Online safety Policy 2022
St. Michael in the Hamlet Primary School

Key Staff

Designated Safeguarding Lead (DSL) Miss L Moreton
Deputy Safeguarding Lead (joint) Mrs C Jones and Miss A Bedford
Safeguarding Team – Mrs H Day
Online-safety lead – Mr C Ramsden
Online-safety / safeguarding link governor - Rona Lucas

Scope

This policy applies to all members of St Michael in the Hamlet community (including staff, governors, volunteers, contractors, students/pupils, parents/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.
Online safety is an integral part of safeguarding and requires a whole school, cross-curricular approach and collaboration between key school leads. 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 subjects including Health, Relationships and Sex Education, Citizenship and Computing; it is designed to sit alongside our school's statutory Safeguarding Policy. Any issues and concerns with online safety must follow the school's safeguarding and child protection procedures.

This policy aims to:

Set out expectations for all St Michael in the Hamlet 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)

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.

Role	Key Responsibilities
Headteacher - Miss L Moreton (DSL)	• To ensure online safety is fully integrated into whole-school safeguarding • 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 • 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 • To ensure all staff follow safeguarding procedures 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

Online Safety Lead – C. Ramsden supported by H. Day	• "The designated safeguarding lead should take lead responsibility for safeguarding and child protection (including online safety)." • Ensure "An effective approach to online safety [that] empowers school to protect and educate the whole school community in their use of technology and identify, intervene in and escalate any incident where appropriate." • "Liaise with the local authority and work with other agencies in line with Working together to safeguard children" • Take day to day responsibility for online safety issues and be aware of the potential for serious child protection concerns • Stay up to date with the latest trends in online safety • To review policies and to be accepted by Governors. • 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, who are often appreciative of school support in this area, but also including hard-to-reach parents • 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 (is it physical or technical?) and ensure staff are aware. • Ensure the 2018 DfE guidance on sexual violence and harassment is followed throughout the school and that staff adopt a zero-tolerance approach to this, as well as to bullying

Governing Body, led by Online Safety / Safeguarding Link Governor – Rona Lucas	**(quotes are taken from Keeping Children Safe in Education 2019):** • Approve this policy and strategy and subsequently review its effectiveness • "Ensure an appropriate **senior member** of staff, from the school leadership team, is appointed to the role of DSL **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 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 • Where the online-safety coordinator is not the named DSL or deputy DSL, ensure that there is regular review and open communication between these roles and that the DSL's clear overarching responsibility for online safety is not compromised • Check all school staff 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. The training should be regularly updated. • "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 approach to online safety with a clear policy on the use of mobile technology.

All Staff	• 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 are Miss L Moreton and Miss A Bedford • 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. • Sign and follow the staff acceptable use policy and code of conduct/handbook • 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 • 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 • To 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 • 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.

PSHE / RSHE Lead/ Miss J Tsai	• As listed in the 'all staff' section, plus: • Embed consent, mental wellbeing, healthy relationships and staying safe online into the PSHE / Relationships education, relationships and sex education (RSE) and health education curriculum. "This will include being taught what positive, healthy and respectful online relationships look like, the effects of their online actions on others and knowing how to recognise and display respectful behaviour online. Throughout these subjects, teachers will address online safety and appropriate behaviour in an age appropriate way that is relevant to their pupils' lives." • This will complement the computing curriculum, which covers the principles of online safety at all key stages, with progression in the content to reflect the different and escalating risks that pupils face. This includes how to use technology safely, responsibly, respectfully and securely, and where to go for help and support when they have concerns about content or contact on the internet or other online technologies. • Work closely with the DSL/OSL and all other staff to ensure an understanding of the issues, approaches and messaging within PSHE / RSHE.
Computing Lead – Jade Norman	• 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
Subject leads	• As listed in the 'all staff' section, plus: • Look for opportunities to embed online safety in your subject or aspect, and model positive attitudes and approaches to staff and pupils alike • Consider how the UKCIS framework Education for a Connected World and Teaching Online Safety in Schools can be applied in your context • Work closely with the DSL/OSL and all other staff to ensure an understanding of the issues, approaches and messaging within Computing • Ensure subject specific action plans also have an online-safety element

