LGfL SafeguardED

LDST Liverpool Diocesan Schools Trust

ONLINE SAFETY POLICY 2023/24

GLAZEBURY C.E. PRIMARY SCHOOL

Learn, Love and Achieve, Together with Jesus

OUR TRUST'S PRAYER

Heavenly Father
Let peace, friendship and love grow in our schools
Send the Holy Spirit to give excellence to our learning
Love to our actions and Joy to our worship
Guide us to help others so that we may all
Learn, Love and Achieve,
Together with Jesus.
Amen

School values central to life in our community

At Glazebury CE Primary our core values of **Love and Wisdom** are at the centre of all that we do and all that we are. We feel that the values of friendship, truthfulness, hope, peace, creation, trust, compassion, justice, humility and forgiveness are fundamental to the growth of all.

Love never fails, 1 Corinthians 8:13

For the Lord gives wisdom : from his mouth comes knowledge and understanding. Proverbs 2:6

The HEART of our Curriculum:

H – Helping children prepare for life, growing with God.

E – Embracing Christian Values.

A - Achievement for all.

R - Reading at the heart of our school

T – Teaching a knowledge rich curriculum.

Introduction

Key people / dates

Designated Safeguarding Lead (DSL), with lead responsibility for filtering and monitoring	Karen Mowbray Head Teacher
Deputy Designated Safeguarding Leads / DSL Team Members	Karen Wall Deputy Head Teacher
Link governor for safeguarding (includes online safety)	Stuart Roberts Tighe
Curriculum leads with relevance to online safeguarding and their role [e.g. PSHE/RSHE/RSE/Computing leads]	Karen Mowbray Head Teacher
Network manager / other technical support	Tech minder LTD
Date this policy was implemented by school and by whom	September 22

What's different about this policy for September 2023?

This year, changes have been made to reflect trends seen over the past year and especially in the light of changes to KCSIE – the most significant change relating to filtering and monitoring, as well as to shorten this document.

The DSL has now been asked to take lead responsibility for web filtering and monitoring, marking a clear shift. Schools now need to follow the new DfE standards and consider the roles and responsibilities of all staff – for DSLs and SLT, the challenge is to better understand, review and drive the rationale behind decisions in this area. Tech teams and safeguarding teams will need to work much more closely together for this to be possible and technicians will be charged to carry out regular checks and feed back to DSL teams. All staff need to be aware of the changes and renewed emphasis and play their part in feeding back about over-blocking or gaps in the filtering provision. Schools will also be reviewing their approaches to monitoring in line with the standards (note that filtering and monitoring are not the same – there is guidance around this for DSLs at https://safefiltering.lgfl.net. There is also training available via National Online Safety: Filtering and Monitoring (Primary) and Filtering and Monitoring (Secondary)

What is this policy? H T

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' 2023 (KCSIE), 'Teaching Online Safety in Schools', statutory RSHE guidance and other statutory documents. It is cross-curricular (with relevance beyond Relationships, Health and Sex Education, Citizenship and Computing) and designed to sit alongside or be integrated into your school's statutory Child Protection & Safeguarding Policy. Any issues and concerns with online safety must always follow the school's safeguarding and child protection procedures.

Who is it for; when is it reviewed? H T

This policy should be a living document, subject to full annual review but also amended where necessary during the year in response to developments in the school and local area. Although many aspects will be informed by legislation and regulations, we will involve staff, governors, pupils/students and parents in writing and reviewing the policy and make sure the policy makes sense and it is possible to follow it in all respects. This will help ensure all stakeholders understand the rules that are in place and why, and that the policy affects day-to-day practice. Pupils/students could help to design a version in language their peers understand or help you to audit compliance. Acceptable Use Policies for different stakeholders help with this – ensure these are reviewed alongside this overarching policy. Any changes to this policy should be immediately disseminated to all the above stakeholders.

Who is in charge of online safety? T

KCSIE makes clear that "the designated safeguarding lead should take **lead** responsibility for safeguarding and child protection (including online safety)." The DSL can delegate activities but not the responsibility for this area and whilst subject leads, e.g. for RSHE will plan the curriculum for their area, it is important that this ties into a whole-school approach.

What are the main online safety risks in 2023/2024?

Current Online Safeguarding Trends

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: Such as online issues from What's app groups communications, Gaming communications between pupils and viewing and playing of over 18 games such as Grand Theft Auto, and Call of Duty.

Nationally, some of the latest trends of the past twelve months are outlined below. These should be reflected in this policy and the acceptable use agreements we use, and seen in the context of the 5 Cs (see KCSIE for more details), a whole-school contextual safeguarding approach that incorporates policy and practice for curriculum, safeguarding and technical teams.

We may be updating this policy during the year to reflect any changes resulting from the Online Safety Bill being passed into law.

Self-generative artificial intelligence has been a significant change, with students having often unfettered access to tools that generate text and images at home or in school. These tools not only represent a challenge in terms of accuracy when young people are genuinely looking for information, but also in terms of plagiarism for teachers and above all safety: none of the mainstream tools have end-user safety settings, most have an age limit of 13 or even 18 and in spite of basic rude words not delivering results, will easily produce inappropriate material. Schools not only need to tackle this in terms of what comes into school but also educating young people and their parents on use of these tools in the home.

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.

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.

PRIMARY SCHOOLS: 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).

SECONDARY SCHOOLS: Over 95 percent of students have their own mobile phone by the end of Year 7, and the vast majority do not have safety controls or limitations to prevent harm of access to inappropriate material. This is particularly pertinent given that 130,556 cases of self-generated child sexual abuse material were found of 11-13 year olds (Internet Watch Foundation Annual Report). These were predominantly (but importantly not only) girls; it is important also to recognise more and more older teenage boys being financially extorted after sharing intimate pictures online.

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 the 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.

Over the past year, there was a marked increase in the number of schools having issues with fights being filmed and shared, a disturbing increase in the cases of self-harm and sexual abuse being coerced with threats of violence (many even in primary schools).

There has been a significant increase in the number of fake profiles causing issues in schools, both for schools – where the school logo and/or name have been used to share inappropriate content about students and also spread defamatory allegations about staff, and also for students, including where these are used to bully others (sometimes even pretending to be one student to bully a second student).

How will this policy be communicated? H T

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
- Part of school induction pack for all new staff (including temporary, supply and non-classroom-based staff and those starting mid-year)
- 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/students and parents/carers (which must be in accessible language appropriate to these groups), which will be issued to whole school community, on entry to the school, annually and whenever changed, plus displayed in school

Contents

Overview

Aims HEART

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

- Setting out expectations for all school 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)

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 our Child Protection & 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.

Scope

This policy applies to all members of our school community (including teaching, supply and support 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.

Roles and responsibilities

Our 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/students, 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.

Depending on their role, all members of the school community should **read the relevant section in Annex A of this document** that describes individual roles and responsibilities. Please note there is one for All Staff which must be read even by those who have a named role in another section. There are also pupil/student, governor, etc role descriptions in the annex.

