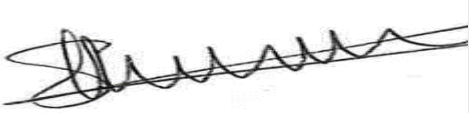
WEAVERS FEDERATION PRIMARY SCHOOLS

Stewart Headlam and Hague

Online Safety Policy - 2024/25

Document edition	Section	Details of Change
Colour Change	All sections	Change all the writing with color to black

Reviewed by	Date
SHH RESOURCES - Millie Otieno-Storey 	10/10/2024
Ratified by Chair of Governors	Date
 Sophie Fanning-Tichborne	23 January 2025

Contents

What's different about this policy for September 2024?

- Some content added about filming in and outside school, including parents not filming covertly.
- Some content added about the use of generative AI.
- Content added about filtering and monitoring - following on from last year's changes where DSL's take lead responsibility for web filtering and monitoring. DSL's need to understand, review and drive the rationale behind decisions in these areas - working closely with tech teams. Tech teams should carry out regular checks and feed back to DSL teams. there is guidance around this for DSLs at https://safefiltering.lgfl.net).

Introduction

Key people / dates

Federation of Stewart Headlam and Hague Schools	Designated Safeguarding Lead (DSL), with lead responsibility for filtering and monitoring	[Judy Knappett – Executive Headteacher]
	Deputy Designated Safeguarding Leads / DSL Team Members	Alison Goodliffe – Head of Hague Nilufar Chowdhury – Head of Stewart Headlam Alison Goodliffe: Online Safety lead
	Link governor for safeguarding	Emily Wright – Safeguarding Officer
	Curriculum leads with relevance to online safeguarding and their role	Computing Lead: Ekram Ali PSHE Lead: Moin Ahmed + Kelly Hitchins
	Network manager / other technical support	Afzal Hussain – Connetix
	Date this policy was reviewed and by whom	8th October 2024. Alison Goodliffe
	Date of next review and by whom	September 2025 Alison Goodliffe

What is this policy?

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' 2024 (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?

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 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. Acceptable Use Policies (see appendices) for different stakeholders help with this and 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?

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 computing and 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 2024/2025?

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:

- Children sharing / copying login details and leaving unkind messages.
- Bullying / unkind messages about both staff and pupils online.
- Children sharing self-generated videos on personal Tik Tok / You Tube accounts.
- Children playing or watching inappropriate games, content online. This often leads to children using inappropriate language in school and is an indication of unsupervised / unfiltered access to online content.
- Children discussing online influencers, including misogynistic influencers such as Andrew Tate.

Nationally, some of the latest trends of the past twelve months are outlined below. These are 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 become rapidly more accessible, 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 (gen AI can be responsible for incorrect and sometimes harmful 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. Self-generative AI has also made it easier than ever to create sexualised images and deepfake video. Whilst they may not be real, they have a devastating effect on a young person's emotional wellbeing and physical safety, and can also be used to blackmail, humiliate and abuse. The Internet Watch Foundation has reported AI generated imagery of child sexual abuse progressing at such a worrying rate.
- Ofcom's 'Children and parents: media use and attitudes report 2024' 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 (especially with the minimum age for use of WhatsApp now 13). With children aged 3 - 17 spending an average of 3 hours and 5 minutes per day online, four in ten parents report finding it hard to control their child's screen time. Notably, 45% of 8-11s feel their parents' screen time is too high, underlining the importance of modelling good behaviour.
- Given the 13+ minimum age requirement on most social media platforms, it is notable that half (51%) of children under 13 use them. Despite age restrictions, four in ten admit to giving a fake age online, exposing them to content inappropriate for their age and increasing their risk of harm, with over a third (36%) of parents of all 3-17s saying they would allow their child to have a profile on sites or apps before they had reached the minimum age.

- 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 will remind about best practice while remembering the reality for most of our students is quite different.

- This is striking when you consider that 25% 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 remains the fastest growing for this form of child sexual abuse material.

- 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 facts or veracity of influencers sharing news. The alarming speed and scale at which misinformation about the attack in Southport (August 2024) was shared, resulting in Islamophobic and racist violence, rioting and looting across England is particularly concerning, with much of it fuelled by false online accusations about the

assailant. Despite attempts by Police and national news to correct the misleading information, it racked up millions of views on social media sites like X and was actively promoted by several high-profile users with large followings.

