL.

Dealing with Filtering Breaches

The school has a clear procedure for reporting filtering breaches.

- If pupils discover unsuitable sites, they will be required 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 and technical staff.
- The breach will be recorded and escalated as appropriate.
- Parents/carers will be informed of filtering breaches involving their child.
- Any material that the school believes is illegal will be reported immediately to the appropriate agencies, such as: CEOP, Report Harmful Content, Internet Watch Foundation.

Monitoring

The school will appropriately monitor internet use on all school owned or provided internet enabled devices. All users will be informed that use of school systems can be monitored and that all monitoring will be in line with data protection, human rights and privacy legislation, in line with KCSIE, 2025.

Security and Management of Information Systems

The school takes appropriate steps to ensure the security of our information systems, including:

- Virus protection being updated regularly.
- Not using portable media without specific permission; portable media will be checked by an anti-virus /malware scan before use. Staff and children are not allowed to bring work into school on USBs, instead email to the class email account.
- Not downloading unapproved software to work devices or opening unfamiliar email attachments.
- The appropriate use of user logins and passwords to access the school network.
- All users are expected to log off or lock their screens/devices if systems are unattended.
- Staff will undertake RPA Cyber Training annually.

Managing the Safety of the School Website

- The school will ensure that information posted on our website meets the requirements as identified by the Department for Education (DfE)
- The school will ensure that our website complies with guidelines for publications including: accessibility; data protection; respect for intellectual property rights; privacy policies and copyright.
- Staff or pupils' personal information will not be published on our website; the contact details on the website will be the school address, email and telephone number.
- The administrator account for the school website will be secured with an appropriately strong password.
- The school will post appropriate information about safeguarding, including online safety, on the school website for members of the community.

Managing Email

- Access to school email systems will always take place in accordance with Data protection legislation and in line with other school policies
- The forwarding of any chain messages/emails is not permitted. Spam or junk mail will be blocked and reported to the email provider.
- School email addresses and other official contact details will not be used for setting up personal social media accounts.
- Members of the school community will immediately tell the Head Teacher if they receive offensive communication, and this will be recorded in the school safeguarding files/records.

Staff

The use of personal email addresses by staff for any official school business is not permitted. All members of staff are provided with a specific school email address, to use for all official communication.

Pupils

- Classes will sign up to an AUP annually and will receive education regarding safe and appropriate email etiquette before access is permitted.

Management of Remote Learning Environment

- Leaders and staff will regularly monitor the usage of the Seesaw in all areas, in particular, message and communication tools and publishing facilities.
- Only current members of staff, pupils and parents will have access to the Seesaw.
- When staff and/or pupils' leave the school, their account or rights to specific school areas will be disabled.
- Pupils and staff will be advised about acceptable conduct and use when using the RLE
- All users will be mindful of copyright and will only upload appropriate content onto the Seesaw.

Any concerns about content on Seesaw will be recorded and dealt with in the following ways:

- The user will be asked to remove any material deemed to be inappropriate or offensive.
- If the user does not comply, the material will be removed by the site administrator.
- Access to Seesaw for the user may be suspended.
- The user will need to discuss the issues with a member of leadership before reinstatement. A pupil's parent/carer may be informed.

- If the content is considered to be illegal, then the school will respond in line with existing child protection procedures.

Staff using work devices outside school

All staff members will take appropriate steps to ensure their devices remain secure. This includes, but is not limited to:

- Keeping the device password-protected – strong passwords are at least 8 characters, with a combination of upper and lower-case letters, numbers and special characters (e.g. asterisk or currency symbol)
- Ensuring their hard drive is encrypted – this means if the device is lost or stolen, no one can access the files stored on the hard drive by attaching it to a new device
- Making sure the device locks if left inactive for a period of time
- Not sharing the device among family or friends
- Installing anti-virus and anti-spyware software
- Keeping operating systems up to date by always installing the latest updates

Staff members must not use the device in any way that would violate the school's terms of acceptable use.

Work devices must be used solely for work activities.

If staff have any concerns over the security of their device, they must seek advice from Eduthing.

Social Media

Expectations

- The expectations regarding safe and responsible use of social media apply to all members of the school community.
- The term social media may include (but is not limited to): blogs; wikis; social networking sites; forums; bulletin boards; online gaming; apps; video/photo sharing sites; chatrooms and instant messenger.
- All members of Marian Vian Primary School are expected to engage in social media in a positive, safe and responsible manner, at all times.
- All members of Marian Vian Primary School are advised not to publish specific and detailed private thoughts, concerns, pictures or messages on any social media services, especially content that may be considered threatening, hurtful or defamatory to others.
- The school will control pupil and staff access to social media whilst using school provided devices and systems on site.

- Concerns regarding the online conduct of any member of staff on social media, should be reported to the school and will be managed in accordance with our Anti-bullying, Allegations against staff, Behaviour and Child Protection policies.
- Whilst we acknowledge that parents will use social media, and that they may choose, for example, to set up class or year group WhatsApp groups, these are not endorsed by the schools, and they should not be used as a forum for unsubstantiated or malicious content.

Staff Personal Use of Social Media

- The safe and responsible use of social networking, social media and personal publishing sites will be discussed with all members of staff as part of staff induction and will be revisited and communicated via regular staff training opportunities.
- Safe and professional behaviour will be outlined for all members of staff (including volunteers) as part of the school code of conduct.
- No member of staff should engage with children or parents through social media. Where staff members are also parents, they have a responsibility to be professional at all times in their communication with parents via group or individual messaging.