In 2023/2024, it is vital that all members understand their responsibilities and those of others when it comes to filtering and monitoring. All staff have a key role to play in feeding back on potential issues.

Education and curriculum HEART

It is important that schools establish a carefully sequenced curriculum for online safety that builds on what pupils/students have already learned and identifies subject content that is appropriate for their stage of development.

As well as teaching about the underpinning knowledge and behaviours that can help pupils/students navigate the online world safely and confidently regardless of the device, platform or app, Teaching Online Safety in Schools recommends embedding teaching about online safety and harms through a whole school approach and provides an understanding of these risks to help tailor teaching and support to the specific needs of pupils/students, including vulnerable pupils/students.

RSHE guidance also recommends schools assess teaching to "identify where pupils need extra support or intervention [through] tests, written assignments or self evaluations, to capture progress."

The following subjects have the clearest online safety links (see the relevant role descriptors above for more information):

- Relationships education, relationships and sex education (RSE) and health (also known as RSHE or PSHE)
- 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, supporting curriculum/stage/subject leads, and making the most of unexpected learning opportunities as they arise (which have a unique value for pupils/students).

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 (ask your DSL what appropriate filtering and monitoring policies are in place). “Parents and carers are likely to find it helpful to understand what systems schools use to filter and monitor online use. It will be especially important for parents and carers to be aware of what their children are being asked to do online, including the sites they will be asked to access and be clear who from the school or college (if anyone) their child is going to be interacting with online” (KCSIE 2023).

Equally, all staff should carefully supervise and guide pupils/students when engaged in learning activities involving online technology (including, extra-curricular, extended school activities if relevant and remote teaching), supporting them with search skills, critical thinking (e.g. disinformation, misinformation and fake news), age appropriate materials and signposting, and legal issues such as copyright and data law.

Handling safeguarding concerns and incidents H E

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; safeguarding is often referred to as a jigsaw puzzle, so all stakeholders should err on the side of talking to the online-safety lead / designated safeguarding lead to contribute to the overall picture or highlight what might not yet be a problem.

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 (primarily in the first key document):

- Safeguarding and Child Protection Policy
- Anti-Bullying Policy
- Behaviour Policy (including school sanctions)
- Acceptable Use Policies
- Data Protection Policy, agreements and other documentation (e.g. privacy statement and consent forms for data sharing, image use etc)
- ICT Regulations

This school commits to take all reasonable precautions to ensure safeguarding pupils online, but recognises that incidents will occur both inside school and outside school (and that those from outside school will continue to impact pupils/students when they come into school or during extended periods away from 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 complaint is referred to the Chair of Governors and the LADO (Local Authority’s Designated Officer). Staff may also use the NSPCC Whistleblowing Helpline 0800 028 0285.

Our school will actively seek support from other agencies as needed (i.e. Trust DSL, the local authority, SIL, UK Safer Internet Centre’s Professionals’ Online Safety Helpline (POSH), NCA CEOP, Prevent Officer, Police, IWF and Harmful Sexual Behaviour Support Service).

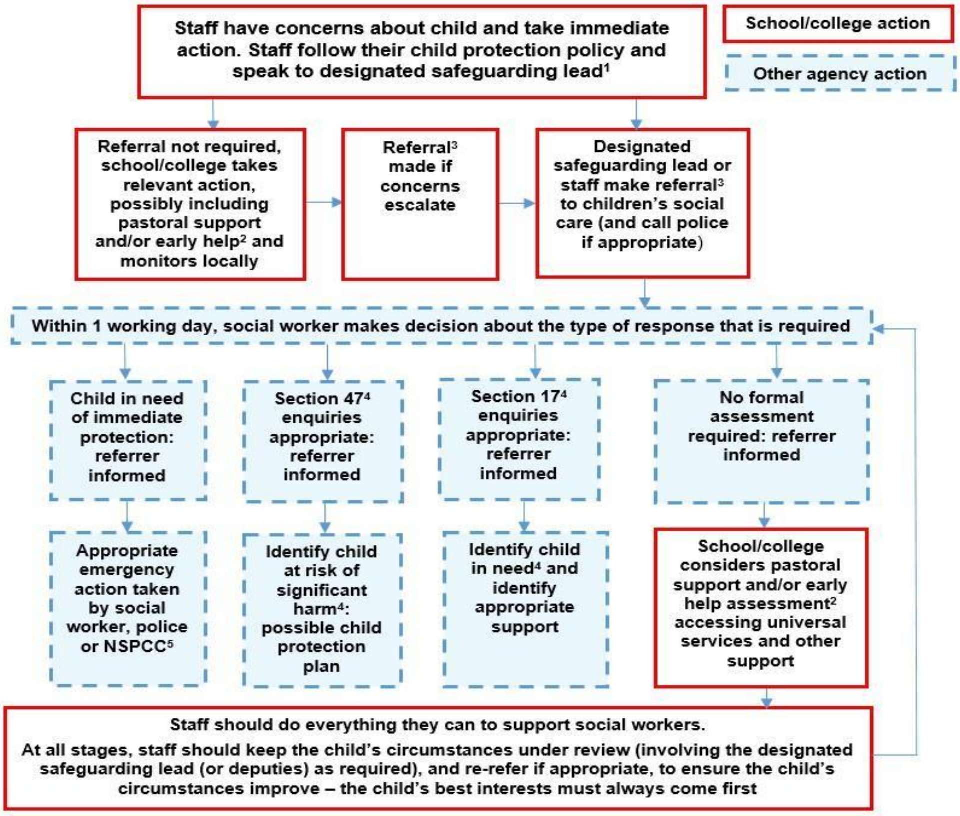
The DfE guidance Behaviour in Schools, advice for headteachers and school staff September 2022 provides advice and related legal duties including support for pupils and powers of staff when responding to incidents – see pages 32-34 for guidance on child on child sexual violence and harassment, behaviour incidents online and mobile phones.

We will inform parents/carers of online-safety incidents involving their children, and the Police where staff or pupils/students 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; see section below).

Our school evaluates whether reporting procedures are adequate for any future closures/lockdowns/isolation etc and make alternative provisions in advance where these might be needed.

Actions where there are concerns about a child HT

The following flow chart is taken from page 22 of Keeping Children Safe in Education 2022 as the key education safeguarding document. As outlined previously, online safety concerns are no different to any other safeguarding concern.