- There have also been significant safeguarding concerns where parents have filmed interactions with staff outside the school gates and posted this on social media, putting children and the wider school community at risk of harm. See nofilming.lgfl.net to find out more.
- Cyber Security is an essential component in safeguarding children and now features within KCSIE. Sadly, the education sector remains a clear target for cyber-attacks, with the Cyber Security Breaches Survey 2024 highlighting an increase in school attacks nationally, with 71% of secondary schools reporting a breach or attack in the past year, and 52% of primary schools.

How will this policy be communicated?

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

- Posted on the SHH Federation school website
- Available on the internal staff drive
- Available in paper format in each of the school staffrooms
- 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 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

Overview

Aims

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

- Setting out expectations for all Federation of Stewart Headlam and Hague Schools 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 your 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).

Beyond this, **reporting.lgfl.net** has a list of curated links to external support and helplines for both pupils and staff, including the Professionals' Online-Safety Helpline from the UK Safer Internet Centre and the NSPCC Report Abuse Helpline for sexual harassment or abuse, as well as hotlines for hate

crime, terrorism and fraud which might be useful to share with parents, and anonymous support for children and young people. Training is also available via **safetraining.lgfl.net**

Scope

This policy applies to all members of the Federation of Stewart Headlam and Hague Schools 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

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

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, governor, etc role descriptions in the annex.

In 2024/2025, 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

Despite the risks associated with being online, Hague and Stewart Headlam schools recognise the opportunities and benefits of children being online. Technology is a fundamental part of our adult lives and so developing the competencies to understand and use it, are critical to children's later positive outcomes. The choice to use technology in school will always be driven by pedagogy and inclusion.

SHH Federation have established a carefully sequenced curriculum for online safety that builds on what pupils 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 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, including vulnerable pupils – dedicated training around this with curriculum mapping for computing, RSHE/PSHE and online safety leads is available at safetraining.lgfl.net

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." [See LGfL's SafeSkills Online Safety Quiz and diagnostic teaching tool which is linked to statements from UKCIS Education for a Connected World framework, enabling teachers to monitor progress throughout the year and drill down to school, class and pupil level to identify areas for development at **safeskillsinfo.lgfl.net**]

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)

Whenever overseeing the use of technology (devices, the internet, generative AI tools, 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 tasks. This includes supporting them with search skills, reporting and accessing help, critical thinking (eg. disinformation, misinformation and fake news), access to age appropriate materials and signposting, and legal issues such as copyright and data law. safesources.lgfl.net has regularly updated theme-based resources, materials and signposting for teachers and parents.

At the Federation of Stewart Headlam and Hague schools, we recognise that online safety and broader digital resilience must be thread throughout the curriculum and that is why we are working to adopt the cross-curricular framework 'Education for a Connected World – 2020 edition' from UKCIS (the UK Council for Internet Safety).

Annual reviews of curriculum plans / schemes of work (including for SEND pupils) are used as an opportunity to follow this framework more closely in its key areas. This is done within the context of an annual online safety audit, which is a collaborative effort led by Alison Goodliffe.

Handling safeguarding concerns and incidents

It is vital that all staff recognise that online safety is a part of safeguarding (as well as being a curriculum strand of Computing, PSHE/RSHE and Citizenship).

General concerns must be handled in the same way as any other safeguarding concern; 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 including, Sexual Harassment / Child-on-Child Abuse Policy.
- Anti-Bullying Policy
- Behaviour Policy (including school sanctions)
- Acceptable Use Policies (see Appendixes at the end of this policy)
- Prevent Policy / Risk Assessment
- Data Protection Policy, agreements and other documentation (e.g. privacy statement and consent forms for data sharing, image use etc)
- Cybersecurity [there are templates at elevate.lgfl.net]

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 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 (you may want to display a poster with details of this / other helplines in the staff room – see posters.lgfl.net and reporting.lgfl.net).

