MARTIN PRIMARY SCHOOL

Online Safety Policy

Reviewed and ratified by the Governing Body: autumn 2020

Reviewed every year

1. Introduction

Online safety is an integral part of safeguarding and requires a whole school, cross-curricular approach and collaboration between key school leads. Accordingly, this policy is written in line with 'Keeping Children Safe in Education' 2019 (KCSIE), 'Teaching Online Safety in Schools' 2019 and other statutory documents. It complements existing and forthcoming subjects including Health, Relationships and Sex Education, Citizenship and Computing; it is designed to sit alongside your school's statutory Safeguarding Policy. Any issues and concerns with online safety must follow the school's safeguarding and child protection procedures.

This Policy has been written by the school, building on the London Grid for Learning (LGfL) exemplar policy and Becta guidance.

This policy links with the UN Rights of the Child:

Article 13

Every child must be free to say what they think and to seek and receive all kinds of information, as long as it is within the law.

Article 17

Every child has the right to reliable information from the media. This should be information that children can understand. Governments must help protect children from materials that could harm them.

2. Key people

Designated Safeguarding team	Janine Waterman Ziz Chater
Online safety team	Chantal Lust Marco Ardani Alex Fuller Sussan Khatir Neng Chong
Online safety / safeguarding link governor	Paul Rossi
Technical support	Neng Chong

3. Rationale

The purpose of this policy is to:

- set out the key principles expected of all members of the school community at Martin Primary School with respect to the use of ICT-based technologies
- safeguard and protect the children and staff of Martin Primary School
- assist school staff working with children to work safely and responsibly with the internet and other communication technologies and to monitor their own standards and practice
- set clear expectations of behaviour and/or codes of practice relevant to responsible use of the internet for educational, personal or recreational use
- have clear structures to deal with online abuse such as cyberbullying which are cross referenced with other school policies
- ensure that all members of the school community are aware that unlawful or unsafe behaviour is unacceptable and that, where appropriate, disciplinary or legal action will be taken
- minimise the risk of misplaced or malicious allegations made against adults who work with pupils.

4. The main areas of risk for our school community can be summarised as follows:

4.1 Content

- exposure to inappropriate content, including online pornography, ignoring age ratings in games (exposure to violence associated with often racist language and misogynist language and scenarios), substance abuse
- lifestyle websites, for example pro-anorexia/self-harm/suicide sites
- hate sites
- exposure to websites connected to radicalisation and extremism
- content validation: how to check authenticity and accuracy of online content.

4.2 Contact

- grooming
- grooming for radicalisation
- online-bullying in all forms
- identity theft (including 'frape' (hacking Facebook profiles)) and sharing passwords.

4.3 Conduct

- privacy issues, including disclosure of personal information
- digital footprint and online reputation
- health and well-being (amount of time spent online (internet or gaming))
- sexting (sending and receiving of personally intimate images) also referred to as SGII (self-generated indecent images)
- copyright (little care or consideration for intellectual property and ownership – such as image, text, music and film).

5. How will this policy be communicated?

This policy can only impact upon practice if it is a (regularly updated) living document. It must be accessible to and understood by all stakeholders. It will be communicated in the following ways:

- posted on the school website
- available on the staff shared drive
- part of school induction pack for new staff
- integral to safeguarding updates and training for all staff (especially in September refreshers)
- clearly reflected in the Acceptable Use Policies (AUPs) for staff, volunteers, contractors, governors, pupils and parents/carers/carers.

6. Aims

This policy aims to:

- set out expectations for all Martin Primary School community members' online behaviour, attitudes and activities and use of digital technology (including when devices are offline)
- help all stakeholders to recognise that online/digital behaviour standards (including social media activity) must be upheld beyond the confines of the school gates and school day, and regardless of device or platform
- facilitate the safe, responsible and respectful use of technology to support teaching & learning, increase attainment and prepare children and young people for the risks and opportunities of today's and tomorrow's digital world, to survive and thrive online
- help school staff working with children to understand their roles and responsibilities to work safely and responsibly with technology and the online world:
    - for the protection and benefit of the children and young people in their care, and
    - for their own protection, minimising misplaced or malicious allegations and to better understand their own standards and practice
    - for the benefit of the school, supporting the school ethos, aims and objectives, and protecting the reputation of the school and profession

- establish clear structures by which online misdemeanours will be treated, and procedures to follow where there are doubts or concerns (with reference to other school policies such as Behaviour Policy or Anti-Bullying Policy).