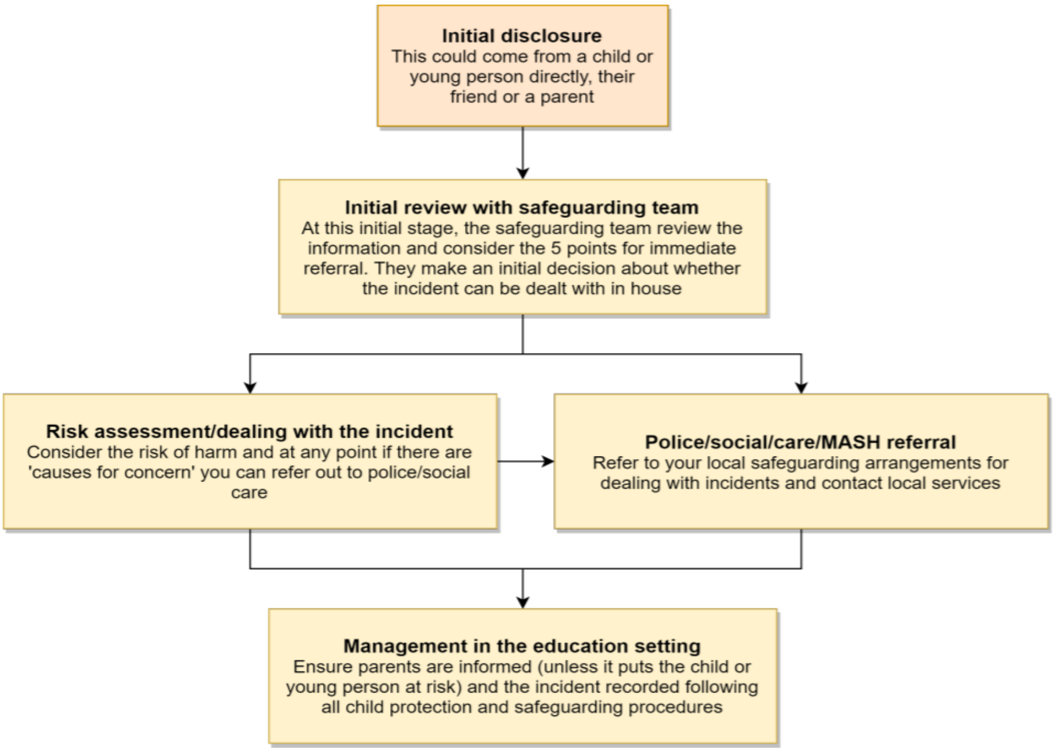

Staff have concerns about child and take immediate action. Staff follow their child protection policy and speak to designated safeguarding lead[1]
School/college action
Other agency action
Referral not required, school/college takes relevant action, possibly including pastoral support and/or early help[2] and monitors locally
Referral[3] made if concerns escalate
Designated safeguarding lead or staff make referral[3] to children's social care (and call police if appropriate)
Within 1 working day, social worker makes decision about the type of response that is required
Child in need of immediate protection: referrer informed
Section 47[4] enquiries appropriate: referrer informed
Section 17[4] enquiries appropriate: referrer informed
No formal assessment required: referrer informed
Appropriate emergency action taken by social worker, police or NSPCC[5]
Identify child at risk of significant harm[4]: possible child protection plan
Identify child in need[4] and identify appropriate support
School/college considers pastoral support and/or early help assessment[2] accessing universal services and other support
Staff should do everything they can to support social workers.
At all stages, staff should keep the child's circumstances under review (involving the designated safeguarding lead (or deputies) as required), and re-refer if appropriate, to ensure the child's circumstances improve – the child's best interests must always come first

Sexting – sharing nudes and semi-nudes HT

All schools (regardless of phase) 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.

Our 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.



Initial disclosure
This could come from a child or young person directly, their friend or a parent

Initial review with safeguarding team
At this initial stage, the safeguarding team review the information and consider the 5 points for immediate referral. They make an initial decision about whether the incident can be dealt with in house

Risk assessment/dealing with the incident
Consider the risk of harm and at any point if there are 'causes for concern' you can refer out to police/social care

Police/social/care/MASH referral
Refer to your local safeguarding arrangements for dealing with incidents and contact local services

Management in the education setting
Ensure parents are informed (unless it puts the child or young person at risk) and the incident recorded following all child protection and safeguarding procedures

***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 HET

Online bullying, including incidents that take place outside school or from home 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, including issues arising from banter.

It is important to be aware that in the past 12 months there has been an increase in anecdotal reports of fights being filmed and fake profiles being used to bully children in the name of others. When considering bullying, staff will be reminded of these issues.

Materials to support teaching about bullying and useful Department for Education guidance and case studies are at bullying.lgfl.net

Child-on-child sexual violence and sexual harassment HET

Part 5 of Keeping Children Safe in Education covers 'Child-on-child sexual violence and sexual harassment' and it would be useful for all staff to be aware of many aspects outlined there to support a whole-school response; case studies are also helpful for training.

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 and maintain an attitude of 'it could happen here'. 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 perpetuate. The document makes specific reference to behaviours such as bra-strap flicking and the careless use of language.

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.

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).

These are defined in the relevant Acceptable Use Policy as well as in this document, for example in the sections relating to the professional and personal use of school platforms/networks/clouds, devices and other technology, as well as to BYOD (bring your own device) policy.

Where pupils/students 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.

It will be necessary to reinforce these as usual at the beginning of any school year but also to remind pupils/students that **the same applies for any home learning** that may take place in future periods of absence/ closure/quarantine etc.

Further to these steps, our 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.

The new responsibilities for filtering and monitoring, led by the DSL and following the new DfE standards, may mean that more such incidents will be discovered in the coming year.

Social media incidents HT

See the social media section later in this document for rules and expectations of behaviour for children and adults in the school community. These are also governed by school Acceptable Use Policies.

Breaches will be dealt with in line with the school behaviour policy (for pupils/students) or code of conduct/handbook (for staff).

Further to this, 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, POSH, (run by the UK Safer Internet Centre) for support or help to accelerate this process.

Data protection and cybersecurity H

All pupils, staff, governors, volunteers, contractors and parents are bound by the school's data protection policy and our Trust's ICT Regulations. It is important to remember that there is a close relationship between both data protection and cybersecurity and a school's ability to effectively safeguard children. Schools are reminded of this in KCSIE which also refers to the DfE Standards of Cybersecurity for the first time in 2023.

Schools should remember that data protection does not prevent, or limit, the sharing of information for the purposes of keeping children safe. As outlined in *Data protection in schools*, 2023, "It's not usually necessary to ask for consent to share personal information for the purposes of safeguarding a child." And in KCSIE 2023, "The Data Protection Act 2018 and UK GDPR do not prevent the sharing of information for the purposes of keeping children safe. Fears about sharing information must not be allowed to stand in the way of the need to safeguard and promote the welfare and protect the safety of children."

Appropriate filtering and monitoring H

Keeping Children Safe in Education has long asked schools to ensure "appropriate filtering and monitoring" systems which keep children safe online but not "overblock".

Since KCSIE 2023, in recognition of the importance of these systems to keeping children safe, the designated safeguarding lead now has lead responsibility for filtering and monitoring (see page 1 for the DSL name and the named governor with responsibility for filtering and monitoring).