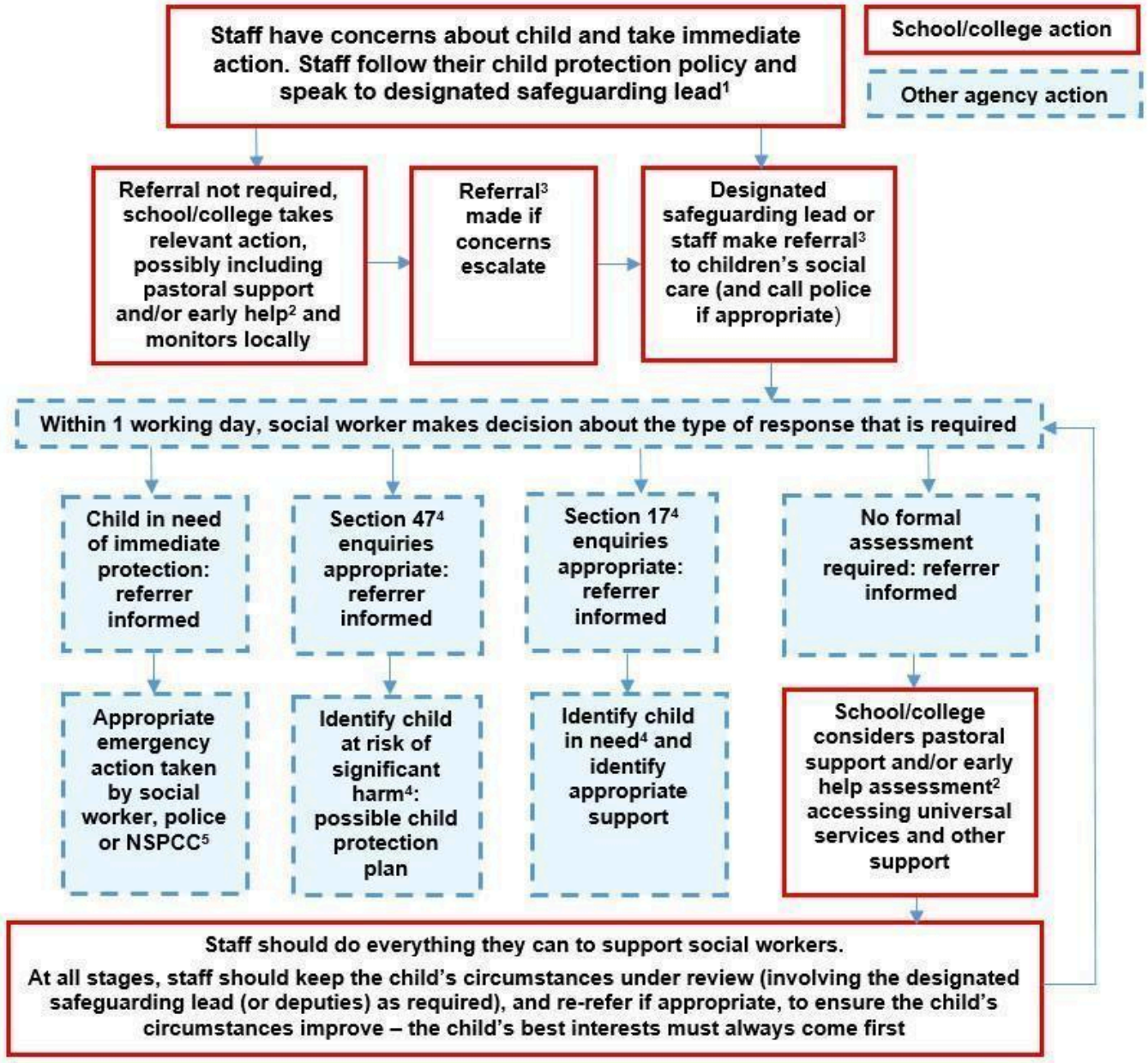
The school will actively seek support from other agencies as needed (i.e. the local authority, LGfL, UK Safer Internet Centre's Professionals' Online Safety Helpline (POSH), NCA CEOP, Prevent Officer, Police, IWF and Harmful Sexual Behaviour Support Service). The DfE guidance Behaviour in Schools, advice for headteachers and school staff September 2024 provides advice and related legal duties including support for pupils and powers of staff when responding to incidents – see pages 31-33 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 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).

The school should evaluate whether reporting procedures are sustainable for any unforeseen periods of closure.

Actions where there are concerns about a child – see SHH Federation Child Protection Posters from Safeguard and Child Protection policy which are displayed in each school.

The following flow chart (it cannot be edited) 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.