Network Technician – Mr S. Rogers (external agency)	• 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 / LGfL nominated contact 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 on Twitter, Facebook, YouTube and Class Dojo. and that any misuse/attempted misuse is identified and reported in line with school policy • Work with the Headteacher to ensure the school website meets statutory DfE requirements

Pupils must:

- 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
- To 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

Parents/carers must:

- 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.
- Monitor their child/rens activity online on a daily basis

The following subjects have the clearest online safety links

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

However, as stated in the role descriptors above, 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 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.

At St Michael in the Hamlet we recognise that online safety and broader digital resilience must be thread throughout the curriculum and that is why we are working to adopt the cross-curricular framework 'Education for a Connected World' from UKCIS (the UK Council for Internet Safety.

Handling online-safety concerns and incidents

It is vital that all staff recognise that online-safety is a part of safeguarding. General concerns must be handled in the same way as any other safeguarding concern. Support staff will often have a unique insight and opportunity to find out about issues first in the playground, corridors, toilets and other communal areas outside the classroom (particularly relating to bullying and sexual harassment and violence).

School procedures for dealing with online-safety will be mostly detailed in the following policies:

- Safeguarding and Child Protection Policy
- Anti-Bullying Policy
- Behaviour Policy
- Data Protection Policy, agreements and other documentation

Our 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.)

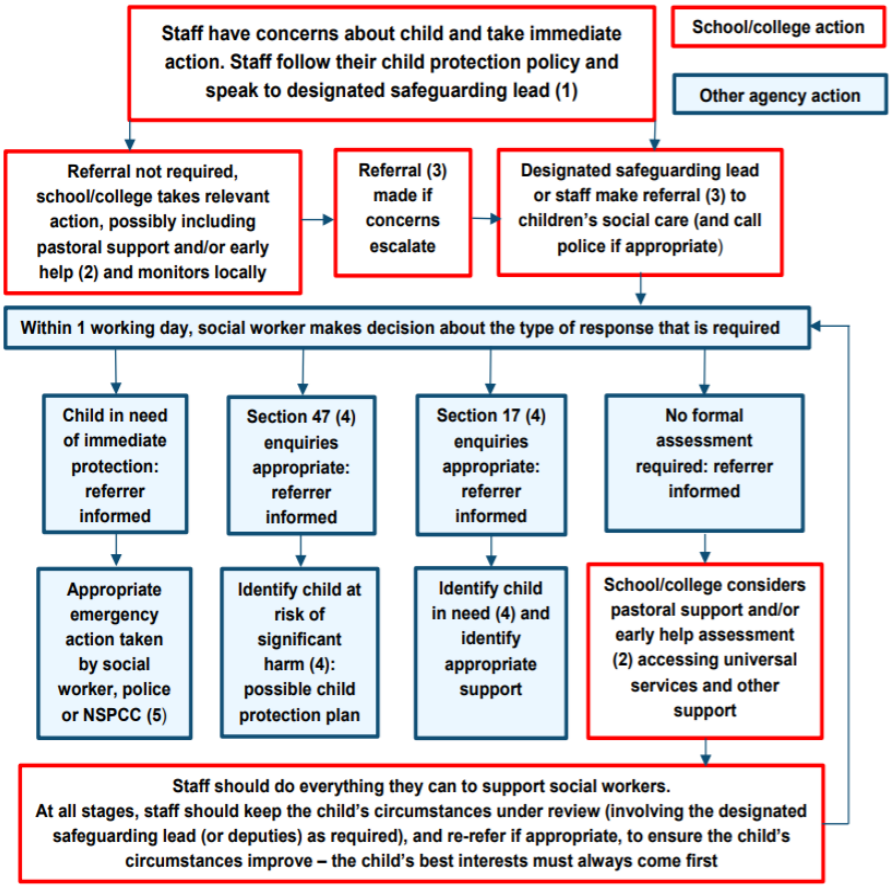
Any suspected online risk or infringement should be reported to the online safety lead / designated safeguarding lead on the same day – where clearly urgent, it will be made by the end of the lesson.

