Online Safety Policy 2023/2024

'Working together to achieve success'

This policy has been written in line with 'Keeping Children Safe in Education' 2023, 'Teaching Online Safety in Schools', statutory RSHE guidance and other statutory documents. Any issues and concerns with online safety must always follow the school's safeguarding and child protection procedures.

What are the main online safeguarding risks?
In our school over the past year, we have particularly noticed the following in terms of device use and abuse and types of online/device-based incidents which affect the wellbeing and safeguarding of our students:

- Unsupervised viewing of inappropriate videos by Reception to Y3 children at home.
- Name-calling and falling out using What'sApp in KS2.
- Creating and sharing videos using What'sApp.

The continued cost-of-living crisis has meant that children have spent more time online and therefore exposed to all manner of online harms as families have had to cut back on leisure activities and the public provision of free activities for young people has reduced further.

Mossgate primary school

Our mission:

'Working together to achieve success'

- As active and healthy **individuals** who are inquisitive, have the belief to try new things and manage risks safely.
- As resilient, confident and independent **learners** who strive to achieve their best.
- As honest, courteous and kind **friends** who respect and value difference and have the courage to challenge discrimination.
- As active and responsible and respectful **citizens** who have a positive impact within their school, community and wider world.

Against this background, the Ofcom 'Children and parents: media use and attitudes report 2023' has shown that YouTube remains the most used site or app among all under 18s and the reach of WhatsApp, TikTok and Snapchat increased yet further. As a school we recognise that many of our children and young people are on these apps regardless of age limits, which are often misunderstood or ignored. We therefore remember to remind about best practice while remembering the reality for most of our students is quite different.

This is striking when you consider that 20% of 3-4 year olds have access to their OWN mobile phone (let alone shared devices), rising to over 90 percent by the end of Primary School, and the vast majority have no safety controls or limitations to prevent harm or access to inappropriate material. At the same time, even 3 to 6 year olds are being tricked into 'self-generated' sexual content (Internet Watch Foundation Annual Report) while considered to be safely using devices in the home and the 7-10 year old age group is the fastest growing for this form of child sexual abuse material, up 60 percent within 12 months to represent over 60,000 cases found (of this same kind where the abuser is not present).

In the past year, more and more children and young people used apps such as snapchat as their source of news and information, with little attention paid to the veracity of influencers sharing news. The 2023 Revealing-Reality: Anti-social-Media Report highlights that this content is interspersed with highly regular exposure to disturbing, graphic and illegal content such as fights, attacks, sexual acts and weapons. At the same time, the Children's Commissioner revealed that ever younger children are regularly consuming pornography and living out inappropriate behaviour and relationships due to 'learning from' pornography. This has coincided with the rise of misogynistic influencers such as Andrew Tate, which had a significant influence on many young boys over the past year which schools have had to counter.

Purpose and aims
This policy aims to promote a whole school approach to online safety by:

- Setting out expectations for all Mossgate community members' online behaviour, attitudes and activities and use of digital technology (including when devices are offline)

- Helping safeguarding and senior leadership teams to have a better understanding and awareness of all elements of online safeguarding through effective collaboration and communication with technical colleagues (e.g. for filtering and monitoring), curriculum leads (e.g. RSHE) and beyond.
- Helping 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, regardless of device or platform, and that the same standards of behaviour apply online and offline.
- Facilitating the safe, responsible, respectful and positive 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
- Helping 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
- Establishing 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)
- Ensuring that, as an organisation, we operate in line with our values and within the law in terms of how we use online devices

This policy applies to all staff, volunteers, children and anyone involved in activities with Mossgate Primary School and should be read alongside our policies and procedures on:

- Safeguarding & Child Protection Policy
- Behaviour Policy
- Anti-Bullying Policy
- Mobil Phone Policy
- Home School Agreement
- Code of Conduct Policy
- Social Media & Networking Sites Policy