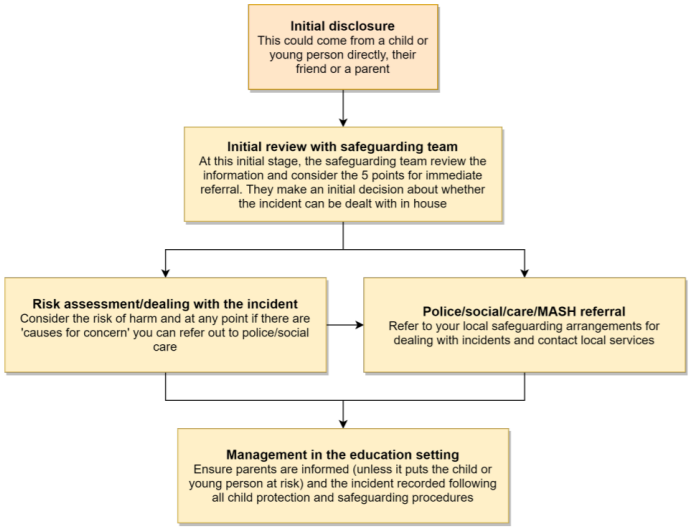
Sexting – sharing nudes and semi-nudes

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.

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.**

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. The UKCIS guidance seeks to avoid unnecessary criminalisation of children.

The school DSL will in turn use the full guidance document, Sharing nudes and semi-nudes – advice for educational settings to decide next steps and whether other agencies need to be involved. See flow chart below from UKCIS guidance.



***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

The documents referenced above and materials to support teaching about sexting can be found at nudes.lgfl.net

Upskirting

It is important that everyone understands that upskirting (taking a photo of someone under their clothing, not necessarily a skirt) is now a criminal offence and constitutes a form of sexual harassment as highlighted in Keeping Children Safe in Education. As with other forms of child on child abuse pupils/students can come and talk to members of staff if they have made a mistake or had a problem in this area.

Bullying

Online bullying, 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 not to treat online bullying separately to offline bullying and to recognise that much bullying will often have both online and offline elements.

It is important to be aware that sometimes fights are being filmed, live streamed or shared online and fake profiles are 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

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. In our schools there have been incidents of children referring to Andrew Tate as a role model, and staff need to monitor children's behaviours carefully.

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 Policies (See Appendixes to this document) as well as throughout 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 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 that **the same applies for any home learning** that may take place in future periods of absence/ closure/quarantine etc.

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

Social media incidents

See the social media section later in this document for rules and expectations of behaviour for children and adults in the SHH Federation community.

Breaches will be dealt with in line with the school behaviour policy (for pupils) 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, the schools 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.

Extremism

The schools have obligations relating to radicalisation and all forms of extremism under the Prevent Duty. Staff will not support or promote extremist organisations, messages or individuals, give them a voice or opportunity to visit the school, nor browse, download or send material that is considered offensive or of an extremist nature. We ask for parents' support in this also, especially relating to social media, where extremism and hate speech can be widespread on certain platforms.

Data protection and cybersecurity

All pupils, staff, governors, volunteers, contractors and parents are bound by the school's data protection (Information Governance Policy) and cybersecurity policy. 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.

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 2024, "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

The designated safeguarding lead (DSL) - Judy Knappett, has lead responsibility for filtering and monitoring and works closely with Connetix and Alison Goodliffe (online Safety Lead) to implement the DfE filtering and monitoring standards which require schools 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

We look to provide "appropriate filtering and monitoring" as outlined win Keeping Children Safe in Education at all times.

We ensure ALL STAFF are aware of filtering and monitoring systems and play their part in feeding back about areas of concern, potential for students to bypass systems and any potential overblocking. They can submit concerns at any point via CPOMS and will be asked for feedback at the time of the regular checks which will now take place.

Technical and safeguarding colleagues work together closely to carry out annual reviews and checks to ensure that the schools respond to issues and integrate issues within our curriculum.

We carry out termly checks to ensure all systems are in operation, functioning as expected, etc and an annual review as part of an online safety audit of strategy and approach. More details of both documents and results are available on request from Alison Goodliffe.
We use templates from LGFL for this documentation. https://safefiltering.lgfl.net or https://onlinesafetyaudit.lgfl.net

Safe search is enforced on any accessible search engines on all devices.

Our You Tube mode is: open for staff users and blocked for pupils.

School devices loaned to pupils are protected through LGFL Home Protect.

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.

The DSL checks filtering reports and notifications monthly and takes any necessary action.

According to the DfE standards, “a variety of monitoring strategies may be required to minimise safeguarding risks on internet connected devices.