Schools are also asked to follow the new DfE filtering and monitoring standards, which require them to:

- identify and assign roles and responsibilities to manage filtering and monitoring systems
- review filtering and monitoring provision at least annually
- block harmful and inappropriate content without unreasonably impacting teaching and learning
- have effective monitoring strategies in place that meet their safeguarding needs

As schools get to grips with these new standards, the challenge for DSLs and SLT is to better understand, review and drive the rationale behind decisions in this area. Tech teams and safeguarding teams will need to work much more closely together for this to be possible and technicians will be charged to carry out regular checks and feed back to DSL teams.

ALL STAFF need to be aware of the changes and renewed emphasis and play their part in feeding back about areas of concern, potential for pupils/students to bypass systems and any potential overblocking. They can submit concerns at any point via email and will be asked for feedback at the time of the regular checks which will now take place.

Staff will be reminded of the systems in place and their responsibilities at induction and start of year safeguarding as well as via AUPs and regular training reminders in the light of the annual review and regular checks that will be carried out.

It is very important that schools understand the difference between filtering and monitoring, the meaning of overblocking and other terms, as well as how to get the best out of systems. There are guidance videos and flyers to help with this at https://safefiltering.lgfl.net and training is provided for all staff / safeguarding teams / technical teams as appropriate.

At our school:

- web filtering and web monitoring is provided by Techminder -on school site and
- changes can be made by K Mowbray HT, K Wall DHT, K Holcroft SBM
- overall responsibility is held by the
- technical support and advice, setup and configuration are from Tech minder

- regular checks are made half termly by Techminder and DSL to ensure filtering is still active and functioning everywhere. These are evidenced BY report to Governors
- an annual review is carried out by DSL/Trust and Tech minder

According to the DfE standards, "a variety of monitoring strategies may be required to minimise safeguarding risks on internet connected devices and may include:

- physically monitoring by staff watching screens of users
- live supervision by staff on a console with device management software
- network monitoring using log files of internet traffic and web access
- individual device monitoring through software or third-party services

At our school, we use Sophos Firewall SFOS, provided BY TECH Minder company (SEE appendix for details)

Messaging/commenting systems (incl. email, learning platforms & more)

Authorised systems

- Pupils/students at our school communicate with each other and with staff using Class dojo only, children do not use email.
- Staff at this school use the e-mail system provided by our Trust for all school e-mails. They **never use a personal/private email account or other personal/private messaging platform** to communicate with children or parents, or to colleagues when relating to school/child data, using a non-school-administered system. Staff are permitted to use this e-mail system to communicate with parents, external organisation but not with under 18s.

- Staff at this school use Class dojo to communicate with parents and we also use Teacher to Parents software to email and text.

- Any systems above are 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/students 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 Trust Corporate Services Director, Data Protection Officer, 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 a private account is used for communication or to store data by mistake, the DSL/Headteacher/Data Protection Lead/DPO (the particular circumstances of the incident will determine whose remit this is) should be informed immediately.

Behaviour / usage principles HEART

- More detail for all the points below are given in the Social media section of this policy as well as the school's acceptable use agreements, behaviour policy and staff code of conduct. Appropriate behaviour is expected at all times, and the system should not be used to send inappropriate materials or language which is or could be construed as bullying, aggressive, rude, insulting, illegal or otherwise inappropriate, or which (for staff) might bring the school into disrepute or compromise the professionalism of staff.
- Data protection principles will be followed at all times when it comes to all school communications, in line with the school Data Protection Policy and only using the authorised systems mentioned above.
- Pupils/students and staff are allowed to use the e-mail system for reasonable (not excessive, not during lessons) personal use but should be aware that all use is monitored, their e-mails may be read and the same rules of appropriate behaviour apply at all times. E-mails using inappropriate language, images, malware or to adult sites may be blocked and not arrive at their intended destination and will be dealt with according to the appropriate policy and procedure.

Online storage or learning platforms HT

All the principles outlined above also apply to any system to which you log in online to conduct school business, whether it is to simply store files or data (an online 'drive') or collaborate, learn, teach, etc.

For all these, it is important to consider data protection and cybersecurity before adopting such a platform or service and at all times when using it. Our school has a clear data protection policy which staff, governors and volunteers must follow at all times.

School website HEART

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 and Governors have delegated the day-to-day responsibility of updating the content of the website and ensuring compliance with DfE stipulations to School Business Manager. Our Trust provides a website audit document which our school uses to ensure compliance.

The website is managed and hosted by E Schools.

Where staff submit information for the website, they are asked to remember that schools have the same duty as any person or organisation to respect and uphold copyright law – schools have been fined thousands of pounds for copyright breaches. Sources must always be credited and material only used with permission. There are many open-access libraries of public-domain images/sounds etc that can be used. Finding something on Google or YouTube does not mean that copyright has been respected. If in doubt, check with Alson Tennant Trust or K Mowbray Head Teacher.

Digital images and video

When a pupil/student 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 (beyond internal assessment, which does not require express consent) and for how long. In Year 8, and at which point all students are aged 12+, consent is sought directly from the student if they have the relevant capacity and maturity to understand what they are agreeing to. Parents/carers and students (12+) answer as follows:

- For displays around the school
- For the newsletter
- For use in paper-based school marketing
- For online prospectus or websites
- For social media
- For a specific high-profile image for display or publication

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

Any pupils/students shown in public facing materials are rarely identified with more than first name. Occasionally, a pupil/student may be holding a certificate of achievement or work they have produced it this possibility is detailed in our consent forms. Photo file names/tags are checked to make sure they 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/students, and where these are stored. At our school, members of staff may occasionally (i.e. only when school devices are temporarily not available or there are insufficient devices) use personal phones to capture photos or videos of pupils/students, but these will be appropriate, linked to school activities, taken without secrecy and not in a one-to-one situation, and always moved to school storage as soon as possible, after which they are deleted from personal devices or cloud services.

Photos are stored on the school network in line with the retention schedule and 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. Further detail on this can be found in the Data Protection Policy.

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/students 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/students 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/students 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 H T

Our SM presence

Our school 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.

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.

Safeguarding Governor Mr S Roberts Tighe with support from the SBM, is responsible for managing our social media accounts and checking our Wikipedia and Google reviews and other mentions online.

Staff, pupils'/students' and parents' SM presence HT

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/students 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/students and parents, also undermining staff morale and the reputation of the school (which is important for the pupils/students we serve).

Many social media platforms have a minimum age of 13 (note that WhatsApp is 16+), and schools regularly deal 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. It is worth noting that Online Harms regulation is likely to require more stringent age verification measures 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 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).

Although our school has official social media accounts and will respond to general enquiries about the school, we ask parents/carers not to use these channels, especially not to communicate about their children or to make requests for information (subject access and Freedom of Information Requests).

E-mail 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.

Where social media is more widely used as part of school life, e.g. if a Facebook class group is allowed, then at least a second unrelated teacher will be part of the group to monitor activity between the teacher and students

Pupils/students are not allowed[1] to be 'friends' with or make a friend request[2] to any staff, governors, volunteers and contractors or otherwise communicate via social media.