This policy has been drawn up on the basis of legislation, policy and guidance that seeks to protect children in England. Summaries of the key legislation and guidance are available on:

- **online abuse** https://learning.nspcc.org.uk/child-abuse-and-neglect/online-abuse
- **bullying** https://learning.nspcc.org.uk/child-abuse-and-neglect/bullying
- **child protection** https://learning.nspcc.org.uk/child-protection-system/england

Online Safety Approach

Online safety is an integral part of safeguarding and requires a whole school, cross-curricular approach and collaboration between key school leads. At Mossgate, our online safety approach includes:

- appointing a senior leader with responsibility for online safety leader, which includes responsibility for internet filtering and monitoring
- teaching Online Safety using the cross-curricular framework 'Education for a Connected World – 2020 edition' from UKCIS (the UK Council for Internet Safety). Units are mapped to different curriculum areas and taught throughout the year using the Project Evolve resources.
- Regularly monitoring the online safety curriculum through pupil voice, book looks and learning walks to ensure all pupils (including for SEND and disadvantaged pupils) are being equipped with the knowledge and skills to stay safe online
- supporting and encouraging children to use the internet, social media and mobile phones in a way that keeps them safe and shows respect for others (this occurs through our school values, Computing & PSHEC curriculum, Anti-Bullying Week in November and Online Safety Week in February)
- supporting and encouraging parents and carers to do what they can to keep their children safe online through online safety information shared in our newsletters, assemblies and workshops when relevant
- developing age-appropriate online safety agreements in class every year with the children – see example at the end of this policy

- developing clear and robust procedures to enable us to respond appropriately to any incidents of inappropriate online behaviour, whether by an adult or a child – see Behaviour, Anti-Bullying, Staff Code of Conduct, Safeguarding and Whistleblowing Policies
- reviewing and updating our cybersecurity arrangements regularly to keep our information systems secure
- ensuring that user names, logins and passwords are used effectively and kept private
- ensuring personal information about the adults and children at Mossgate, is held securely and shared only as appropriate
- examining and risk assessing any social media platforms and new technologies before they are used with suitable training
- ensuring appropriate filters and monitoring systems are in place so that children cannot access harmful or inappropriate material from our school network
- providing clear and specific directions to staff and volunteers on how to behave online through our induction process which includes the relevant policies listed at the start of this policy
- actively seeking support from other agencies as needed (i.e. the local authority, LGfL, Mental Health Services, UK Safer Internet Centre's Professionals' Online Safety Helpline (POSH), NCA CEOP, Prevent Officer, Police, Nurse, IWF and Harmful Sexual Behaviour Support Service)
- 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 concerning or breaks the law (particular procedures are in place for sexting and upskirting)
- completing an annual online safety audit and government's digital & technology standards, which involve a link governor, to review our approach an procedures
- seeking parents' consent, through our Home School Agreement, for photos / videos to be shared externally. Photos or videos do not display the child's name unless this is for the local newspaper and parents' consent has been given. See Home School Agreement for more detail. Class registers list children who do not have consent.

If online incidents or abuse occurs, we will respond to it by:
- having clear and robust behaviour, anti-bullying and safeguarding procedures (see relevant policies) in place for responding to incidents and abuse (including online abuse)
- providing support and training for all staff and volunteers on dealing with all forms of abuse, including child-on-child abuse, bullying/cyberbullying, emotional abuse, sexting, sexual abuse and sexual exploitation
- making sure our response takes the needs of the person experiencing abuse, any bystanders and our school as a whole into account
- reviewing the plan developed to address online abuse at regular intervals, in order to ensure that any problems have been resolved in the long term
- staff reporting concerns about adults to the Headteacher. If the concern is about the Headteacher, this is referred to the Chair of Governors and the LADO (Local Authority's Designated Officer). If staff have concerns about the safeguarding culture or procedures, they should follow the whistleblowing Policy. Useful names and numbers are included in the Safeguarding Poters in communal areas of the school.