Reputation

- All members of staff are advised that their online conduct on social media can have an impact on their role and reputation within school. Civil, legal or disciplinary action may be taken if they are found to bring the profession or institution into disrepute, or if something is felt to have undermined confidence in their professional abilities.
- All members of staff are advised to safeguard themselves and their privacy when using social media sites. Advice will be provided to staff via staff training and by sharing appropriate guidance and resources on a regular basis. This will include (but is not limited to):
    - Setting the privacy levels of their personal sites as strictly as they can.
    - Being aware of location sharing services.
    - Opting out of public listings on social networking sites.
    - Logging out of accounts after use.
    - Keeping passwords safe and confidential.
    - Ensuring staff do not represent their personal views as that of the school.
- Members of staff are encouraged not to identify themselves as employees of either Marian Vian Primary School on their personal social networking accounts. This is to prevent information on these sites from being linked with the school and also to safeguard the privacy of staff members.
- All members of staff are encouraged to carefully consider the information, including text and images, they share and post online and to ensure that their social media use

is compatible with their professional role and is in accordance with school's policies and the wider professional and legal framework.

- Information and content that staff members have access to as part of their employment, including photos and personal information about pupils and their family members or colleagues will not be shared or discussed on social media sites.
- Members of staff will notify the Head Teacher immediately if they consider that any content shared on social media sites conflicts with their role in the school.

Communicating with pupils and parents and carers

- All members of staff are advised not to communicate with or add as 'friends' any current or past pupils or current or past pupils' family members via any personal social media sites, applications or profiles.
- Staff will not use personal social media accounts to make contact with pupils or parents, nor should any contact be accepted
- Any communication from pupils and parents received on personal social media accounts will be reported to the Head Teacher.

Pupils' Personal Use of Social Media

- Safe and appropriate use of social media will be taught to pupils as part of an embedded and progressive education approach, via age appropriate sites and resources.
- The school is aware that many popular social media sites state that they are not for children under the age of 13, therefore the school will not create accounts for any child on a social media site that is not age appropriate. We will also recommend to parents that they do not allow their children to access sites which are not age-appropriate.
- Any concerns regarding pupils' use of social media, both at home and at school, will be dealt with in accordance with existing school policies including anti-bullying and behaviour. Concerns will also be raised with parents/carers as appropriate, particularly when concerning underage use of social media sites or tools.

Pupils will be advised:

- To consider the benefits and risks of sharing personal details on social media sites which could identify them and/or their location. Examples would include real/full name, address, mobile or landline phone numbers, school attended, other social media contact details, email addresses, full names of friends/family, specific interests and clubs.
- To only approve and invite known friends on social media sites and to deny access to others by making profiles private/protected.

- Not to meet any online friends without a parent/carer or other responsible adult's permission and only when a trusted adult is present.
- To use safe passwords.
- To use social media sites which are appropriate for their age and abilities.
- How to block and report unwanted communications and report concerns both within school and externally.

Official Use of Social Media

- The official use of social media sites, by the school, only takes place with clear educational or community engagement objectives, with specific intended outcomes.
- Official school social media channels have been set up as distinct and dedicated social media sites or accounts for educational or engagement purposes only.
- Staff use school provided email addresses to register for and manage any official school social media channels.
- Official social media sites are suitably protected.
- Official social media use will be conducted in line with existing policies, including: Anti-bullying, Image use, Data protection, Confidentiality and Child protection.
- All communication on official social media platforms will be clear, transparent and open to scrutiny.
- Parents, carers and pupils will have given consent of any official social media use, along with expectations for safe use and action taken to safeguard the community.
- Parents and carers will have given consent of any official social media use with pupils as required.

Staff expectations

- Members of staff who follow and/or like the school social media channels will be advised to use dedicated professionals accounts, where possible, to avoid blurring professional boundaries.
- If members of staff are participating in online social media activity as part of their capacity as an employee of the school, they will:
    - Be professional at all times and aware that they are an ambassador for the school.
    - Disclose their official role and/or position, but make it clear that they do not necessarily speak on behalf of the school.
    - Be responsible, credible, fair and honest at all times and consider how the information being published could be perceived or shared.
    - Always act within the legal frameworks they would adhere to within the workplace, including: Libel, Defamation, Confidentiality, Copyright, Data protection and Equalities laws.
    - Ensure that they have appropriate written consent before posting images on the official social media channel.

- Not disclose information, make commitments or engage in activities on behalf of the school unless they are authorised to do so.
- Not engage with any direct or private messaging with current, or past, pupils, parents and carers.
- Inform the Head Teacher of any concerns, such as criticism, inappropriate content or contact from pupils.

Use of Personal Devices and Mobile Phones

Whilst the schools recognise that personal communication through mobile technologies is an accepted part of everyday life for pupils, staff and parents/carers, technologies do need to be used safely and appropriately within school.

Examining electronic devices

The headteacher, and any member of staff authorised to do so by the headteacher (usually a member of the SLT), can carry out a search and confiscate any electronic device that they have reasonable grounds for suspecting:

- Poses a risk to staff or pupils, and/or
- Is identified in the school rules as a banned item for which a search can be carried out, and/or
- Is evidence in relation to an offence

Before a search, if the authorised staff member is satisfied that they have reasonable grounds for suspecting any of the above, they will also:

- Make an assessment of how urgent the search is, and consider the risk to other pupils and staff. If the search is not urgent, they will seek advice from the headteacher or DSL.
- Explain to the pupil why they are being searched, how the search will happen, and give them the opportunity to ask questions about it
- Seek the pupil's co-operation

Authorised staff members may examine, and in exceptional circumstances erase, any data or files on an electronic device that they have confiscated where they believe there is a 'good reason' to do so.

When deciding whether there is a 'good reason' to examine data or files on an electronic device, the staff member should reasonably suspect that the device has, or could be used to:

- Cause harm, and/or
- Undermine the safe environment of the school or disrupt teaching, and/or
- Commit an offence

If inappropriate material is found on the device, it is up to the safeguarding team to decide on a suitable response. If there are images, data or files on the device that staff reasonably

suspect are likely to put a person at risk, they will first consider the appropriate safeguarding response.