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). We will inform parents/carers of online-safety incidents involving their children, and the Police where staff or pupils engage in or are subject to behaviour which we consider is particularly disturbing or breaks the law.

Actions were there are concerns about a child:

The following flow chart, taken from page 13 of Keeping Children Safe in Education 2019 as the key education safeguarding document. As outlined previously, online safety concerns are no different to any other safeguarding concern.



(1) In cases which also involve a concern or an allegation of abuse against a staff member, see Part Four of this guidance.

(2) Early help means providing support as soon as a problem emerges at any point in a child's life. Where a child would benefit from co-ordinated early help, an early help inter-agency assessment should be arranged. Chapter one of Working Together to Safeguard Children provides detailed guidance on the early help process.

(3) Referrals should follow the process set out in the local threshold document and local protocol for assessment. Chapter one of Working Together to Safeguard Children.

(4) Under the Children Act 1989, local authorities are required to provide services for children in need for the purposes of safeguarding and promoting their welfare. Children in need may be assessed under section 17 of the Children Act 1989. Under section 47 of the Children Act 1989, where a local authority has reasonable cause to suspect that a child is suffering or likely to suffer significant harm, it has a duty to make enquiries to decide whether to take action to safeguard or promote the child's welfare. Full details are in Chapter one of Working Together to Safeguard Children.

(5) This could include applying for an Emergency Protection Order (EPO).

Sexting

All schools (regardless of phase) should refer to the UK Council for Internet Safety (UKCIS) guidance on sexting (also referred to as 'youth produced sexual imagery') in schools. NB - where one of the parties is over 18, this is no longer sexting but child sexual abuse.

There is a one-page overview called Sexting; how to respond to an incident for all staff (not just classroom-based staff) to read, in recognition of the fact that it is mostly someone other than the

designated safeguarding lead (DSL) or online safety lead to first become aware of an incident, and it is vital that the correct steps are taken. Staff other than the DSL must not attempt to view, share or delete the image or ask anyone else to do so, but to go straight to the DSL.

The school DSL will in turn use the full guidance document, Sexting in Schools and Colleges to decide next steps and whether other agencies need to be involved.

It is important that everyone understands that whilst sexting is illegal, pupils/students can come and talk to members of staff if they have made a mistake or had a problem in this area.

Upskirting

It is important that everyone understands that upskirting (taking a photo of someone under their clothing) is now a criminal offence, as highlighted in Keeping Children Safe in Education and that pupils/students can come and talk to members of staff if they have made a mistake or had a problem in this area.