Filtering and Monitoring
An active and well managed filtering system is an important part of providing a safe environment for pupils to learn at Mossgate. Working with Schools Broadband and our IT support (Tech-Hub), our school's filtering system blocks internet access to harmful sites and inappropriate content. We work closely to ensure it does not unreasonably impact teaching and learning or school administration or restrict pupils from learning how to assess and manage risk themselves.

All staff and governors receive regular training about filtering and monitoring and how they contriute to its effectiveness in keeping children and staff safe.

Monitoring user activity on school devices is an important part of providing a safe environment for children and staff. Unlike filtering, it does not stop users from accessing material through internet searches or software.

Monitoring allows us to review user activity on school devices. For monitoring to be effective it must pick up incidents urgently which are shared daily with the Headteacher by email so that prompt action can be taken. Additional monitoring activities include:

- physically monitoring by staff watching screens of users
- pupils only permitted to use devices when supervised
- devices numbered and allocated to pupils so that they can be trace
- network monitoring using log files of internet traffic and web access
- individual device monitoring through software or third-party services
- senior leaders, with a governor if possible, carrying out specific checks of the filter and monitoring software – this must be done in pairs to safeguard the leader from allegations

Staff must report if:

- they witness or suspect unsuitable material has been accessed
- they can access unsuitable material
- they are teaching topics which could create unusual activity on the filtering logs
- there are perceived unreasonable restrictions that affect teaching and learning or administrative tasks
- they notice abbreviations or misspellings that allow access to restricted material
- devices used at home have been used to access inappropriate content

To safeguard themselves, staff must:

- take care if/when accessing the school WI-FI
- protect their usernames and passwords – do not share
- not access personal emails on school devices / networks
- take care when using your mobile or other personal device in school during breaks
- not use your mobile to take photos – see Mobile Phone Policy

Staff email and communication systems

Staff must only use their Office 365 email account (@mossgate.lancs.sch.uk) for all school emails. They never use a personal/private email account (or other messaging platform) to communicate with children or parents, or to colleagues when relating to school/child data, using a non-school-administered system. Staff emails are monitored and may be read by the Headteacher or other person with delegated responsibility.

If messages need to be sent to parents, this can be done using School Spider using the School Spider app for free, or as a paid text if the parent does not access the app. School Spider is centrally managed and administered by the school or authorised IT partner (i.e. they can be monitored/audited/viewed centrally; are not private or linked to private accounts). This is for the mutual protection and privacy of all staff, pupils and parents, supporting safeguarding best-practice, protecting children against abuse, staff against potential allegations and in line with UK data protection legislation.

Use of any new platform with communication facilities or any child login or storing school/child data must be approved in advance by the Headteacher and centrally managed. Any unauthorised attempt to use a different system 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).

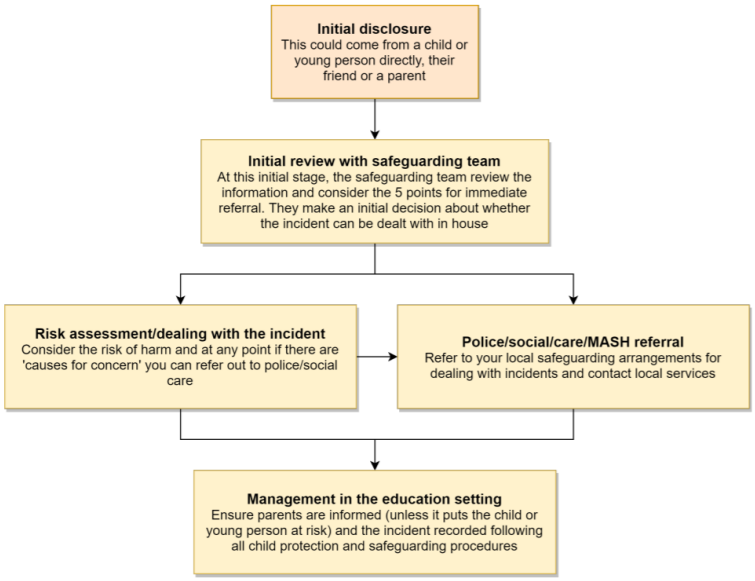
Where devices have multiple accounts for the same app, mistakes can happen, such as an email being sent from or data being uploaded to the wrong account. If this a private account is used for communication or to store data by mistake, the DSL/Headteacher/DPO (the particular circumstances of the incident will determine whose remit this is) should be informed immediately.