When deciding if there is a good reason to erase data or files from a device, staff members will consider if the material may constitute evidence relating to a suspected offence. In these instances, they will not delete the material, and the device will be handed to the police as soon as reasonably practicable. If the material is not suspected to be evidence in relation to an offence, staff members may delete it if:

- They reasonably suspect that its continued existence is likely to cause harm to any person, and/or
- The pupil and/or the parent/carer refuses to delete the material themselves
- If a staff member **suspects** a device **may** contain an indecent image of a child (also known as a nude or semi-nude image), they will:
- **Not** view the image
- Confiscate the device and report the incident to the DSL (or equivalent) immediately, who will decide what to do next. The DSL will make the decision in line with the DfE's latest guidance on screening, searching and confiscation and the UK Council for Internet Safety (UKCIS) guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people
- Any searching of pupils will be carried out in line with:
- The DfE's latest guidance on searching, screening and confiscation
- UKCIS guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people
- Our Child Protection and Safeguarding policy

Any complaints about searching for or deleting inappropriate images or files on pupils' electronic devices will be dealt with through the school complaints procedure.

Expectations of mobile device use:

- All use of personal devices and mobile phones will take place in accordance with the law and other appropriate school policies, including, but not limited to: Anti-bullying, Behaviour and Child Protection.
- Electronic devices of any kind that are brought onto site are the responsibility of the user at all times.
- All members of staff are advised to take steps to protect their mobile phones or devices from loss, theft or damage; the school accepts no responsibility for the loss, theft or damage of such items on school premises.
- All members of staff are advised to use passwords/pin numbers to ensure that unauthorised calls or actions cannot be made on their phones or devices; passwords

and pin numbers should be kept confidential and mobile phones and personal devices should not be shared.

- The sending of abusive or inappropriate messages/ content via mobile phones or personal devices is forbidden by any member of the community; any breaches will be dealt with as part of our Behaviour policy.
- All members of staff are advised to ensure that their mobile phones and personal devices do not contain any content which may be considered to be offensive, derogatory or would otherwise contravene the school Behaviour or Child Protection policies.

Staff Use of Personal Devices and Mobile Phones

- Members of staff will ensure that use of personal phones and devices takes place in accordance with the law, as well as, relevant school policy and procedures, such as: Confidentiality, Child Protection, Data Protection and Acceptable use.
- Staff will be advised to:
  - Keep mobile phones and personal devices in a safe and secure place during lesson time
  - Keep mobile phones and personal devices switched off or switched to 'silent' mode during lesson times.
  - Not use personal devices during teaching periods, unless permission has been given by the Head Teacher, such as in emergency circumstances.
  - Ensure that any content bought onto site via mobile phones and personal devices are compatible with their professional role and expectations.
  - Members of staff are not permitted to use their own personal phones or devices for contacting pupils or parents and carers.
  - Staff will not use personal devices, such as: mobile phones, tablets or cameras: to take photos or videos of pupils and will only use work-provided equipment for this purpose.
  - Talk directly with pupils, and will only use work-provided equipment during lessons/educational activities.
  - If a member of staff breaches the school policy, action will be taken in line with the school behaviour and allegations policy
  - If a member of staff is thought to have illegal content saved or stored on a mobile phone or personal device or have committed a criminal offence, the police will be contacted.

Pupils' Use of Personal Devices and Mobile Phones

- Pupils will be educated regarding the safe and appropriate use of personal devices and mobile phones and will be made aware of boundaries and consequences.
- Children should not bring mobile phones into school, unless they are in Years 6 at the, and have completed the safety workshop and agreed to the usage rules.
- Pupil's mobile phones must be turned off when on any part of the school grounds.
- Y6 pupil's mobile phones must be handed into the class teacher at registration, who will lock the phones away until the end of the day.
- If a pupil breaches the school policy, the phone or device will be confiscated and will be held in a secure place.
- School staff may confiscate a pupil's mobile phone or device if they believe it is being used to contravene the school's Behaviour or Bullying policy, or could contain youth produced sexual imagery (sexting).
- Pupils' mobile phones or devices may be searched by a member of Leadership Team with the consent of the pupil or a parent/ carer.
- Mobile phones and devices that have been confiscated will be released to parents or carers over the age of 18.
- If there is suspicion that material on a pupil's personal device or mobile phone may be illegal or may provide evidence relating to a criminal offence, the device will be handed over to the police for further investigation.

Any use of mobile devices in school by pupils must be in line with the acceptable use agreement (see appendices 1 and 2).
Any breach of the acceptable use agreement by a pupil may trigger disciplinary action in line with the school behaviour policy, which may result in the confiscation of their device

Visitors' Use of Personal Devices and Mobile Phones

- Parents, carers and visitors (including volunteers and contractors) must use their mobile phones and personal devices in accordance with the school's Acceptable Use Policy and other associated policies, such as: Anti-bullying, Behaviour and Child Protection.
- Members of staff are expected to challenge visitors if they have concerns and will always inform the Head Teacher of any breaches of school policy.

Responding to Online Safety Incidents and Concerns

- All members of the school community will be made aware of the reporting procedure for online safety concerns, including: breaches of filtering, youth produced sexual imagery (sexting), up-skirting, cyberbullying and illegal content.
- All members of the community must respect confidentiality and the need to follow the official school procedures for reporting concerns.