7. Further help and support

Internal school channels will always be followed first for reporting and support, as documented in our policy documents, especially in response to safeguarding incidents which are reported in line with our Safeguarding Policy. The DSL will handle referrals to Barnet's Multi-Agency Safeguarding Hub (MASH) and normally the headteacher will handle referrals to the LA designated officer (LADO).

Beyond this, **reporting.lgfl.net** has a list of curated links to external support and helplines for both pupils and staff, including the Professionals' Online safety Helpline from the UK Safer Internet Centre and the NSPCC Whistleblowing Helpline, as well as hotlines for hate crime, terrorism and fraud which might be useful to share with parents/carers, and anonymous support for children and young people.

8. Scope

This policy applies to all members of the Martin Primary School community (including staff, governors, volunteers, contractors, students/pupils, parents/carers/carers, visitors and community users) who have access to our digital technology, networks and systems, whether on-site or remotely, and at any time, or who use technology in their school role.

9. Roles and responsibilities

This school is a community and all members have a duty to behave respectfully online and offline, to use technology for teaching and learning and to prepare for life after school, and to immediately report any concerns or inappropriate behaviour, to protect staff, pupils, families and the reputation of the school. We learn together, make honest mistakes together and support each other in a world that is online and offline at the same time.

9.1 Headteacher

Key responsibilities:

- foster a culture of safeguarding where online safety is fully integrated into whole-school safeguarding
- oversee the activities of the designated safeguarding lead and ensure that the DSL responsibilities listed in the section below are being followed and fully supported
- ensure that policies and procedures are followed by all staff
- undertake training in offline and online safeguarding, in accordance with statutory guidance and relevant Local Safeguarding Partnerships
- liaise with the designated safeguarding lead on all online safety issues which might arise and receive regular updates on school issues and broader policy and practice information
- take overall responsibility for data management and information security ensuring the school's provision follows best practice in information handling; work with the DPO, DSL and governors to ensure a GDPR-compliant framework for storing data, but helping to ensure that child protection is always put first and data-protection processes support careful and legal sharing of information
- ensure the school implements and makes effective use of appropriate ICT systems and services including school-safe filtering and monitoring, protected email systems and that all technology including cloud systems are implemented according to child-safety first principles
- be responsible for ensuring that all staff receive suitable training to carry out their safeguarding and online safety roles
- understand and make all staff aware of procedures to be followed in the event of a serious online safeguarding incident
- ensure suitable risk assessments are undertaken so the curriculum meets needs of pupils, including risk of children being radicalised

- ensure that there is a system in place to monitor and support staff (e.g. network manager) who carry out internal technical online safety procedures
- ensure governors are regularly updated on the nature and effectiveness of the school's arrangements for online safety
- ensure the school website meets statutory requirements (see appendices for website audit document).

9.2 Designated Safeguarding Lead

Key responsibilities:

- "The designated safeguarding lead should take lead responsibility for safeguarding and child protection (including online safety)."
- ensure that there is regular review and open communication between the DSL and the Online Safety team and that the DSL's clear overarching responsibility for online safety is not compromised
- ensure that all procedures outlined in our Safeguarding and Child Protection Policy are followed including the requirements to ensure that all staff receive appropriate and up-to-date training.

9.3 Online Safety team

Key responsibilities:

- ensure "An effective approach to online safety [that] empowers a school or college to protect and educate the whole school or college community in their use of technology and establishes mechanisms to identify, intervene in and escalate any incident where appropriate."
- take day to day responsibility for online safety issues and be aware of the potential for serious child protection concerns
- work with the headteacher, DPO and governors to ensure a GDPR-compliant framework for storing data, but helping to ensure that child protection is always put first and data-protection processes support careful and legal sharing of information
- stay up to date with the latest trends in online safety
- review and update this policy, other online safety documents (e.g. Acceptable Use Policies) and the strategy on which they are based (in harmony with policies for behaviour, safeguarding, Prevent and others) and submit for review to the governors/trustees.
- receive regular updates in online safety issues and legislation, be aware of local and school trends
- ensure that online safety education is embedded across the curriculum (e.g. by use of the UKCIS framework 'Education for a Connected World') and beyond, in wider school life
- promote an awareness and commitment to online safety throughout the school community, with a strong focus on parents/carers, who are often appreciative of school support in this area, but also including hard-to-reach parents/carers
- liaise with school technical, pastoral, and support staff as appropriate
- communicate regularly with SLT and the designated safeguarding and online safety governor/committee to discuss current issues (anonymised), review incident logs and filtering/change control logs and discuss how filtering and monitoring
- ensure all staff are aware of the procedures that need to be followed in the event of an online safety incident, and that these are logged in the same way as any other safeguarding incident
- oversee and discuss 'appropriate filtering and monitoring' with governors and ensure staff are aware.