Sexting

All schools should refer to the UK Council for Internet Safety (UKCIS) guidance on sexting (now referred to as Sharing nudes and semi-nudes: advice for education settings) to avoid unnecessary criminalisation of children. 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 Sharing nudes and semi-nudes: 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, Sharing nudes and semi-nudes – advice for educational settings to decide next steps and whether other agencies need to be involved.



***Consider the 5 points for immediate referral at initial review:**

1. The incident involves an adult
2. There is reason to believe that a child or young person has been coerced, blackmailed or groomed, or there are concerns about their capacity to consent (for example, owing to special educational needs)
3. What you know about the images or videos suggests the content depicts sexual acts which are unusual for the young person's developmental stage, or are violent
4. The images involves sexual acts and any pupil in the images or videos is under 13
5. You have reason to believe a child or young person is at immediate risk of harm owing to the sharing of nudes and semi-nudes, for example, they are presenting as suicidal or self-harming

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, not necessarily a skirt) is now a criminal offence and constitutes a form of sexual harassment as highlighted in Keeping Children Safe in Education. As with other forms of child-on-child abuse 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 or cyberbullying, including incidents that take place outside school or from home, should be treated like any other form of bullying and our school Anti-Bullying Policy will be followed, including issues arising from 'banter'. More detail can be found in the separate policy.

Child-on-child sexual violence and sexual harassment

Any incident of sexual harassment or violence (online or offline) should be reported to the DSL who will follow the full guidance in line with our Safeguarding Policy. Staff should work to foster a zero-tolerance culture and maintain an attitude of 'it could happen here'.

At Mossgate, we 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 perpetuate. In the online environment, the recent proliferation of misogynistic content is particularly relevant when it comes to considering reasons for and how to combat this kind of behaviour.

School's Social Media

We work 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.

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, POSH, (run by the UK Safer Internet Centre) for support or help to accelerate this process using their email (POSH: helpline@saferinternet.org.uk).

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. The Headteacher and Office

Manager is responsible for managing our Facebook account and checking our Wikipedia and Google reviews and other mentions online.

Social Media Use by Others
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, 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 (note that WhatsApp is 16+), but the school regularly deals with issues arising on social media involving 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.

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 best help our pupils/students 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 best 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 refer to the Digital Family Agreement to help establish shared expectations and the Top Tips for Parents poster along with relevant items and support available from parentsafe.lgfl.net and introduce the Children's Commission Digital 5 A Day.

Although the school has an official Facebook account and will respond to general enquiries about the school, it asks parents/carers not to use these channels, especially not to communicate about their children.

Email is the official electronic communication channel between parents and the school. Social media, including chat apps such as WhatsApp, are not appropriate for school use.
Pupils 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 are discouraged from 'following' staff, governor, volunteer or contractor public accounts (e.g. following a staff member with a public Instagram account) as laid out in the AUPs. 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/Principal, 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 has been a significant number of Prohibition Orders issued by the Teacher Regulation Agency to teaching staff that involved misuse of social media/technology.

Mobile Phones
Pupils in the Y5 & Y6 are allowed to bring mobile phones into school if they walk to / from school on their own so that they can communicate with their parents. As soon as children enter the school grounds, they must take the phone to the school office where it will be stored securely. Parents must sign our Mobile Phone Agreement for this arrangement to be put in place. Phones must not be used in the school grounds – this includes at school events outside of the school day. See Mobile Phone Policy for more detail.