- Pupils, parents and staff will be informed of the school's complaints procedure and staff will be made aware of the whistleblowing procedure.
- The school requires staff, parents, carers and pupils to work in partnership to resolve online safety issues.
- After any investigations are completed, the school will debrief, identify lessons learnt and implement any policy or curriculum changes as required.
- If the school is unsure how to proceed with an incident or concern, the leadership team will seek advice from the Bromley Safeguarding Team.
- Where there is suspicion that illegal activity has taken place, the school will contact the Bromley's Safeguarding Team or Police using 101, or 999 if there is immediate danger or risk of harm.
- If an incident or concern needs to be passed beyond the school community (for example if other local schools are involved or the public may be at risk), the school will speak with the Police and/or Bromley's Safeguarding Team first, to ensure that potential investigations are not compromised.

Concerns about Pupils Welfare

- The DSL will be informed of any online safety incidents involving safeguarding or child protection concerns
- The DSL will ensure that online safety concerns are escalated and reported to relevant agencies in line with the Bromley's Safeguarding Children's Board thresholds and procedures.
- The school will inform parents and carers of any incidents or concerns involving their child, as and when required.

Staff Misuse

- Any complaint about staff misuse will be referred to the Head Teacher
- Any allegations regarding a member of staff's online conduct will be discussed with the LADO (Local Authority Designated Officer).
- Appropriate action will be taken in accordance with the Behaviour policy and Code of conduct.

Procedures for Responding to Specific Online Incidents or Concerns

Youth Produced Sexual Imagery or "Sexting"

- Marian Vian Primary School recognises youth produced sexual imagery (known as "sexting") as a safeguarding issue; therefore, all concerns will be reported to and dealt with by Designated Safeguarding Leads.

Dealing with 'Sexting'

If the school are made aware of an incident involving the creation or distribution of youth produced sexual imagery, the school will:

- Act in accordance with our Child Protection and Safeguarding policies and the relevant Safeguarding Child Board's procedures.
- Immediately notify the Inclusion Manager
- Store the device securely.
- If an indecent image has been taken or shared on the school network or devices, the school will take action to block access to all users and isolate the image.
- Carry out a risk assessment which considers any vulnerability of pupil(s) involved; including carrying out relevant checks with other agencies.
- Inform parents and carers, if appropriate, about the incident and how it is being managed.
- Make a referral to Bromley Children's Services and/or the Police, as appropriate.
- Provide the necessary safeguards and support for pupils.
- Implement appropriate sanctions in accordance with the school's Behaviour policy, but taking care not to further traumatise victims where possible.
- The school will take action regarding youth produced sexual imagery, regardless of whether the incident took place on/off school premises, using school or personal equipment.

The school will not:

- View any images suspected of being youth produced sexual imagery, unless there is no other possible option, or there is a clear need or reason to do so.
- In this case, the image will only be viewed by the Inclusions Manager or Head Teacher and their justification for viewing the image will be clearly documented.
- Send, share, save or make copies of content suspected to be an indecent image of children (i.e. youth produced sexual imagery) and will not allow or request pupils to do so.

Online Child Sexual Abuse and Exploitation

- The school will implement preventative approaches for online child sexual abuse via a range of age and ability appropriate education for pupils, staff and parents/carers.
- The school will ensure that the 'Click CEOP' report button is visible on the web sites, and available to pupils and other members of the school community

Dealing with Online Child Sexual Abuse and Exploitation

If the school are made aware of an incident involving online sexual abuse of a child, the school will:

- Act in accordance with the school's Child Protection and Safeguarding policies and the relevant Safeguarding Child Board's procedures.
- Immediately notify the Designated Safeguarding Leads.
- Store any devices involved securely.
- Immediately inform the police via 101 (or 999 if a child is at immediate risk).
- Carry out a risk assessment which considers any vulnerabilities of pupil(s) involved (including carrying out relevant checks with other agencies).
- Inform parents/carers about the incident and how it is being managed.
- Make a referral to Bromley Children's Services (if required/ appropriate).
- Provide the necessary safeguards and support for pupils, such as, offering pastoral support.

Cyberbullying

Cyberbullying, along with all other forms of bullying, will not be tolerated and will be dealt with in line with the schools' Anti-bullying and Behaviour Policy and Safeguarding Policy.

Marian Vian Primary School uses this definition of Cyber-bullying:

Cyberbullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of 1 person or group by another person or group, where the relationship involves an imbalance of power. (See also Child Protection and Safeguarding and Behaviour policies.)

To help prevent cyber-bullying, we will ensure that pupils understand what it is and what to do if they become aware of it happening to them or others. We will ensure that pupils know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.

Teachers, staff and Digital Leaders will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be.
Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes personal, social, health and economic (PSHE) education, and other subjects where appropriate.
All staff, governors and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training.
The school also publishes information/leaflets on cyber-bullying to parents/carers so they are aware of the signs, how to report it and how they can support children who may be affected.
In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the school behaviour policy. Where illegal, inappropriate or harmful material has been

spread among pupils, the school will use all reasonable endeavours to ensure the incident is contained.

The DSL will report the incident and provide the relevant material to the police as soon as is reasonably practicable, if they have reasonable grounds to suspect that possessing that material is illegal. They will also work with external services if it is deemed necessary to do so.

Generative artificial intelligence (AI)

AI tools are now widespread and easy to access. Staff, pupils and parents/carers may be familiar with generative chatbots such as ChatGPT and Google Bard.

Marian Vian Primary School recognise that AI has many uses to help pupils learn, but may also have the potential to be used to bully others. For example, in the form of 'deepfakes', where AI is used to create images, audio or video hoaxes that look real. This includes deepfake pornography: pornographic content created using AI to include someone's likeness.

Marian Vian Primary School will treat any use of AI to bully pupils in line with our Child Protection and Safeguarding Policy and Behaviour Policy

.

Staff should be aware of the risks of using AI tools whilst they are still being developed and should carry out a risk assessment where new AI tools are being used by the school/trust.