[1] 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/student or staff member to the school).

[2] 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).

Pupils/students 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 pupil/student accounts.

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.

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

The statements of the Acceptable Use Policies (AUPs) which all members of the school community have signed are also relevant to social media activity, as is the school's Data Protection Policy.

Device usage H

AUPs remind those with access to school devices about rules on the misuse of school technology – devices used at home should be used just like if they were in full view of a teacher or colleague. Please read the following in conjunction with those AUPs and the sections of this document which impact upon device usage, e.g. 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** are allowed to bring mobile phones to school for emergency use only, these are handed in at the start of the day and stored in class basket and/or school office. **Smartwatches are not allowed in our school**. Important messages and phone calls to or from parents can be made at the school office, which will also pass on messages from parents to pupils/students in emergencies.
- **All staff who work directly with children** should leave their mobile phones on silent and only use them in private staff areas during school hours. See also the 'Digital images and video' section of this document and the school data protection policies. 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/Carers** are asked to leave their phones in their pockets and turned off when they are on site. They should ask permission before taking any photos, e.g. of displays in corridors or classrooms, and avoid capturing other children. When at school events, please refer to the Digital images and video section of this document. Parents are asked not to call pupils/students on their mobile phones during the school day; urgent messages can be passed via the school office.

Use of school devices

Staff and pupils/students are expected to follow the terms of the school acceptable use policies for appropriate use and behaviour when on school devices, whether on site or at home.

School devices are not to be used in any way which contravenes AUPs, behaviour policy / staff code of conduct.

WiFi is accessible for use of BYOD, guest networks and school-related internet use within the framework of the acceptable use policy. All such use is monitored.

School devices for staff or pupil/students are restricted to the apps/software installed by the school, whether for use at home or school, and may be used for learning and reasonable as well as appropriate personal use.

All and any usage of devices and/or systems and platforms may be tracked.

Trips / events away from school H

For school trips/events away from school, teaching staff will be issued with a school duty phone and this number will be 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. Teaching staff using their personal phone in an emergency will ensure that the number is hidden to avoid a parent or pupil/student accessing a member of staff's private phone number.

Searching and confiscation H

In line with the DfE guidance '[Searching, screening and confiscation: advice for schools]', the Headteacher and staff authorised by them have a statutory power to search pupils/students 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.

Full details of the school's search procedures are available in the school Behaviour Policy.

Appendix – Roles

Please read the relevant roles & responsibilities section from the following pages.

All school staff must read the "All Staff" section as well as any other relevant to specialist roles

Roles:

- All Staff
- Headteacher
- Designated Safeguarding Lead
- Governing Body, led by Online Safety / Safeguarding Link Governor
- PSHE / RSHE Lead/s
- Computing Lead
- Subject leaders
- Network Manager/technician
- Data Protection Officer (DPO)
- Volunteers and contractors (including tutor)
- Pupils/students
- Parents/carers
- External groups including parent associations

All staff

All staff should sign and follow the staff acceptable use policy in conjunction with this policy, the school's main child protection policy, the safeguarding code for adults, staff handbook and relevant parts of Keeping Children Safe in Education to support a whole-school safeguarding approach.

This includes reporting any concerns, no matter how small, to the designated safeguarding lead as named in the AUP, maintaining an awareness of current online safety issues (see the start of this document for issues in 2023) and guidance (such as KCSIE), modelling safe, responsible and professional behaviours in their own use of technology at school and beyond and avoiding scaring, victim-blaming language.

Staff should also be aware of the new DfE standards and relevant changes to filtering and monitoring and play their part in feeding back about overblocking, gaps in provision or pupils bypassing protections.

Headteacher – Mrs K Mowbray

Key responsibilities:

- Foster a culture of safeguarding where online-safety is fully integrated into whole-school safeguarding
- Oversee and support the activities of the designated safeguarding lead team and ensure they work technical colleagues to complete an online safety audit in line with KCSIE (including technology in use in the school)

- Undertake training in offline and online safeguarding, in accordance with statutory guidance and Local Safeguarding Children Partnership support and guidance
- Ensure ALL staff undergo safeguarding training (including online-safety) at induction and with regular updates and that they agree and adhere to policies and procedures
- Ensure ALL governors and trustees undergo safeguarding and child protection training and updates (including online-safety) to provide strategic challenge and oversight into policy and practice and that governors are regularly updated on the nature and effectiveness of the school's arrangements. *LDST has procured online safety training via National Online Safety.*
- 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 remote systems are implemented according to child-safety first principles
- Better understand, review and drive the rationale behind decisions in filtering and monitoring as per the new DfE standards—through regular liaison with technical colleagues and the DSL– in particular understand what is blocked or allowed for whom, when, and how as per KCSIE. LGfL's Safeguarding Shorts: Filtering for DSLs and SLT twilight provides an overview.
    - In 2023/4 this will involve starting regular checks and annual reviews, upskilling the DSL and appointing a filtering and monitoring governor
- 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
- Support safeguarding leads and technical staff as they review protections for pupils in the home and remote-learning procedures, rules and safeguards.
- 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 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
- 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 the school website meets statutory requirements

Designated Safeguarding Lead / Online Safety Lead – Mrs K Mowbray

Key responsibilities (remember the DSL can delegate certain online-safety duties but not the overall responsibility; this assertion and all quotes below are from Keeping Children Safe in Education):

- The DSL should "take **lead responsibility** for safeguarding and child protection (**including online safety and understanding the filtering and monitoring** systems and processes in place).
- Ensure "An effective whole school approach to online safety as per KCSIE