Low-level Concerns Concerning Adults
The term 'low-level' concern does not mean that it is insignificant. A low-level concern is any concern – no matter how small, and even if no more than causing a sense of unease or a 'nagging doubt' – that an adult working in or on behalf of the school may have acted in a way that:
• is inconsistent with the staff code of conduct, including inappropriate conduct outside of work, and
• does not meet the harm threshold or is otherwise not serious enough to consider a referral to the LADO.

Examples of such behaviour could include, but are not limited to:

- not treating all children fairly and consistently in accordance with school policies
- humiliating children
- being over friendly with children
- having favourites
- taking photographs of children on their mobile phone, contrary to school policy, or
- engaging with a child on a one-to-one basis in a secluded area or behind a closed door.

If staff have a safeguarding concern or an allegation about another member of staff (including supply staff, volunteers or contractors) that does not meet the harm threshold, then this should be shared with the Headteacher. If your concerns relate to the Headteacher, you should raise them with a senior leader and the Chair of Governors.

Monitoring and Review
Monitoring is the responsibility of the Headteacher, Governors (through the School Improvement Committee) and senior leader with responsibility for Online Safety. Any incidents will be reported termly to Governors by the Headteacher. The policy will be reviewed annually.

The school is aware of our legal duties under the Equality Act 2010, to promote equality of opportunity and to reduce discrimination.

Reviewed by the Subject Leader:	Approved by Governors:	Next review date:
Autumn 2023	Autumn 2023	Autumn 2024

This policy has been written in accordance to recent advice, publications and the law:

- 'KCSIE – Keeping Children Safe in Education 2023 – Statutory Guidance for Schools and Colleges' Department for Education (September 2023)
- 'Teaching online safety in schools' Department for Education (Updated 12th January 2023)
- 'Example online safety policy statement and agreement' NSPCC (February 2022)
- LGfL 'Online Safety Policy 2023/2024' Template (August 2023)

Online Safety Agreement

'Working together to achieve success'

Young person: please read the following agreement and discuss it with your parents/carers

Parents/carers: please read and discuss this agreement with your child and then sign it, ask your child to sign it, and return it to their class teacher.

If you have any questions or concerns, please speak to Mr Smith or Mrs Taylor.

Mossgate primary school

Our mission:

'Working together to achieve success'

- As active and healthy individuals who are inquisitive, have the belief to try new things and manage risks safely.
- As resilient, confident and independent learners who strive to achieve their best.
- As honest, courteous and kind friends who respect and value difference and have the courage to challenge discrimination.
- As active and responsible and respectful citizens who have a positive impact within their school, community and wider world.

Young person's agreement

1. I will be responsible for my behaviour when using the internet, including social media platforms, games and apps. This includes the resources I access and the language I use.
2. I will not deliberately browse, download or upload material that could be considered inappropriate, offensive or illegal.
3. If I accidentally come across any such material, I will report it immediately to an adult.
4. I will not send anyone material that could be considered inappropriate, threatening, bullying, offensive or illegal.
5. I will not give out any personal information online, such as my name, phone number or address.
6. I will keep my passwords private.
7. I will not arrange a face-to-face meeting with someone I meet online, and if I am asked to do so, I will discuss this with a trusted adult like my parents or teacher.
8. If I am concerned or upset about anything I see on the internet, or any messages that I receive, I know I can talk to a trusted adult like my parents or teacher.
9. I understand that my internet use at Mossgate Primary School will be monitored, and logged, and can be made available to Mr Smith, other teachers and parents.
10. I understand that these rules are designed to keep me safe and that if I choose not to follow them, teachers may contact my parents/carers.
11. If I have permission to bring my mobile phone to school, I will take this to the school office as soon as I enter the school grounds and not use for an inappropriate use. (This includes events outside of the school day.)

Signatures:

We have discussed this online safety agreement and _____ agrees to follow the rules set out above.

Parent/carer signature: _____ Date: _____

Young person's signature: _____ Date: _____