Online Radicalisation and Extremism

- The school will take all reasonable precautions to ensure that children are safe from terrorist and extremist material when accessing the internet in school.
- If the school is concerned that a child or parent/carer may be at risk of radicalisation online, the Inclusions Manager will be informed immediately and action will be taken in line with the Child Protection Policy.
- If the school is concerned that member of staff may be at risk of radicalisation online, the Head Teacher will be informed immediately and action will be taken in line with the Child protection and Allegations policies.

Misuse of Technology

Where a pupil misuses the school's IT systems or internet, we will follow the procedures set out in our policies on behaviour and IT and internet acceptable use. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.

Where a staff member misuses the school's IT systems or the internet, or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the staff disciplinary procedures / staff code of conduct. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

The school will consider whether incidents that involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

- Children can abuse their peers online through:
    - Abusive, threatening, harassing and misogynistic messages
    - Non-consensual sharing of indecent nude and semi-nude images and/or videos, especially around chat groups
    - Sharing of abusive images and pornography, to those who don't want to receive such content
- Physical abuse, sexual violence and initiation/hazing type violence can all contain an online element

Training will also help staff:

- Develop better awareness to assist in spotting the signs and symptoms of online abuse
- Develop the ability to ensure pupils can recognise dangers and risks in online activity and can weigh up the risks
- Develop the ability to influence pupils to make the healthiest long-term choices and keep them safe from harm in the short term

The DSL / Safeguarding Team will undertake child protection and safeguarding training, which will include online safety, at least every 2 years. They will also update their knowledge and skills on the subject of online safety at regular intervals, and at least annually.

Governors will receive training on safe internet use and online safeguarding issues as part of their safeguarding training.

Volunteers will receive appropriate training and updates, if applicable.

More information about safeguarding training is set out in our child protection and safeguarding policy.

Links with other policies and practices

This policy links with a number of other policies, practices and action plans including:

- Anti-bullying policy
- Acceptable Use Policies (AUP) and/or the Code of conduct
- Behaviour and discipline policy
- Child protection policy
- Confidentiality policy
- Curriculum policies, such as: Computing, Personal Social and Health Education (PSHE), Citizenship and Sex and Relationships Education (SRE)
- Data Protection

- Child Protection and Safeguarding Policy
- Staff Code of Conduct
- Whistleblowing Policy

Monitoring and Review

- This policy will be reviewed at least annually
- We will ensure that we regularly monitor internet use and evaluate online safety mechanisms to ensure that this policy is consistently applied.
- To ensure they have oversight of online safety, the Head Teacher will be informed of online safety concerns, as appropriate.