9.4 Governing Body, led by the Online Safety/Safeguarding Link Governor

Key responsibilities: (all quotes are taken from Keeping Children Safe in Education)

- approve this policy and strategy and subsequently review its effectiveness, e.g. by asking the questions in the helpful document from the UK Council for Child Internet Safety (UKCIS)

- "Ensure an appropriate **senior member** of staff, from the school or college leadership team, is appointed to the role of DSL [with] **lead responsibility** for safeguarding and child protection (including online safety) [with] the appropriate status and authority [and] time, funding, training, resources and support…"
- support the school in encouraging parents/carers and the wider community to become engaged in online safety activities
- have regular strategic reviews with the online safety co-ordinator / DSL and incorporate online safety into standing discussions of safeguarding at governor meetings
- ensure that there is regular review and open communication between the DSL and the Online Safety team and that the DSL's clear overarching responsibility for online safety is not compromised
- work with the DPO, DSL and headteacher to ensure a GDPR-compliant framework for storing data, but helping to ensure that child protection is always put first and data-protection processes support careful and legal sharing of information
- check all school staff have read Part 1 of KCSIE; SLT and all working directly with children have read Annex A; check that Annex C on Online Safety reflects practice in your school
- "Ensure that all staff undergo safeguarding and child protection training (including online safety) at induction."
- "Ensure appropriate filters and appropriate monitoring systems are in place [but…] be careful that 'overblocking' does not lead to unreasonable restrictions as to what children can be taught with regard to online teaching and safeguarding".
- "Ensure that children are taught about safeguarding, including online safety […] as part of providing a broad and balanced curriculum […] Consider a whole school or college approach to online safety [with] a clear policy on the use of mobile technology."

9.5 All staff

Key responsibilities:

- understand that online safety is a core part of safeguarding; as such it is part of everyone's job – never think that someone else will pick it up
- know who the Designated Safeguarding Lead (DSL) and Online Safety Lead (OSL) are
- read Part 1, Annex A and Annex C of Keeping Children Safe in Education (whilst Part 1 is statutory for all staff, Annex A for SLT and those working directly with children, it is good practice for all staff to read all three sections)
- read and follow this policy in conjunction with the school's main safeguarding policy
- record online safety incidents in the same way as any safeguarding incident and report in accordance with school procedures
- understand that safeguarding is often referred to as a jigsaw puzzle – you may have discovered the missing piece so do not keep anything to yourself
- sign and follow the staff acceptable use policy and code of conduct/handbook
- notify the DSL/OSL if policy does not reflect practice in your school and follow escalation procedures if concerns are not promptly acted upon
- identify opportunities to thread online safety through all school activities, both outside the classroom and within the curriculum, supporting curriculum/stage/subject leads, and making the most of unexpected learning opportunities as they arise (which have a unique value for pupils)
- whenever overseeing the use of technology (devices, the internet, new technology such as augmented reality, etc) in school or setting as homework tasks, encourage sensible use, monitor what pupils/students are doing and consider potential dangers and the age appropriateness of websites
- carefully supervise and guide pupils when engaged in learning activities involving online technology (including, extra-curricular and extended school activities if relevant), supporting them with search skills, critical thinking (e.g. fake news), age appropriate materials and signposting, and legal issues such as copyright and data law
- prepare and check all online source and resources before using within the classroom
- encourage pupils/students to follow their acceptable use policy, remind them about it and enforce school sanctions

- notify the DSL/OSL of new trends and issues before they become a problem
- take a zero-tolerance approach to bullying and low-level sexual harassment (your DSL will disseminate relevant information from the new DfE document on this)
- be aware that you are often most likely to see or overhear online safety issues (particularly relating to bullying and sexual harassment and violence) in the playground, corridors, toilets and other communal areas outside the classroom – let the DSL/OSL know
- receive regular updates from the DSL/OSL and have a healthy curiosity for online safety issues

model safe, responsible and professional behaviours in their own use of technology. This includes outside the school hours and site, and on social media, in all aspects upholding the reputation of the school and of the professional reputation of all staff.