At SHH Federation , we use :

- Physical monitoring by staff watching the screens of users.
- Teachers carefully select resources for younger children and teach older children how to use appropriate resources and make sensible choices. Children are taught strategies to report anything that worries them online.
- When pupils log into google classroom from home on a school or personal device, activity may be monitored through our Gsuite.
- We are hoping to install SENSO through LGFL during the year to monitor pupil use of devices which create automatic alerts for search terms causing concern.

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

Authorised systems

- Pupils at this school communicate with each other and with staff using Google Classroom. Pupils in older classes also have access to Education gmail through google suite for education. Their accounts are restricted to emailing within school domains.
- Staff at Hague School use the email system provided by Education Gmail through google suite for education for all school emails.
- Staff at Stewart Headlam School use staffmail through LGFL for all school emails. They also have gmail education accounts through google suite for education.
- Staff never use a personal/private email account (or other messaging platform) to communicate with children or parents, or to colleagues when relating to school/child data, using a non-school-administered system. Staff are permitted to use this email system to communicate with other staff or professionals outside the school.
- When communicating with parents, emails should go through the admin team rather than directly from staff accounts. Teachers should not use their email accounts to send private messages to pupils.

- Staff or personal data should not be sent / shared or stored on email.

- Internally staff should use the school network or google drive to store or share data. This also facilitates the access of data remotely without the need for carrying sensitive data on memory sticks.
- If data needs to be shared with external agencies, USO-Fx and Egress systems are available through lgfl.

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 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 school SLT and centrally managed. A record of these will be kept centrally by the SLT.

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/DPO (the particular circumstances of the incident will determine whose remit this is) should be informed immediately.

Behaviour / usage principles

- 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.
- Staff are allowed to use the email system for reasonable (not excessive, not during lessons) personal use but should be aware that all use is monitored, their emails may be read and the same rules of appropriate behaviour apply at all times. Emails using inappropriate language, images, malware or to adult sites may be blocked and not arrive at their intended destination (and will be dealt with according to the appropriate policy and procedure). Pupils should only be using emails as directed by their class teachers.

Use of generative AI

At Stewart headlam and Hague Federation, we acknowledge that generative AI platforms (e.g. ChatGPT or Bard for text creation or the use of Co-Pilot or Adobe Firefly to create images and videos) are becoming widespread. We are aware of and follow the DfE's guidance on this. In particular:

- We will talk about the use of these tools with pupils, staff and parents – their practical use as well as their ethical pros and cons [insert more detail e.g. when/how/subject etc if available]

- We are aware that there will be use of these apps and exposure to AI creations on devices at home for some students – these experiences may be both positive/creative and also negative (inappropriate data use, misinformation, bullying, deepfakes, undressing apps).

- The use of any generative AI to plagiarise and cheat is prohibited, and the Behaviour Policy will be used for any pupil found doing so.

- In school, the use of AI is limited to teachers. Staff can request that certain resources are unblocked if they are required for lessons.

- The approval of new AI platforms will be made in consultation between the Computing Lead, class teachers and DSLs.

We are in the process of reviewing the use of AI in our curriculum and considering the skills that children need to be taught to use AI effectively and when this is appropriate.

We are in the process of reviewing the use of AI to reduce staff workload and will build in training for staff in the use of selected AI tools.

Online storage or learning platforms

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. SHH Federation has a clear cybersecurity and data protection policy which staff, governors and volunteers must follow at all times. Any new systems will be approved by the DSL.

School website

The school website is a key public-facing information portal for the school community (both existing and prospective stakeholders) with a key reputational value. The Executive Headteacher and Governors share the day-to-day responsibility of updating the content of the website and ensuring compliance

with DfE stipulations with the Heads of School. This is monitored annually using LGFL's audit at https://lgfl.net/safeguarding/school-website-rag-audit-tool.

The site is managed by / hosted by Debeer Digital.

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 Heads of School.

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. Parents answer as follows:

- For displays around the school
- For the school newsletter
- For use in paper-based school marketing
- For the school websites
- For Online learning platforms in the EYFS eg Tapestry
- For E1 partnership website
- For EHCP and medical needs.
- For use in Google classrooms.

For other uses, eg by visitors to the school or for wider publicity separate permission is obtained.

Whenever a photo or video is taken/made, the member of staff taking it will check the latest database before using it for any purpose. Photos should be taken using school devices and stored on school drives.