Bullying

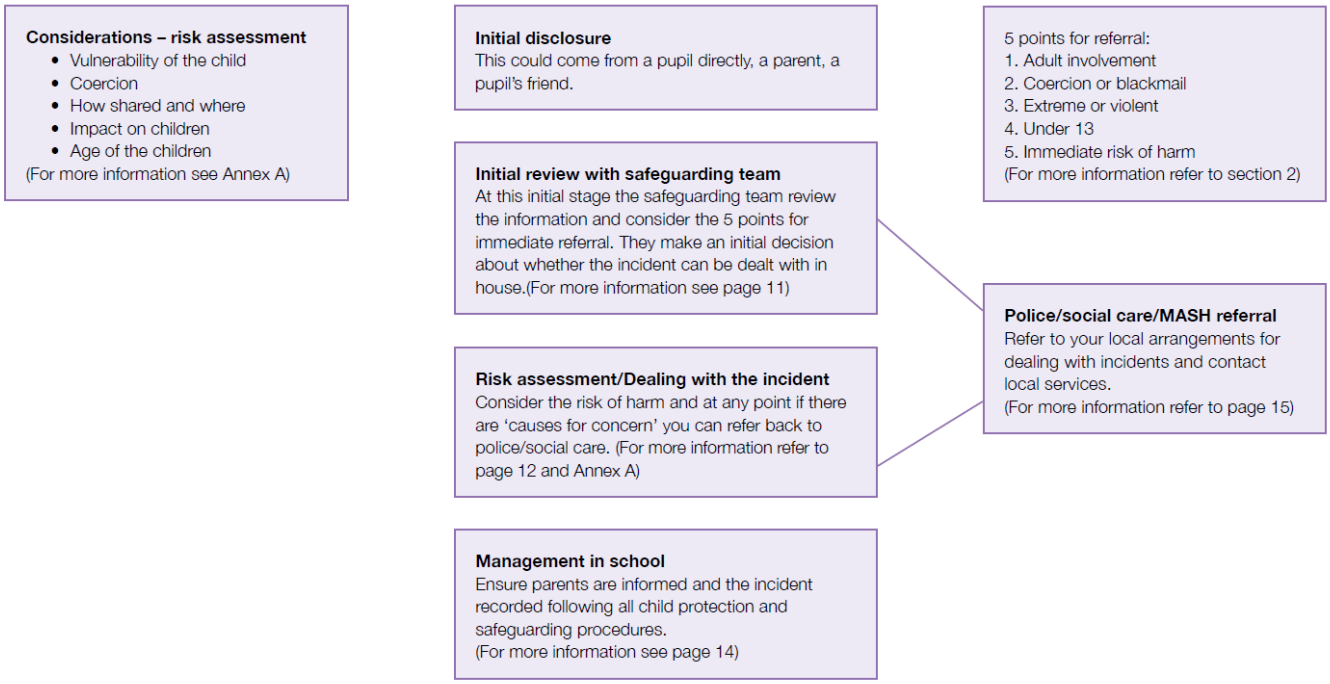
Online bullying should be treated like any other form of bullying and the school bullying policy should be followed for online bullying, which may also be referred to as cyberbullying

Sexual violence and harassment

Any incident of sexual harassment or violence (online or offline) should be reported to the DSL who will follow the full guidance. Staff should work to foster a zero-tolerance culture. The guidance stresses that schools must take all forms of sexual violence and harassment seriously, explaining how it exists on a continuum and that behaviours incorrectly viewed as 'low level' are treated seriously and not allowed to

Annex G

Flowchart for responding to incidents



perpetuate. KCSiE makes specific reference to behaviours such as bra-strap flicking and the careless use of language.

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

Clear and well communicated rules and procedures are essential to govern pupil and adult use of school networks, connections, internet connectivity and devices, cloud platforms and social media (both when on school site and outside of school).

Where pupils contravene these rules, the school behaviour policy will be applied; where staff contravene these rules, action will be taken as outlined in the staff code of conduct/handbook.

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.

Social media incidents

Where an incident relates to an inappropriate, upsetting, violent or abusive social media post by a member of the school community, we 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.

Digital images and videos

When a pupil joins the school, parents/carers are asked if they give consent for their child's image to be captured in photographs or videos, for what purpose. The permission lasts for an academic year unless changed by a parent/carer throughout the year. Parents answer as follows:

- around school
- on our website
- Twitter
- Facebook

Whenever a photo or video is taken/made, the member of staff taking it will check the latest database before using it for any purpose.

Any pupils shown in public facing materials are never identified with more than first name (and photo file names/tags do not include full names to avoid accidentally sharing them).

All staff are governed by their contract of employment and the school's Acceptable Use Policy, which covers the use of mobile phones/personal equipment for taking pictures of pupils, and where these are stored. At St Michael in the Hamlet no member of staff will ever use their personal phone to capture photos or videos of pupils.

Photos are stored on the school network/cameras/iPads/laptops, in line with the retention schedule of the school Data Protection Policy.

Staff and parents are reminded annually about the importance of not sharing without permission, due to reasons of child protection (e.g. looked-after children often have restrictions for their own protection), data protection, religious or cultural reasons, or simply for reasons of personal privacy.

We encourage young people to think about their online reputation and digital footprint, so we should be good adult role models by not oversharing (or providing embarrassment in later life – and it is not for us to judge what is embarrassing or not).