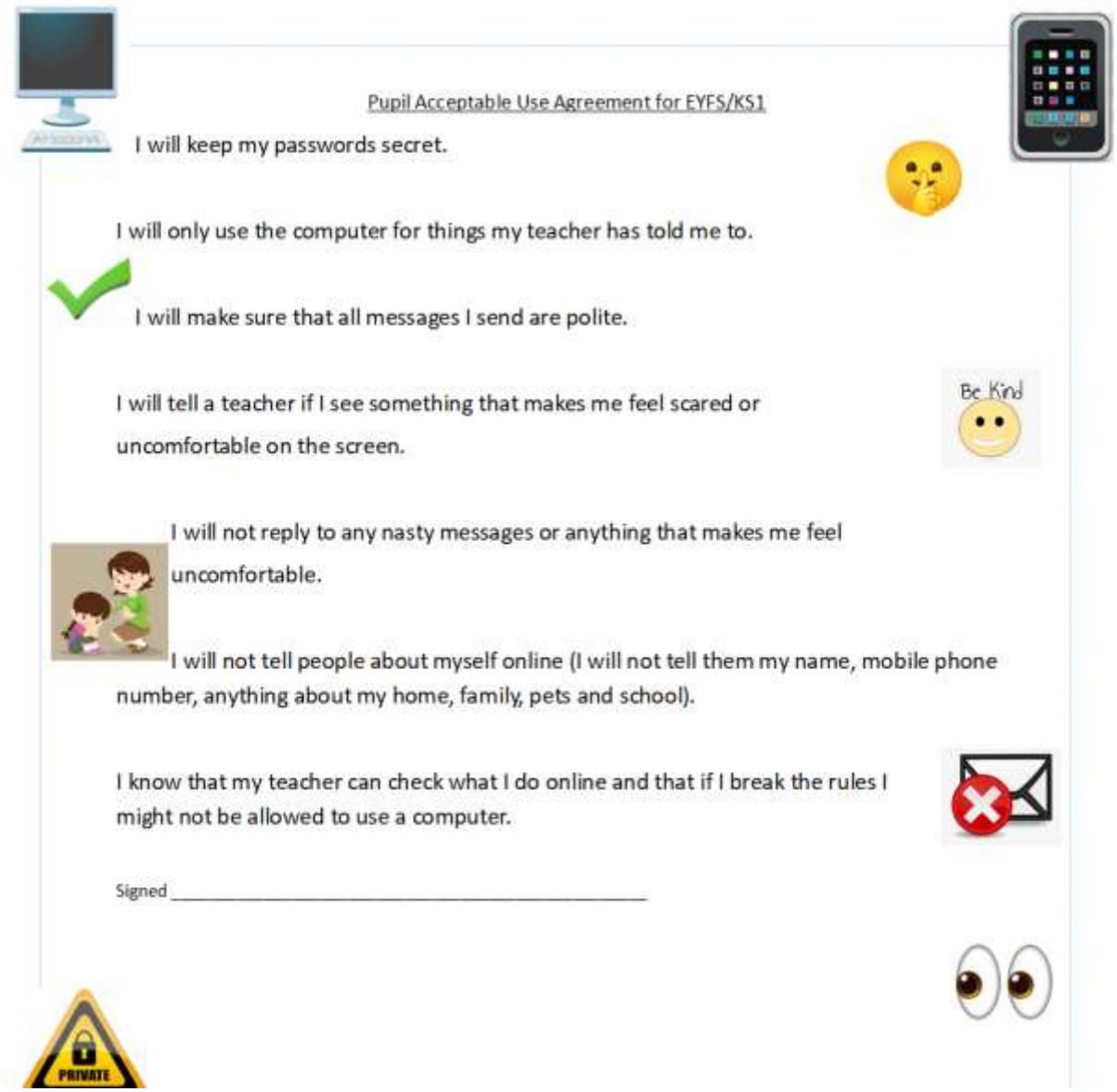
Useful Links for Educational Settings

National Links and Resources

- Action Fraud: www.actionfraud.police.uk
- CEOP:
  - www.thinkuknow.co.uk
  - www.ceop.police.uk
- Childnet: www.childnet.com
- Get Safe Online: www.getsafeonline.org
- Internet Matters: www.internetmatters.org
- Internet Watch Foundation (IWF): www.iwf.org.uk
- Lucy Faithfull Foundation: www.lucyfaithfull.org
- NSPCC: www.nspcc.org.uk/onlinesafety
  - ChildLine: www.childline.org.uk
  - Net Aware: www.net-aware.org.uk
- The Marie Collins Foundation: www.mariecollinsfoundation.org.uk
- UK Safer Internet Centre: www.saferinternet.org.uk
  - Professional Online Safety Helpline: www.saferinternet.org.uk/about/helpline
  - Turn IT On filtering information: https://www.lgfl.net/services/webscreen

Appendix 1

Marian Vian Primary School AUP (To be discussed as a class rather than individual signing)



Pupil Acceptable Use Agreement for EYFS/KS1

I will keep my passwords secret.

I will only use the computer for things my teacher has told me to.

I will make sure that all messages I send are polite.

I will tell a teacher if I see something that makes me feel scared or uncomfortable on the screen.

I will not reply to any nasty messages or anything that makes me feel uncomfortable.

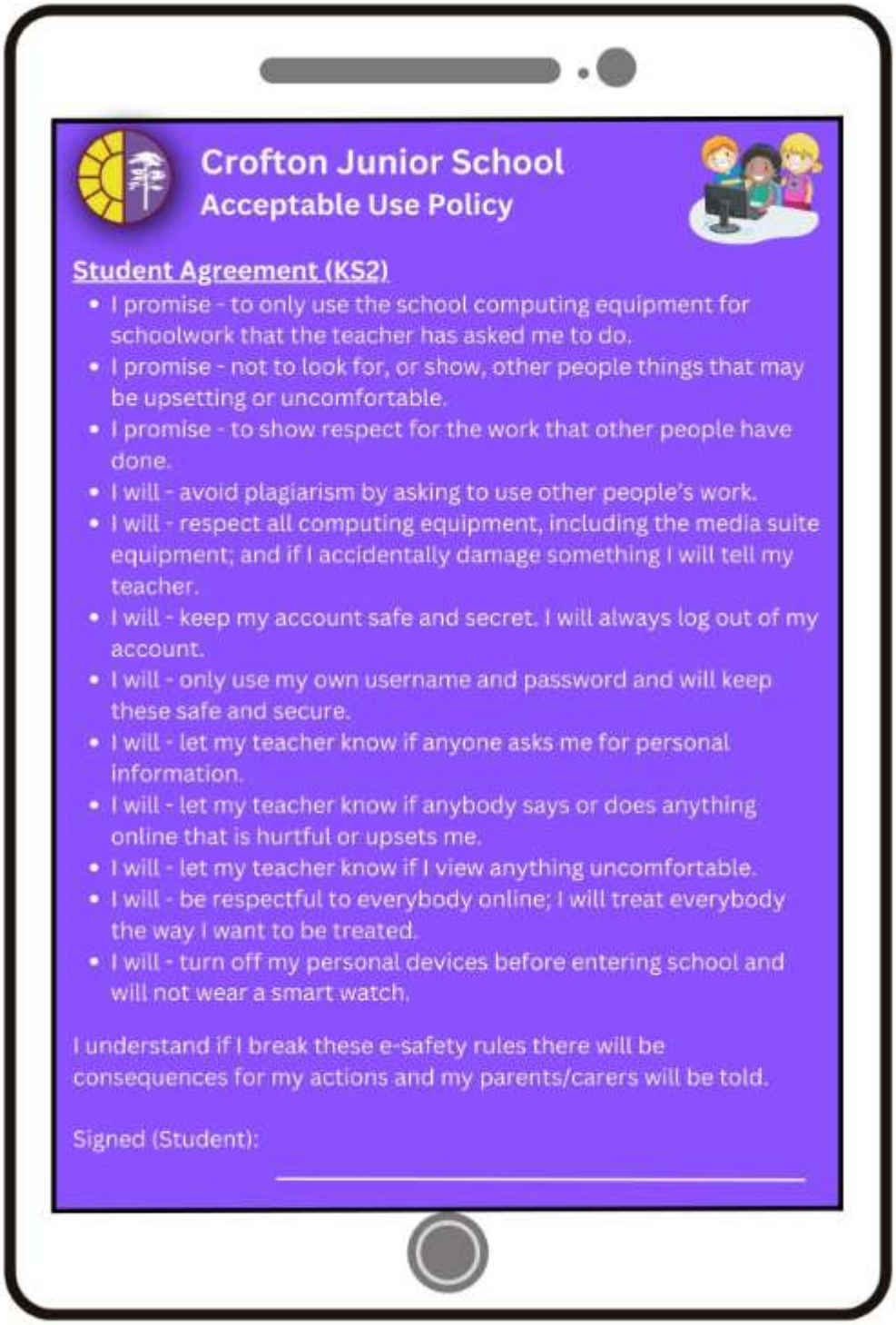
I will not tell people about myself online (I will not tell them my name, mobile phone number, anything about my home, family, pets and school).