- In 2023/4 working to take up the new responsibility for filtering and monitoring by working closely with technical colleagues, SLT and the new filtering governor to learn more about this area, better understand, review and drive the rationale behind systems in place and initiate regular checks and annual reviews, including support for devices in the home. LGfL's Safeguarding Shorts: Filtering for DSLs and SLT twilight provides a quick overview and there is lots of information for DSLs at safefiltering.lgfl.net and appropriate.lgfl.net
- Where online-safety duties are delegated and in areas of the curriculum where the DSL is not directly responsible but which cover areas of online safety (e.g. RSHE), ensure there is regular review and open communication and that the DSL's clear overarching responsibility for online safety is not compromised or messaging to pupils confused
- Ensure ALL staff and supply staff undergo safeguarding and child protection training (including online-safety) at induction and that this is regularly updated.
    - In 2023/4 this must include filtering and monitoring and help them to understand their roles
    - all staff must read KCSIE Part 1 and all those working with children also Annex B – translations are available in 13 community languages at kcsietranslate.lgfl.net (B the condensed Annex A can be provided instead to staff who do not directly work with children if this is better)
    - cascade knowledge of risks and opportunities throughout the organisation
    - safecpd.lgfl.net has helpful CPD materials including PowerPoints, videos and more
- Ensure that ALL governors and trustees undergo safeguarding and child protection training (including online-safety) at induction to enable them to provide strategic challenge and oversight into policy and practice and that this is regularly updated – LGfL's Safeguarding Training for school governors is free to all governors at safetraining.lgfl.net
- Take day-to-day responsibility for safeguarding issues and be aware of the potential for serious child protection concerns
- Be mindful of using appropriate language and terminology around children when managing concerns, including avoiding victim-blaming language - see spotlight.lgfl.net for a resource to use with staff on how framing things linguistically can have a safeguarding impact, and some expressions we use might be unhelpful
- Remind staff of safeguarding considerations as part of a review of remote learning procedures and technology, including that the same principles of online-safety and behaviour apply
- Work closely with SLT, staff and technical colleagues to complete an online safety audit (including technology in use in the school) – see LGfL's template with questions to use at onlinesafetyaudit.lgfl.net
- Work with the headteacher, DPO and governors to ensure a 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 safeguarding and "undertake Prevent awareness training." – see safetraining.lgfl.net and prevent.lgfl.net
- 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 – see safeblog.lgfl.net for examples or sign up to the LGfL safeguarding newsletter
- Ensure that online-safety education is embedded across the curriculum in line with the statutory RSHE guidance (e.g. by use of the updated UKCIS framework 'Education for a Connected World – 2020 edition') and beyond, in wider school life
- Promote an awareness of and commitment to online-safety throughout the school community, with a strong focus on parents, including hard-to-reach parents – dedicated resources at parentsafe.lgfl.net
- Communicate regularly with SLT and the safeguarding governor/committee to discuss current issues (anonymised), review incident logs and filtering/change control logs and discuss how filtering and monitoring work and have been functioning/helping.
- 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.
- Ensure adequate provision for staff to flag issues when not in school and for pupils to disclose issues when off site, especially when in isolation/quarantine, e.g. a survey to facilitate disclosures and an online form on the school home page about 'something that worrying me' that gets mailed securely to the DSL inbox
- Ensure staff adopt a zero-tolerance, whole school approach to all forms of child-on-child abuse, and don't dismiss it as banter (including bullying).
- Pay particular attention to **online tutors**, both those engaged by the school as part of the DfE scheme who can be asked to sign the contractor AUP, and those hired by parents.

Governing Body, led by Online Safety / Safeguarding Link Governor – Mr S Roberts Tighe

Key responsibilities (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) Online safety in schools and colleges: Questions from the Governing Board
- Undergo (and signpost all other governors and Trustees to attend) safeguarding and child protection training (including online safety) at induction to provide strategic challenge and into policy and practice, ensuring this is regularly

updated – LGfL's Safeguarding Training for school governors is free to all governors at safetraining.lgfl.net

- Ensure that all staff also receive appropriate safeguarding and child protection (including online) training at induction and that this is updated
- Appoint a filtering and monitoring governor to work closely with the DSL on the new filtering and monitoring standards - there is guidance for governors at safefiltering.lgfl.net
- 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 coordinator / DSL and incorporate online safety into standing discussions of safeguarding at governor meetings
- Work with the DPO, DSL and headteacher to ensure a 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 B
- Ensure that all staff undergo safeguarding and child protection training (including online safety and now also reminders about filtering and monitoring
- "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."

PSHE / RSHE Lead/s – Mrs K Wall DHT

Key responsibilities:

- As listed in the 'all staff' section, plus:
- Embed consent, mental wellbeing, healthy relationships and staying safe online as well as raising awareness of the risks and challenges from recent trends in self-generative artificial intelligence, financial extortion and sharing intimate pictures 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." - training is available at safetraining.lgfl.net]
- Focus on the underpinning knowledge and behaviours outlined in Teaching Online Safety in Schools in an age appropriate way to help pupils to navigate the online world safely and confidently regardless of their device, platform or app.
- Assess teaching to "identify where pupils need extra support or intervention [through] tests, written assignments or self evaluations, to capture progress" – to complement the computing curriculum,.

- Work closely with the DSL/OSL and all other staff to ensure an understanding of the issues, approaches and messaging within PSHE / RSHE.
- Note that an RSHE policy should be included on the school website.
- Work closely with the Computing subject leader to avoid overlap but ensure a complementary whole-school approach, and with all other lead staff to embed the same whole-school approach

Computing Lead – SLT inc Mrs K Mowbray HT

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 RSHE lead to avoid overlap but ensure a complementary whole-school approach
- 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 Leaders

Key responsibilities:

- As listed in the 'all staff' section, plus:
- Look for opportunities to embed online safety in your subject or aspect, especially as part of the RSHE curriculum, 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 Manager/other technical support roles – Techminder company

Key responsibilities:

- As listed in the 'all staff' section, plus:
- Collaborate regularly with the DSL and leadership team to help them make key strategic decisions around the safeguarding elements of technology.
- Note that KCSIE changes expect a great understanding of technology and its role in safeguarding when it comes to filtering and monitoring and in 2023/4

you will be required to support safeguarding teams to understand and manage these systems and carry out regular reviews and annual checks.

- Support DSLs and SLT to carry out an annual online safety audit as now recommended in KCSIE. This should also include a review of technology, including filtering and monitoring systems (what is allowed, blocked and why and how 'over blocking' is avoided as per KCSIE) to support their role as per the new DfE standards, protections for pupils in the home and remote-learning.
- 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 / RSHE lead to ensure that school systems and networks reflect school policy and there are no conflicts between educational messages and practice.
- 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
- 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.
- Ensure the data protection policy and cybersecurity policy are up to date, easy to follow and practicable
- 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
- Work with the Headteacher to ensure the school website meets statutory DfE requirements (the technical team is likely to play at least some role in working with the web team).

Trust Data Protection Officer (DPO): Alison Tennant / School Designated Data Protection Lead – Mrs K Mowbray HT

Key responsibilities:

- Alongside those of other staff, provide data protection expertise and training and support the DP and cybersecurity policy and compliance with those and legislation and ensure that the policies conform with each other and with this policy.
- Not prevent, or limit, the sharing of information for the purposes of keeping children safe. As outlined in *Data protection in schools*, 2023, "It's not usually necessary to ask for consent to share personal information for the purposes of safeguarding a child." And in KCSIE 2023, "The Data Protection Act 2018 and

UK GDPR do not prevent the sharing of information for the purposes of keeping children safe. Fears about sharing information must not be allowed to stand in the way of the need to safeguard and promote the welfare and protect the safety of children."

- Note that retention schedules for safeguarding records may be required to be set as very long term need (minimum of 25 years). Those child protection records that relate to an allegation or a case of child sexual abuse need to be kept until the individual is 75 years old – the LDST Retention Policy sets out the retention period.
- Ensure that all access to safeguarding data is limited as appropriate, and also monitored and audited

Volunteers and contractors (including tutor)

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
- Maintain an awareness of current online safety issues and guidance
- Model safe, responsible and professional behaviours in their own use of technology at school and as part of remote teaching or any online communications
- Note that as per AUP agreement a contractor will never attempt to arrange any meeting, **including tutoring session,** without the full prior knowledge and approval of the school, and will never do so directly with a pupil. The same applies to any private/direct communication with a pupil.