Pupils are taught about how images can be manipulated in their online safety education programme and also taught to consider how to publish for a wide range of audiences which might include governors, parents or younger children

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. We teach 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.

Social Media

St Michael in the Hamlet works on the principle that if we don't manage our social media reputation, someone else will.
Online Reputation Management (ORM) is about understanding and managing our digital footprint (everything that can be seen or read about the school online). Few parents will apply for a school place without first 'googling' the school, and the Ofsted pre-inspection check includes monitoring what is being said online (Mumsnet is a favourite).

Negative coverage almost always causes some level of disruption. Up to half of all cases dealt with by the Professionals Online Safety Helpline (POSH: helpline@saferinternet.org.uk) involve schools' (and staff members') online reputation.

Accordingly, we manage and monitor our social media footprint carefully to know what is being said about the school and to respond to criticism and praise in a fair, responsible manner. Miss L Moreton and Mrs S Burch is responsible for managing our Twitter/Facebook accounts and checking our Wikipedia and Google reviews. They follow the guidance in the LGfL / Safer Internet Centre online-reputation management document here.

Staff, pupil and parent's SM presence

Social media (including here 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, 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 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, also undermining staff morale and the reputation of the school (which is important for the pupils we serve).

Many social media platforms have a minimum age of 13, but the school deals with issues arising on social media with pupils/students under the age of 13. We ask parents to respect age ratings on social media platforms wherever possible and not encourage or condone underage use. It is worth noting that following on from the government's Safer Internet Strategy, enforcement and age checking is likely to become more stringent over the coming years.

However, the school has to strike a difficult balance of not encouraging underage use at the same time as needing to acknowledge reality in order to help our pupils to avoid or cope with issues if they arise. Online safety lessons will look at social media and other online behaviour. How to be a

good friend online and how to report bullying, misuse, intimidation or abuse. However, children will often learn most from the models of behaviour they see and experience, which will often be from adults.

Parents can support this by, talking to their children about the apps, sites and games they use (you don't need to know them – ask your child to explain it to you). With whom, for how long, and when (late at night / in bedrooms is not helpful for a good night's sleep and productive teaching and learning at school the next day). You may wish to introduce the Children's Commission Digital 5 A Day.
It is encouraging that 73% of pupils (from the 40,000 who answered that LGfL DigiSafe pupil online safety survey) trust their parents on online safety (although only half talk about it with them more than once a year at the moment).

The school has an official Facebook / Twitter account (managed by Mrs Burch) and will respond to general enquiries about the school, but asks parents/carers not to use these channels to communicate about their children.

Email is the official electronic communication channel between parents and the school, and between staff and pupils

Pupils/students are not allowed to be 'friends' with or make a friend request to any staff, governors, volunteers and contractors or otherwise communicate via social media.

Pupils/students are discouraged from 'following' staff, governor, volunteer or contractor public accounts (e.g. following a staff member with a public Instagram account). However, we accept that this can be hard to control (but this highlights the need for staff to remain professional in their private lives). In the reverse situation, however, staff must not follow such public student accounts.

Exceptions may be made, e.g. for pre-existing family links, but these must be approved by the Headteacher and should be declared upon entry of the pupil or staff member to the school.

Any attempt to do so may be a safeguarding concern or disciplinary matter and should be notified to the DSL (if by a child) or to the Headteacher (if by a staff member).

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, and permission is sought before uploading photographs, videos or any other information about other people.

Device usage

Please read the following in conjunction with acceptable use policies and the following sections of this document which all impact upon device usage: copyright, data protection, social media, misuse of technology, and digital images and video.

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

Pupils/students in Year 6 are allowed to bring mobile phones in for emergency use only, when they are allowed to walk home from school. Mobile phones are handed to the teachers, then stored in the main office until the end of the day.

All staff who work directly with children should leave their mobile phones on silent and away in bags/lockers. They can only be used in private staff areas during school hours. Child/staff data should never be downloaded onto a private phone. 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.