9.6 Computing team

Key responsibilities:

As listed in the 'all staff' section, plus:

- oversee the delivery of the online safety element of the Computing curriculum in accordance with the national curriculum
- work closely with the DSL/OSL and all other staff to ensure an understanding of the issues, approaches and messaging within Computing
- collaborate with technical staff and others responsible for ICT use in school to ensure a common and consistent approach, in line with acceptable-use agreements.

9.7 Technical support

Key responsibilities:

As listed in the 'all staff' section, plus:

- keep up to date with the school's online safety policy and technical information in order to effectively carry out their online safety role and to inform and update others as relevant
- work closely with the designated safeguarding lead / online safety lead / data protection officer to ensure that school systems and networks reflect school policy
- ensure the above stakeholders understand the consequences of existing services and of any changes to these systems (especially in terms of access to personal and sensitive records / data and to systems such as YouTube mode, web filtering settings, sharing permissions for files on cloud platforms etc
- support and advise on the implementation of 'appropriate filtering and monitoring' as decided by the DSL and senior leadership team
- maintain up-to-date documentation of the school's online security and technical procedures
- to report online safety related issues that come to their attention in line with school policy
- manage the school's systems, networks and devices, according to a strict password policy, with systems in place for detection of misuse and malicious attack, with adequate protection, encryption and backup for data, including disaster recovery plans, and auditable access controls
- monitor the use of school technology, online platforms and social media presence and that any misuse/attempted misuse is identified and reported in line with school policy

9.8 Volunteers and contractors

Key responsibilities:

- read, understand, sign and adhere to an acceptable use policy (AUP)
- report any concerns, no matter how small, to the designated safety lead / online safety coordinator as named in the AUP
- maintain an awareness of current online safety issues and guidance
- model safe, responsible and professional behaviours in their own use of technology.

9.9 Pupils

Key responsibilities:

- read, understand, sign and adhere to the student/pupil acceptable use policy and review this annually
- understand the importance of reporting abuse, misuse or access to inappropriate materials
- know what action to take if they or someone they know feels worried or vulnerable when using online technology
- understand the importance of adopting safe and responsible behaviours and good online safety practice when using digital technologies outside of school and realise that the school's acceptable use policies cover actions out of school, including on social media
- understand the benefits/opportunities and risks/dangers of the online world and know who to talk to at school or outside school if there are problems.

9.10 Parents/carers/carers

Key responsibilities:

- read, sign and promote the school's parental acceptable use policy (AUP) and read the pupil AUP and encourage their children to follow it
- consult with the school if they have any concerns about their children's and others' use of technology
- promote positive online safety and model safe, responsible and positive behaviours in their own use of technology, including on social media: not sharing other's images or details without permission and refraining from posting negative, threatening or violent comments about others, including the school staff, volunteers, governors, contractors, pupils or other parents/carers/carers.

9.11 External groups including the MHSA

Key responsibilities:

- any external individual/organisation will sign an acceptable use policy prior to using technology or the internet within school
- support the school in promoting online safety and data protection
- model safe, responsible, respectful and positive behaviours in their own use of technology, including on social media: not sharing other's images or details without permission and refraining from posting negative, threatening or violent comments about others, including the school staff, volunteers, governors, contractors, pupils or other parents/carers/carers.

10. Education and curriculum

The following subjects have the clearest online safety links:

- PSHE
- Relationships education, relationships and sex education (RSE) and health
- Computing

However, it is the role of all staff to identify opportunities to thread online safety through all school activities, both outside the classroom and within the curriculum, supporting curriculum/stage/subject leads, and making the most of unexpected learning opportunities as they arise (which have a unique value for pupils).

Whenever overseeing the use of technology (devices, the internet, new technology such as augmented reality, etc) in school or setting as homework tasks, all staff should encourage sensible use, monitor what pupils/students are doing and consider potential dangers and the age appropriateness of websites). Equally, all staff should carefully supervise and guide pupils when engaged in learning activities involving online technology (including, extra-curricular and extended school activities if relevant), supporting them with search skills, critical thinking (e.g. fake news), age appropriate materials and signposting, and legal issues such as copyright and data law.