I know that my teacher can check what I do online and that if I break the rules I might not be allowed to use a computer.

Signed _____

Appendix 2

Marian Vian Primary School AUP (Taken from Crofton Junior School) to be discussed and signed up to as a class.



Crofton Junior School
Acceptable Use Policy

Student Agreement (KS2)

- I promise - to only use the school computing equipment for schoolwork that the teacher has asked me to do.
- I promise - not to look for, or show, other people things that may be upsetting or uncomfortable.
- I promise - to show respect for the work that other people have done.
- I will - avoid plagiarism by asking to use other people's work.
- I will - respect all computing equipment, including the media suite equipment; and if I accidentally damage something I will tell my teacher.
- I will - keep my account safe and secret. I will always log out of my account.
- I will - only use my own username and password and will keep these safe and secure.
- I will - let my teacher know if anyone asks me for personal information.
- I will - let my teacher know if anybody says or does anything online that is hurtful or upsets me.
- I will - let my teacher know if I view anything uncomfortable.
- I will - be respectful to everybody online; I will treat everybody the way I want to be treated.
- I will - turn off my personal devices before entering school and will not wear a smart watch.

I understand if I break these e-safety rules there will be consequences for my actions and my parents/carers will be told.

Signed (Student): _____

Appendix 3: acceptable use agreement (staff, governors, volunteers and visitors)

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR STAFF, GOVERNORS, VOLUNTEERS AND VISITORS
Name of staff member/governor/volunteer/visitor:
When using the school's IT systems and accessing the internet in school, or outside school on a work device (if applicable), I will not: • Access, or attempt to access inappropriate material, including but not limited to material of a violent, criminal or pornographic nature (or create, share, link to or send such material) • Use them in any way that could harm the school's reputation • Access social networking sites or chat rooms • Use any improper language when communicating online, including in emails or other messaging services • Install any unauthorised software, or connect unauthorised hardware or devices to the school's network • Share my password with others or log in to the school's network using someone else's details • Take photographs of pupils without checking with teachers first • Share confidential information about the school, its pupils or staff, or other members of the community • Access, modify or share data I'm not authorised to access, modify or share • Promote private businesses, unless that business is directly related to the school
I will only use the school's IT systems and access the internet in school, or outside school on a work device, for educational purposes or for the purpose of fulfilling the duties of my role. I agree that the school will monitor the websites I visit and my use of the school's IT facilities and systems. I will take all reasonable steps to ensure that work devices are secure and password-protected when using them outside school, and keep all data securely stored in accordance with this policy and the school's data protection policy. I will let the designated safeguarding lead (DSL) and IT manager know if a pupil informs me they have found any material that might upset, distress or harm them or others, and will also do so if I encounter any such material. I will always use the school's IT systems and internet responsibly, and ensure that pupils in my care do so too.

Appendix 4: online safety training needs – self-audit for staff

ONLINE SAFETY TRAINING NEEDS AUDIT	
Name of staff member/volunteer:	**Date**:
Question	**Yes/No (add comments if necessary)**
Do you know the name of the person who has lead responsibility for online safety in school?	
Are you aware of the ways pupils can abuse their peers online?	
Do you know what you must do if a pupil approaches you with a concern or issue?	
Are you familiar with the school's acceptable use agreement for staff, volunteers, governors and visitors?	
Are you familiar with the school's acceptable use agreement for pupils and parents/carers?	
Are you familiar with the filtering and monitoring systems on the school's devices and networks?	
Do you understand your role and responsibilities in relation to filtering and monitoring?	
Do you regularly change your password for accessing the school's ICT systems?	
Are you familiar with the school's approach to tackling cyber-bullying?	
Are there any areas of online safety in which you would like training/further training?	

Appendix 5: online safety incident report log

ONLINE SAFETY INCIDENT LOG				
Date	**Where the incident took place**	**Description of the incident**	**Action taken**	**Name and signature of staff member recording the incident**

AI Appendix for Marian Vian Primary School

Introduction

In alignment with the 2014 National Curriculum in England, our primary school recognises the importance of integrating Artificial Intelligence (AI) into the educational ethos. This AI Appendix aims to provide a structured framework for the effective incorporation of AI tools and practices to enhance teaching and learning outcomes. Furthermore, it ensures adherence to the expectations outlined by Ofsted, fostering an environment of excellence in all aspects of education.

Our AI objectives are:

- To equip students with the knowledge and skills to understand and utilise AI technologies.
- To enhance teaching methodologies and learning experiences through the integration of AI.
- To ensure responsible, ethical, and safe use of AI in the school environment.
- To promote critical thinking, creativity, and digital literacy among students.
- To support staff in professional development relating to AI technologies.

AI Curriculum Framework

Curriculum Integration

- **Key Stages**: AI-related learning objectives will be incorporated across all key stages (EYFS, Key Stage 1 & 2) emphasising age-appropriate activities that introduce students to basic concepts of AI, algorithms, and programming in a safe way.
- **Cross-Curricular Links**: AI will be integrated within other subjects, for example Mathematics (algorithms), Science (data collection and analysis), Computing (coding and robotics) and English (scaffolded and challenge materials).

Skill Development

- **Digital Literacy**: Students will develop essential skills for understanding data protection, privacy, and responsible online behaviour.
- **Critical Thinking**: Opportunities for students to critically assess the information produced by AI tools, fostering analytical and evaluative skills.
- **Creativity and Problem Solving**: Engaging students in projects that require them to create AI-based solutions to real-world problems and creativity.

Teacher Training and Development

- **Professional Development**: Regular training sessions and workshops for staff to enhance their understanding of AI tools and their application in the classroom.
- **Collaboration**: Foster collaborative planning sessions for staff to share best practices and develop interdisciplinary projects and adaptive teaching involving AI.