Pupils

Key responsibilities:

Read, understand, sign and adhere to the student/pupil acceptable use policy

Parents/carers

Key responsibilities:

- Read, sign and adhere to the school's parental acceptable use policy (AUP), read the pupil AUP and encourage their children to follow it

External groups including parent associations – Glazebury CE PTA

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

Appendix: Filtering Provider Checklist Reponses

Schools in England (and Wales) are required “to ensure children are safe from terrorist and extremist material when accessing the internet in school, including by establishing appropriate levels of filtering”. Furthermore, the Department for Education’s statutory guidance ‘Keeping Children Safe in Education’ obliges schools and colleges in England to “ensure appropriate filters and appropriate monitoring systems are in place*” and they “should be doing all that they reasonably can to limit children’s exposure to the above risks from the school’s or college’s IT system*” however, schools will need to “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.”

Included within the Scottish Government national action plan on internet safety, schools in Scotland are expected to “have policies in place relating to the use of IT and to use filtering as a means of restricting access to harmful content.”

It is important to recognise that no filtering systems can be 100% effective and need to be supported with good teaching and learning practice and effective supervision.

Company / Organisation	Techminder Limited
Address	Beech House, 23 Ladies Lane, Hindley, Wigan, WN2 2QA
Contact details	Support@techminder.co.uk
Filtering System	Sophos Firewall SFOS
Date of assessment	15/03/2023

System Rating response

Where a supplier is able to confirm that their service fully meets the issue identified in a specific checklist the appropriate self-certification colour for that question is GREEN.	🟩
Where a supplier is not able to confirm that their service fully meets the issue identified in a specific checklist question the appropriate self-certification colour for that question is AMBER.	🟧

Illegal Online Content

Filtering providers should ensure that access to illegal content is blocked, specifically that the filtering providers:

Aspect	Rating	Explanation
● Are IWF members	🟩	Yes, Sophos is a member of the Internet Watch Foundation and routinely works with the IWF and other agencies in helping to identify the methods used by child abusers to share content, reporting the discovery of child abuse images online
● and block access to illegal Child Abuse Images (by actively implementing the IWF URL list)	🟩	Yes, Sophos actively implements the IWF CAIC list.
● Integrate the 'the police assessed list of unlawful terrorist content, produced on behalf of the Home Office'	🟩	Yes, Sophos actively integrates the police assessed list of unlawful terrorist content, produced on behalf of the Home Office

Inappropriate Online Content

Recognising that no filter can guarantee to be 100% effective, providers should both confirm, and describe how, their system manages the following content

Content	Explanatory notes – Content that:	Rating	Explanation
Discrimination	Promotes the unjust or prejudicial treatment of people on the grounds of race, religion, age, or sex.	🟩	Sophos provides an "Intolerance and Hate" category to enable blocking of sites that foster racial supremacy or vilify/discriminate against groups or individuals. **Techminder blocks this category**.
Drugs / Substance abuse	displays or promotes the illegal use of drugs or substances	🟩	Sophos provides "Controlled Substances", "Marijuana" and "Legal Highs" categories that enable blocking of sites providing information about or promoting the use, trade or manufacture of drugs. **Techminder blocks these categories.**
Extremism	promotes terrorism and terrorist ideologies, violence or intolerance	🟩	Sophos provides an "Intolerance and Hate" category to enable blocking of sites that promotes terrorism and terrorist ideologies, violence or intolerance. **Techminder blocks this category.**

Malware / Hacking	promotes the compromising of systems including anonymous	🟩	Sophos provides “Anonymizers”, “Hacking, Phishing and Fraud”,

	browsing and other filter bypass tools as well as sites hosting malicious content	🟩	“Spam URLs” and “Spyware and Malware” categories. Sophos recommends blocking these categories. In addition, all unencrypted content is scanned for malware. A cloud-delivered sandbox analyses any downloaded active content and blocks malware. **Techminder blocks this category.**
Pornography	displays sexual acts or explicit images	🟩	Sophos provides “Sexually Explicit”, “Nudity” and “Extreme” categories. Sophos recommends blocking these categories. Also, Sophos provides “Safe-Search” enforcement on the major search engines. The option is also available to add a “Creative Commons” license that only shows images published under Creative Commons licensing laws. To date, using this method has not resulted in any pornographic images being forwarded to Sophos for reclassification. **Techminder blocks this category and enforces Safe Search on all major search engines.**
Piracy and copyright theft	includes illegal provision of copyrighted material	🟩	Sophos provides “Peer to peer and torrents” and “intellectual piracy” categories. **Techminder blocks this category.**
Self Harm	promotes or displays deliberate self harm (including suicide and eating disorders)	🟩	Sophos provides the “Pro-suicide and self-harm” category. **Techminder blocks this category**.
Violence	Displays or promotes the use of physical force intended to hurt or kill	🟩	Sophos provides “Extreme” and “Criminal Activity” categories. **Techminder blocks these categories**, to block sites displaying or promoting the use of physical force intended to hurt or kill.

This list should not be considered an exhaustive list. Please outline how the system manages this content and many other aspects

Sophos currently provides 91 different URL categories. For the full list see: https://www.sophos.com/threat-center/reassessment-request/utm.aspx. Sophos Labs enables us to dynamically update our web categories by providing a URL categorisation services that integrate Sophos URL data with that of multiple third-party suppliers, including IWF and CTIRU, to provide a market-leading database. Sophos classifies sites at the IP level, domain, sub-domain and path URL data is constantly reviewed and unclassified websites

via a cloud delivered service to the Sophos appliance (Physical, Virtual or in Public Cloud), so they are always up-to-date with the latest classifications for sites.

Regarding the duration and extent of logfile (Internet history) data retention, providers should outline their retention policy, specifically including the extent to the identification of individuals and the duration to which all data is retained .

Sophos Firewall retain reports on box for up to a year. This is potentially impacted by disk space which is checked during the scoping phase by Techminder. As the disk reaches its maximum capacity it will delete the eldest records. Therefore, if the box has additional work to do that wasn’t covered in the scoping its possible that the retention phase is reduced. It is possible to choose to use Central Reporting which would give 30 days of reporting with an XGS Xstream license, with increased licensing blocks available for purchase to meet a schools retention needs or purchase additional data storage packs for longer storage on

Providers should be clear how their system does not over block access so it does not lead to unreasonable restrictions

Sophos category database protects more than 400,000 organizations in more than 150 countries. The huge amount of data helps Sophos to fine tune our web filtering policies based on the typical activities of users in different settings. Sophos also provides tools that enable customers to create custom categories that over-ride current URL database classifications and end-users to request page reclassification, by the system administrator, directly from the block page. Further to this Techminder can tweak web filtering policies to make sure they are enabling their staff and students to be the best and brightest they can be. Safe in the knowledge that they are also helping keep our users safe online.