Whilst regulation and technical solutions are very important, their use must be balanced by educating students / pupils to take a responsible approach. The education of pupils in online safety is therefore an essential part of the school's online safety provision. Children and young people need the help and support of the school to recognise and avoid online safety risks and build their resilience.

Online safety should be a focus in all areas of the curriculum and staff should reinforce online safety messages across the curriculum. The online safety curriculum should be broad, relevant and provide progression, with opportunities for creative activities A planned online safety curriculum should be provided as part of computing lessons and should be regularly revisited. Key online safety messages should also be reinforced as part of a planned programme of assemblies and pastoral activities.

Pupils will be taught to:

- be critically aware of the materials / content they access online and be guided to validate the accuracy of information
- understand the importance of using 'strong and safe' passwords
- acknowledge the source of information used and to respect copyright when using material accessed on the internet
- STOP and THINK before they CLICK
- develop a range of strategies to evaluate and verify information before accepting its accuracy
- be aware that the author of a web site / page may have a particular bias or purpose and to develop skills to recognise what that may be
- [for older pupils] understand how search engines work and to understand that this affects the results they see at the top of the listings
- understand acceptable behaviour when using an online environment / email, i.e. be polite, no bad or abusive language or other inappropriate behaviour; keeping personal information private
- understand how photographs can be manipulated and how web content can attract the wrong sort of attention
- understand why online 'friends' may not be who they say they are and to understand why they should be careful in online environments
- understand why they should not post or share detailed accounts of their personal lives, contact information, daily routines, location, photographs and videos and to know how to ensure they have turned-on privacy settings
- understand why they must not post pictures or videos of others without their permission
- understand the impact of cyberbullying, sexting and trolling and know how to seek help if they are affected by any form of online bullying
- know how to report any abuse including cyberbullying; and how to seek help if they experience problems when using the internet and related technologies, i.e. parent or carer, teacher or trusted staff member, or an organisation such as Childline or the CLICK CEOP button
- plan internet use carefully to ensure that it is age-appropriate and supports the learning objectives for specific curriculum areas.

In lessons where internet use is pre-planned, it is best practice that pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches. However particularly in upper KS2 teachers will want pupils to develop as discerning and responsible users of the Internet and to use their self-managing skills, so they will support children in learning how to use search engines for themselves carefully – e.g typing in 'for kids' at the end of a search, looking for familiar sites e.g BBC

11. Handling online safety concerns and incidents

It is vital that all staff recognise that online safety is a part of safeguarding (as well as being a curriculum strand of Computing, PSHE/RSHE and Citizenship). General concerns must be handled in the same way as any other safeguarding concern, as outlined in the school's Safeguarding and Child Protection Policy.

This school commits to take all reasonable precautions to ensure online safety, but recognises that incidents will occur both inside school and outside school and that those from outside school will continue to impact on pupils when they come into school. All members of the school are encouraged to report issues swiftly to allow us to deal with them quickly and sensitively through the school's escalation processes.

Any suspected online risk or infringement should be reported to the online safety lead / designated safeguarding lead on the same day – where clearly urgent, it will be made by the end of the lesson.

Any concern/allegation about staff misuse is always referred directly to the Headteacher, unless the concern is about the Headteacher in which case the compliant is referred to the Chair of Governors and the LADO (Local Authority's Designated Officer). Staff may also use the NSPCC Whistleblowing Helpline.

The school will actively seek support from other agencies as needed (i.e. the local authority, LGfL, UK Safer Internet Centre's Professionals' Online Safety Helpline, NCA CEOP, Prevent Officer, Police, IWF). The school will inform parents/carers/carers of online safety incidents involving their children, and the Police where staff or pupils engage in or are subject to behaviour which the school considers is particularly disturbing or breaks the law.

12. Misuse of school technology (devices, systems, networks or platforms)

Where pupils contravene the rules and guidelines in this Policy, the school's Behaviour Policy will be applied. Where staff contravene the rules and guidelines in this Policy, action will be taken as outlined in Barnet's Capability Policy, the code of conduct and or the staff handbook protocol.

This policy applies to incidents that take place inside or outside school that affects any person(s) within school or the wider community outside school if it reflects on the school. The students will be subject to the Behaviour Policy and the staff will be subject to Barnet's Capability Policy, the code of conduct and or the staff handbook protocol.