Volunteers, contractors, governors should leave their phones in their pockets and turned off. Under no circumstances should they be used in the presence of children or to take photographs or videos. If this is required (e.g. for contractors to take photos of equipment or buildings), permission of the headteacher should be sought (the headteacher may choose to delegate this) and this should be done in the presence of a member staff.

Parents should ask permission before taking any photos, e.g. of displays in corridors or classrooms, and avoid capturing other children. When at school events, parents are told to keep their phones away and to not record or photograph the event. Parents are asked not to call pupils on their mobile phones during the school day; urgent messages can be passed via the school office.

Network/internet access

Pupils/students are not allowed to access school network.

All staff who work directly with children Child/staff data should never be downloaded onto a private phone.

Volunteers, contractors, governors have no access to the school network or wireless internet on personal devices or can no access to networked files/drives, subject to the acceptable use policy. All internet traffic is monitored.

Parents have no access to the school network or wireless internet on personal devices, have no access to networked files/drives, subject to the acceptable use policy. All internet traffic is monitored.

Trips and events away from school

For school trips/events away from school, teachers will be issued a school duty phone and this number used for any authorised or emergency communications with pupils/students and parents. Any deviation from this policy (e.g. by mistake or because the school phone will not work) will be notified immediately to the headteacher. Teachers using their personal phone in an emergency will ensure that the number is hidden to avoid a parent or student accessing a teacher's private phone number.

Searching and confiscation

In line with the DfE guidance 'Searching, screening and confiscation: advice for schools', the Headteacher/Principal and staff authorised by them have a statutory power to search pupils/property on school premises. This includes the content of mobile phones and other devices, for example as a result of a reasonable suspicion that a device contains illegal or undesirable material, including but not exclusive to sexual images, pornography, violence or bullying.

Further help and support

Internal school channels should always be followed first for reporting and support, as documented in school policy documents, especially in response to incidents, which should be reported in line with your Safeguarding Policy. The DSL will handle referrals to local authority multi-agency safeguarding hubs (MASH) and normally the headteacher will handle referrals to the LA designated officer (LADO). The local authority, academy trust or third-party support organisations you work with may also have advisors to offer general support.

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, and anonymous support for children and young people.

St Michael in the Hamlet have access to National Online Safety, which is a website that provides support and guidance for staff and parents/carers. Important and relevant messages will be shared from this website regularly.

Appendix 1 – User Code of Conduct for Computing

To ensure that all members of staff and Governors are fully aware of their professional responsibilities when using information systems and when communicating with pupils, they are asked to sign this code of conduct. All staff should consult the school's Online safety policy for further information and clarification.

- I understand that it is a criminal offence to use a school ICT system for a purpose not permitted by its owner.
- I appreciate that ICT includes a wide range of systems, including mobile phones, digital cameras, email and social networking sites and that ICT use may also include personal ICT devices when used for school business.
- I understand that mobile phones and other personal ICT devices may only be accessed for private use during breaks or and not during scheduled working hours.
- I understand that school information systems may not be used for private purposes without specific permission from the head teacher.
- I understand that use of school information systems, Internet and email may be monitored and recorded to ensure policy compliance.
- I will respect system security and I will not disclose any password or security information to anyone other than an authorised system manager.
- I will not install any software or hardware without permission.
- I will ensure that personal data is stored securely and is used appropriately, whether in school, taken off the school premises or accessed remotely.
- I will respect copyright and intellectual property rights.
- I will report any incidents of concern regarding children's safety to the Online safety coordinator, the Designated Child Protection Coordinator or Head teacher.
- I will promote Online safety with students in my care and will help them to develop a responsible attitude to system use, communications and publishing.

The school may exercise its right to monitor the use of the school's information systems and Internet access, to intercept e-mail and to delete inappropriate materials where it believes unauthorised use of the school's information system may be taking place, or the system may be being used for criminal purposes or for storing unauthorised or unlawful text, imagery or sound.

I have read, understood and accept the User Code of Conduct for ICT.

Signed: ..... Capitals: .....

Date: .....