Filtering System Features

How does the filtering system meet the following principles:

Principle	Rating	Explanation

● Age appropriate, differentiated filtering – includes the ability to vary filtering strength appropriate to age and role	🟩	Techminder applies policy rules based on group information. If the school includes objects related to age then policies can be created that open certain categories of websites once a certain age has been reached (e.g. the "Sex Education" category. Sophos also logs all user group activity separately for reporting. Reports can be generated for a specific event in a specific user group. All alerts can be sent using syslog into a Security Incident and Event Management system (SIEM).
● Circumvention – the extent and ability to identify and manage technologies and techniques used to circumvent the system, specifically VPN, proxy services and DNS over HTTPS.	🟩	Sophos provides the "Anonymizers' category in our web filter. This policies would block users from being able to circumvent our filtering **Techminder blocks this category**
● Control - has the ability and ease of use that allows schools to control the filter themselves to permit or deny access to specific content	🟩	The day-to-day administration of the Sophos Firewall appliance is done by Techminder (Sophos Partner). There is complete flexibility in the policy model to create policies that can block categories, file types, URLs, IPs and much more. Policies can be created easily and intuitively using a very user-friendly interface.
● Contextual Content Filters – in addition to URL or IP based filtering, the extent to which (http and https) content is analysed as it is streamed to the user and blocked. For example, being able to contextually analyse text on a page and dynamically filter	🟩	The Sophos Firewall includes a content scanning feature, whereby URLs and web pages are dynamically analysed for specific keywords or phrases. Techminder can upload multiple keyword lists to support different languages and provide better granularity. Any pages matching words or phrases contained within the keyword lists can be blocked and/or logged. In addition, Administrators/Safeguarding officers can review the blocked keywords using the onboard log viewer and determine the context.
● Filtering Policy – the filtering provider publishes a rationale that details their approach to filtering with classification and categorisation as well as over blocking	🟩	Sophos provides the rationale behind its web classification so that accurate choices can be made by Techminder and the School. This information can be found here: https://support.sophos.com/support/s/article/KB-000036518?language=en_US

● Group / Multi-site Management – the ability for deployment of central policy and central oversight or dashboard	🟩	Sophos provides a central management console that enables you to manage multiple site based (MAT for example) Firewalls in one console. Central policy can be configured and pushed out to your different sites. Whilst reporting and alerting can all be managed centrally
● Identification - the filtering system should have the ability to identify users	🟩	Sophos Firewall can identify users transparently via Single-Sign on or through integration with directory server login processes or via the Sophos Endpoint Protection Client. It can also provide non-transparent authentication where a user is required to login before browsing. Techminder sets the firewall to identify users transparently
● Mobile and App content – mobile and app content is often delivered in entirely different mechanisms from that delivered through a traditional web browser. To what extent does the filter system block inappropriate content via mobile and app	🟩	Sophos Firewall is able to filter all http and https connections including TLS 1.3 encrypted traffic. This is not limited to browser traffic and includes mobile and app connections. Sophos also provides policy-driven application control that can also identify and manage traffic that uses other protocols

technologies (beyond typical web browser delivered content)	🟩	
● Multiple language support – the ability for the system to manage relevant languages	🟩	Sophos Firewall supports multiple block pages to support multiple languages and custom block pages where multiple languages are required on the same page.
● Network level - filtering should be applied at ‘network level’ ie, not reliant on any software on user devices whilst at school (recognising that device configuration/software may be required for filtering beyond the school infrastructure)	🟩	Sophos Firewall can be deployed as a standalone web proxy or in transparent bridge or gateway mode **Techminder deploys Sophos Firewall in transparent mode.**
● Remote devices – with many children and staff working remotely, the ability for devices (school and/or personal) to receive school based filtering to a similar quality to that expected in school	🟩	For Windows and Mac devices that are not on the school network, web filtering can be enforced using our Sophos Central Endpoint protection client. This includes web control, which has specific policies for remote devices. These policies can be managed via Sophos Central (our Cloud management platform) and any violations can be reported on. There are over 48 categories that can be configured, as well as file type blocking. This includes sites that are on the IWF and Counter Terrorism Referral Unit block lists. Webfiltering on Chromebooks can also be controlled via Sophos Mobile (UEM Solution).
● Reporting mechanism – the ability to report inappropriate content for access or blocking	🟩	Sophos provides a number of built-in reports that can be used to see this information. These reports are fully customizable and can be emailed to admins/teachers/safeguarding officers. In addition, the log files can be exported using syslog to third party tools.
● Reports – the system offers clear historical information on the websites visited by your users	🟩	Sophos provides a number of built-in reports that can be used to see this information. In addition the log files can be exported using syslog to third party tools.

Filtering systems are only ever a tool in helping to safeguard children when online and schools have an obligation to “*consider how children may be taught about safeguarding, including online, through teaching and learning opportunities, as part of providing a broad and balanced curriculum”.*[1]

Please note below opportunities to support schools (and other settings) in this regard

[1] https://www.gov.uk/government/publications/keeping-children-safe-in-education--2

Sophos has introduced Sophos Home Premium (https://home.sophos.com). This provides home users access to enterprise-grade security software to block malware and enforce parental category controls for web traffic. In terms of education, Sophos in partnership with SWGFL has produced thousands of educational booklets that redistributed to schools nationwide to advise on online safety. Sophos organises student days where we invite students into our headquarters in Abingdon to learn how Sophos deals with the latest online threats and what students can do to protect themselves more effectively. Many universities use Sophos products as part of their curriculum to learn about filtering and antimalware

Techminder are Sophos certified and setup the Firewalls in line with Sophos and DfE best practices.

Review Schedule

Policy Author	Trust Data Protection Officer
Policy Approver	Trust Corporate Services Director
Current Policy Version	4.0
Policy Effective From	1st September 2023
Policy Review Date	31st August 2024

Revision Schedule

Version	Revisions	By whom
1.0	Original document produced	DPO
2.0	New version due to significant changes throughout the policy to bring it in line with KCSIE 2020 and COVID-19 remote learning/working requirements. DFO and IT Consultant reviewed and provided technical input.	DPO
2.1	Reviewed in line with KCSIE 2021 – updated throughout. Sexting section and references to sexting updated "sharing nudes and semi nudes", reviewed with consideration to the government's peer on peer sexual abuse investigation, IT support provider section added, all links to other documentation/guidance updated, appendices page changed to "Other documentation/guidance relevant to this policy", pupils changed to pupils/students throughout.	DPO
3.0	Reviewed in line with KCSIE 2022. Policy updated in many areas and sections moved around to make it easier to read. New version.	DPO
4.0	Major updates throughout the policy to reflect KCSIE 2023.	DPO