Further to these steps, the school reserves the right to withdraw – temporarily or permanently – any or all access to such technology, or the right to bring devices onto school property.

13. Social media incidents

Where an incident relates to an inappropriate, upsetting, violent or abusive social media post by a member of the school community, the school will request that the post be deleted and will expect this to be actioned promptly.

Where an offending post has been made by a third party, the school may report it to the platform it is hosted on, and may contact the Professionals' Online Safety Helpline (run by the UK Safer Internet Centre) for support or help to accelerate this process.

14. Appropriate filtering and monitoring

Keeping Children Safe in Education obliges schools to "ensure appropriate filters and appropriate monitoring systems are in place [and] not be able to access harmful or inappropriate material [but at the same time] be careful that "over blocking" does not lead to unreasonable restrictions as to what children can be taught with regards to online teaching and safeguarding."

At this school, the internet connection is provided by LGfL. This means we have a dedicated and secure, schoolsafe connection that is protected with firewalls and multiple layers of security, including a web filtering system called WebScreen 3, which is made specifically to protect children in schools.
There are three types of appropriate monitoring identified by the Safer Internet Centre. These are:

1. physical monitoring (adult supervision in the classroom, at all times)
2. internet and web access
3. active/Pro-active technology monitoring services.

15. Email

Staff at this school use the StaffMail system for all school emails. This system is linked to the USO authentication system and is fully auditable, trackable and managed by LGfL on behalf of the school. This is for the mutual protection and privacy of all staff, pupils and parents/carers, as well as to support data protection.

General principles for email use are as follows:

- email may only be sent using the email systems above. There should be no circumstances where a private email is used; if this happens by mistake, the DSL/Headteacher/DPO (the particular circumstances of the incident will determine whose remit this is) should be informed immediately.
- staff or pupil personal data should never be sent/shared/stored on email. If data needs to be shared with external agencies, USO-FX and Egress systems are available from LGfL. Internally. If personal data does need to be shared by email, information should be password protected using a strong password and the email address verified before sending to prevent a data breach.
- staff should use the school network or the Google Drive, including when working from home when remote access is available.
- Staff are NOT allowed to use the email system for personal use and should be aware that all use is monitored, their emails may be read and the same rules of appropriate behaviour apply at all times. Emails using inappropriate language, images, malware or to adult sites may be blocked and not arrive at their intended destination.

See also the social media section of this policy.

16. School website

The school website is a key public-facing information portal for the school community (both existing and prospective stakeholders) with a key reputational value. The Headteacher is responsible for ensuring that the website content is accurate and complies with DfE requirements. Day-to-day responsibility of updating the content of the website to is delegated to a member of the office team.

Where other staff submit information for the website, they are asked to remember:

- schools have the same duty as any person or organisation to respect and uphold copyright law. Sources must always be credited and material only used with permission.
- Where pupil work is published on the website, the identities of the pupils are protected unless specific consent has been obtained (see point 18 below).

19. Google Drive

This school adheres to the principles of the DfE document '[Cloud computing services: guidance for school leaders, school staff and governing bodies]'. The data protection officer and technical support analyse and document systems and procedures before they are implemented, and regularly review them.

The following principles apply:

- the DPO approves new cloud systems, what may or may not be stored in them and by whom. This is noted in a DPIA (data-protection impact statement) and parental permission is sought
- regular training ensures all staff understand sharing functionality and this is audited to ensure that pupil data is not shared by mistake. Open access or widely shared folders are clearly marked as such
- pupils and staff are only given access and/or sharing rights when they can demonstrate an understanding of what data may be stored and how it can be seen
- two-factor authentication is used for access to staff or pupil data will be used when possible and as it can be implemented in to school systems.
- only school-approved platforms are used by staff to store pupil work
- all stakeholders understand the difference between consumer and education products (e.g. a private Gmail account or Google Drive and those belonging to a managed educational domain).