Responsible Use of AI

- **Ethics and Awareness**: Teaching students about the ethical implications of AI, including fairness, accountability, and transparency (eg fake news).
- **Data Protection**: Instruction on the importance of data protection under the UK General Data Protection Regulation (GDPR), ensuring that students and staff understand the impact of their digital footprints.

Resources and Infrastructure

- **Technology Access**: Ensure equitable access to devices and AI tools for all students, providing support via our IT Maintenance firm, where necessary, to bridge the digital divide.
- **Partnerships**: Collaborate with technology companies and educational organisations for resource sharing, professional development, and accessing cutting-edge AI technologies and safeguarding structures.

Monitoring and Evaluation

- **Assessment**: Continuous evaluation of the AI curriculum's impact on student learning and engagement, including regular feedback sessions with students and staff.
- **Adjustments**: Use insights from assessments to refine and enhance the AI curriculum and policies annually.

Conclusion

This AI appendix aligns with the school's vision to cultivate an innovative and safe learning environment. By adhering to the principles here outlined, we ensure that students are not only consumers of technology but also creators and critical thinkers prepared for the future.

Summary of Inspectorate Expectations

According to the latest Ofsted framework, schools are expected to demonstrate:

1. **High-Quality Education**: Schools should provide a broad and balanced curriculum that supports the development of knowledge and skills in students, making use of innovative teaching methodologies including AI.

2. **Personal Development**: Schools must promote integrated personal development, including social, moral, cultural, and emotional educations such as ethical considerations related to AI use.
3. **Leadership and Management**: Effective leadership in embedding new technologies into the curriculum and ensuring staff are equipped with the necessary skills and knowledge to teach them effectively.
4. **Behaviour and Attitudes**: Establishing a positive, respectful environment where students engage productively with technology.

By fulfilling these expectations, our school is committed to excellence, ensuring that every student benefits from quality education enhanced by advances in artificial intelligence.

STAFF INFORMATION
FACTSHEET 2024

Artificial intelligence (AI) at Marian Vian Primary School

AI isn't new

Artificial intelligence (AI) is the use of computer systems to solve problems and make decisions. It's already a part of everyday life – you've probably already come across it in the form of personalised suggestions on social media, shopping sites or route-planning apps.

However, the technology is developing rapidly and throwing up many new challenges for schools.

What's generative AI?

Generative AI takes a written prompt and runs it through an algorithm to generate new, 'natural'-seeming content. Tools include:

- Chatbots such as ChatGPT, Google Gemini and Grammarly GO, which generate text
- Text-to-image programs like DALL-E and Midjourney, which create images (some programs can make AI-generated animations and near-photorealistic videos, too)

Explain our rules on AI use to pupils

Make sure pupils know that using AI without crediting it is not allowed in exams, coursework or any work that's internally assessed to count towards a qualification. Remind pupils of this when they have exams and coursework coming up.
Have an open dialogue with pupils about how and when AI tools can be used to support learning, and when they shouldn't be used:

At Marian Vian Primary School, we use AI in the classroom to:

- Enhance our learning experiences (eg creating images)

- Develop challenge and scaffolding documents to enhance learning
- Only use materials from AI generated sites when they have been carefully reviewed by teaching staff

When using AI in the classroom, we will support pupils to find age-suitable tools and resources and use them appropriately, without relying on them too much (this is set out in the DfE policy paper). For example:

- Use a PSHE / computing lesson to teach pupils how and when to use an appropriate tool
- Discuss the issue if a pupil brings it up in class or submits AI-generated work

Never enter sensitive information into an AI tool

We will continue to follow our data protection principles and rules, and be aware that any text entered into an AI tool is potentially being made public. If we use AI for any reason, we will not enter any personal or sensitive data.

Marian Vian Primary School or MSLT may also be targeted by fraudulent emails, such as 'phishing' attacks, which are often AI-generated and very convincing. We will look out for the following signs:

- Email addresses that don't match the contact details you have on file
- Poor spelling and grammar, including American spellings, or an overly formal tone
- Messages demanding urgent, time-sensitive action
- Suspicious links, e.g. containing strings of numbers
- Generic introductions (e.g. Dear Sir or Madam)
- AI on invites to TEAMS Meetings - these attendees will be removed from the meeting

Report any suspicious emails to our data protection officer (DPO), Karen Wilson at MSLT.

AI could save you time

You can use AI to cut down on some of your workload. For example, it could help you:

- Create vocabulary banks
- Simplify materials
- Create summaries for texts

AI is not always reliable

AI tools are only as accurate as the information they're trained on. They may generate responses that are incorrect, biased, or inappropriate.

Many tools are based on a defined set of information, so won't be able to accurately give you answers about anything that has changed after data was inputted – e.g. new statutory policy requirements or current events.

It is important to check all AI-generated results carefully

You can use AI tools as a starting point, but you should always check and adapt the results so they are:

- Taking the best interests of staff, pupils and the MSLT into account
- In line with our MSLT policies, procedures and guidelines that cover generative AI:

  GDPR, Safeguarding, E Safety, Computing APU

Ofsted will judge Crofton Schools' use of AI (if we choose to use it)

Ofsted expects us to:

- Make sure our AI solutions are safe and secure, and protecting users' data
- Be transparent about the schools' use of AI and make sure we understand the suggestions it makes
- Use AI only when it's ethically appropriate to do so
- Closely monitor the AI we use for bias
- Identify and correct any bias or problems, where appropriate
- Give staff clear roles in monitoring, evaluating, maintaining and using AI tools
- Make sure that staff are empowered to correct and overrule suggestions made by AI
- Respond appropriately to any concerns, or complaints about errors made by AI