20. Digital images and video

- The school imposes a range of restrictions as to what the school digitally records and publishes: all employees and governors are subject to these restrictions.
- No photographs, videos, or digital images of children or adults are permitted to be taken at Martin Primary. The three exceptions to this are: 'Tapestry', which is covered under a separate agreement, photos for the school website (see point 7), and official school photographs of individuals and classes.
- Children's work can be photographed and this may include the child's hands, or other unidentifiable body part. This work will be labelled with the child's name. These images may also be stored e.g. for reference purposes.
- Any events where pupils are performing will not be digitally recorded by the school e.g. Christmas show, Carol Concert, end of Y6 Leavers' show, Year 6 Leavers' book and so on. This includes events on the school premises as well as those at other locations e.g. East Finchley Arts Festival. The school will take every precaution to minimise the chance of other bodies e.g. the local press from taking photographs. However, this cannot be guaranteed in public places, as the school does not have ultimate jurisdiction in this setting.
- Parents/carers/carers will be reminded that any images they take are for personal use only and are not to be shared via social media – attention will be drawn to the safeguarding implications.
- If photos are required for the school's website, then explicit written permission will be sought from individual parents/carers/carers. These photos will be carefully stage-managed and no 'background' children will be permitted. This process will be subjected to audit by non-staff members of the Governing Body, normally the designated safeguarding governor.
- All outside providers where Martin Primary children are involved e.g. after school clubs etc… will be advised of these protocols and will be subject to them. This includes the Y2 jamboree, Forest School and MHSA events for both children and adults e.g. Christmas Fair, Summer Fair, Quiz night, and so on. This list is just for illustrative purposes and is not exhaustive.
- This information will be included in the updated Staff Handbook.
- The parents/carers/carers of children who have a medical condition will be asked to provide a colour photograph, signed on the back, to be displayed where necessary in the school in order to keep their child safe e.g. dining hall, staff room, school office.

Pupils are advised to be very careful about placing any personal photos on social media. They are taught to understand the need to maintain privacy settings so as not to make public, personal information.

Pupils are taught that they should not post images or videos of others without their permission. The school teaches them about the risks associated with providing information with images

(including the name of the file), that reveals the identity of others and their location. We teach them about the need to keep their data secure and what to do if they / or a friend are subject to bullying or abuse.

21. Staff, pupils' and parents/carers' social media presence

Social media (including all apps, sites and games that allow sharing and interaction between users) is a fact of modern life, and as a school, we accept that many parents/carers, staff and pupils will use it. However, as stated in the acceptable use policies which all members of the school community sign, we expect everybody to behave in a positive manner, engaging respectfully with the school and each other on social media, in the same way as they would face to face.

This positive behaviour can be summarised as not making any posts which are or could be construed as bullying, aggressive, rude, insulting, illegal or otherwise inappropriate, or which might bring the school or (particularly for staff) teaching profession into disrepute. This applies both to public pages and to private posts, e.g. parent chats, pages or groups.

If parents/carers have a concern about the school, we would urge them to contact us directly and in private to resolve the matter. If an issue cannot be resolved in this way, the school complaints procedure should be followed. Sharing complaints on social media is unlikely to help resolve the matter, but can cause upset to staff, pupils and parents/carers, also undermining staff morale and the reputation of the school (which is important for the pupils we serve).

Staff are reminded that they are obliged not to bring the school or profession into disrepute and the easiest way to avoid this is to have the strictest privacy settings and avoid inappropriate sharing and oversharing online. They should never discuss the school or its stakeholders on social media and be careful that their personal opinions might not be attributed to the school, trust or local authority, bringing the school into disrepute.

The serious consequences of inappropriate behaviour on social media are underlined by the fact that there have been 200 Prohibition Orders issued to teachers over the past four years related to the misuse of technology/social media.

All members of the school community are reminded that particularly in the context of social media, it is important to comply with the school policy on Digital Images and Video (see point 21) and permission is sought before uploading photographs, videos or any other information about other people.

22. Personal devices including wearable technology and bring your own device (BYOD)

- Mobile phones brought into school are entirely at the staff member, pupils and parents/carers' or visitors own risk. The School accepts no responsibility for the loss, theft or damage of any phone or hand held device brought into school.
- Pupils' mobile phones which are brought into school must be turned off (not placed on silent) and handed in to the school office for safe keeping until the end of the school day when they can be collected.
- Staff must not use mobile phones to take pictures or videos of children in any circumstances.
- Mobile phones are not permitted for use anywhere in school, around the children. This applies to members of staff and other visitors to the school. Mobile phones may only be used in office areas, staffroom etc. If a staff member is expecting an important personal call when teaching or otherwise on duty, they may leave their phone with the school office to answer on their behalf or ask for the message to be left with the school office.
- Child/staff data should never be downloaded onto a private phone.
- The only exception to this is staff taking a mobile phone with them on a school trip/visit outside of school: see Educational Visits Policy. Staff should not share their personal mobile

phone numbers with parents/carers. Parents/carers/carers who accompany a school trip should be given the main school phone number for contact purposes.

- Where staff members are required to use a mobile phone for school duties, for instance in case of emergency during off-site activities, or for contacting students or parents/carers, they should use their own device and hide (by inputting 141) their own mobile number for confidentiality purposes.
- Parents/carers are asked to leave their phones in their pockets and turned off when they are on site.
- Visitors/Contractors are not permitted to use mobile phones and or any other devices use anywhere in school, around the children.

23. Asset disposal

Details of all school-owned hardware will be recorded in a hardware inventory. All redundant equipment that may have held personal data will have the storage media forensically wiped or destroyed by an authorised company. Alternatively, if the storage media has failed, it will be physically destroyed. The school will only use authorised companies who will supply a written guarantee that this will happen.

Disposal of any equipment will conform to The Waste Electrical and Electronic Equipment Regulations 2006 and/or The Waste Electrical and Electronic Equipment (Amendment) Regulations 2007. Further information can be found on the Environment Agency website.

24. Related policies

- Safeguarding and Child Protection Policy
- Anti-Bullying Policy
- Behaviour Policy
- Acceptable Use Policies
- Data Protection Policy

Key Stage 1: Acceptable Use Agreement

I keep **SAFE online** because …	✓
I **CHECK** it's OK to use a website / game / app.	
I **ASK** for help if I get lost online.	
I **THINK** before I click on things.	
I **KNOW** online people are really strangers.	
I am **RESPONSIBLE** so never share private information.	
I am **KIND** and polite online.	
I **TELL** a trusted adult if I am worried about anything.	

My trusted adults are:	Mum
	Dad
	Teacher

My name: Date signed:	

KS2 Pupil Online Acceptable Use Agreement

This agreement will help keep me safe and help me to be fair to others.

- ***I am an online digital learner*** – I use the school's IT for schoolwork, homework and other activities approved by trusted adults.
- ***I am a secure online learner*** - I keep my logins and passwords secret.
- ***I am careful online*** - I think before I click on links and only download when I know it is safe or has been agreed by trusted adults.
- ***I am guarded online*** - I only give out my full home address, phone number or other personal information that could be used to identify me or my family and friends when my trusted adults have agreed.
- ***I am cautious online*** - I know that some websites and social networks have age restrictions and I respect this and I only visit internet sites that I know my trusted adults have agreed.
- ***I am considerate online*** - I do not get involved with bullying or sharing inappropriate material.
- ***I am respectful online*** – I do not respond to unkind or hurtful messages/comments and tell my trusted adults if I receive these.
- ***I am responsible online*** – I keep others safe by talking to my trusted adults if a friend or person I know is being bullied or harassed online or is being affected by things they see or hear online.
- ***I am a creative digital learner online*** - I only edit or delete my own digital work and only use other people's work with their permission or where the work is shared through a Creative Commons licence.
- ***I am a researcher online*** - I use safer search tools approved by my trusted adults and know to 'double check' all information I find online.
- ***I communicate and collaborate online*** - with people I know and have met in real life or that a trusted adult has approved.
- ***I am SMART online*** - I understand that unless I have met people in real life, an online person is actually a stranger. I may sometimes want to meet these strangers so I will always ask my trusted adults for advice.

I have read and understood this agreement.

I know who are my trusted adults are and agree to the above.

Signed: _____ Date: _____

Appendix 2

Remote learning

1.1. All remote learning is delivered in line with the school's Pupil Remote Learning Policy.

1.2. All staff and pupils using video communication must:
- communicate in groups
- 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
- ensure that an adult is present with the pupil throughout the 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.

1.3. 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.

1.4. 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 Headteacher, in collaboration with the SENCO.

1.5. Pupils not using devices or software as intended will be disciplined in line with the school's Behaviour Policy.

1.6. 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.

1.7. The school will communicate to parents/carers in writing 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.

1.8. During the period of remote learning, the school will maintain regular contact with parents/carers to:
- reinforce the importance of children staying safe online
- ensure parents/carers 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/carers to useful resources to help them keep their children safe online.

1.9. 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.