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

All staff are governed by their contract of employment and the school's Acceptable Use Policy, which covers the use of mobile phones/personal equipment for taking pictures of pupils, and where these are stored. At SHH Federation, staff should use a school digital device to capture photos or videos of pupils. Members of staff may occasionally use personal phones to capture photos or videos of pupils, 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 (NB – many phones automatically back up photos so staff should take care to ensure backups are deleted too).

Photos at Hague and Stewart Headlam are stored in the Hague or Stewart Headlam Google Drive. All are stored in line with the retention schedule of the school Data Protection Policy.

Staff and parents are reminded annually and at all school events about the importance of not sharing images on social media or otherwise 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 subject and a sample letter to parents for taking photos or videos at school events can be found at parentfilming.lgfl.net

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

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

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

Pupils are taught that they should not post images or videos of others without their permission. We teach them about the risks associated with providing information with images (including the name of the file), that reveals the identity of others and their location. We teach them about the need to keep their data secure and what to do if they / or a friend are subject to bullying or abuse.

Social media

Our SM presence

The SHH Federation 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.

Judy Knappett, Nilufar Chowdhury, Ekram Ali, Alison Goodliffe and John Waters are responsible for managing our X-Twitter account and checking our Wikipedia and Google reviews and other mentions online.

Staff, pupils' and parents' SM presence

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

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

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

Many social media platforms have a minimum age of 13, but the school occasionally deals with issues arising on social media involving pupils/students under the age of 13. We ask parents to respect age ratings on social media platforms wherever possible and not encourage or condone underage use.

However, the school has to strike a difficult balance of not encouraging underage use at the same time as needing to acknowledge reality in order to best help our pupils/students to avoid or cope with issues if they arise. Online safety lessons will look at social media and other online behaviour, how to be a good friend online and how to report bullying, misuse, intimidation or abuse. However, children will often learn most from the models of behaviour they see and experience, which will often be from adults.

Parents can best support this by talking to their children about the apps, sites and games they use (you don't need to know them – ask your child to explain it to you), with whom, for how long, and when (late at night / in bedrooms is not helpful for a good night's sleep and productive teaching and learning at school the next day). You may wish to refer to the Digital Family Agreement to help establish shared expectations and the Top Tips for Parents poster along with relevant items and support available from parentsafe.lgfl.net and introduce the Children's Commission Digital 5 A Day.

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

Email is the official electronic communication channel between parents and the school. Social media, including chat apps such as WhatsApp, are not appropriate for school use.

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

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

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

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

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

The serious consequences of inappropriate behaviour on social media are underlined by the fact that there has been a significant number of Prohibition Orders issued by the Teacher Regulation Agency to teaching staff that involved misuse of social media/technology.

All members of the school community are reminded that particularly in the context of social media, it is important to comply with the school policy on Digital images and video and permission is sought before uploading photographs, videos or any other information about other people. Parents must **not** covertly film or make recordings of any interactions with pupils or adults in schools or near the school gates, nor share images of other people's children on social media as there may be cultural or legal reasons why this would be inappropriate or even dangerous. The school sometimes uses images or videos of children for internal purposes such as recording attainment, but it will only do so publicly if parents have given consent on the relevant form.

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

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 in Year 5 & Year 6** are allowed to bring mobile phones in if they are walking home alone and parents request it. These must be handed in to the school office as pupils arrive in school and collected at the end of the day.

- Any attempt to use a phone in lessons without permission or to take illicit photographs or videos will be viewed in line with the school's behaviour policy and the withdrawal of mobile privileges.
- 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 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 cybersecurity 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 head teacher should be sought (the head teacher may choose to delegate this) and this should be done in the presence of a member staff.
- **Parents** 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.

Use of school devices

Staff and pupils 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.
School devices are loaned to some pupils. Parents sign an agreement when they borrow a device from school. This includes an undertaking to ensure that parental settings are activated on their wifi at home and that they will supervise pupils when they are online.
Wifi is accessible to staff and visitors to school for school-related internet use and limited personal use within the framework of the acceptable use policy. All such use is monitored. Visitors do not have access to school network or Google drives.

School devices for staff or 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

For school trips/events away from school, teachers will be asked to use the personal phones with number withheld for any authorised or emergency communications with pupils/students and parents. Where possible and appropriate communications with home will be via the school admin team. Any deviation from this policy (e.g. by mistake) will be notified immediately to the Headteacher. Teachers using their personal phone in an emergency will ensure that the number is hidden to avoid a parent or student accessing a teacher's private phone number.

Searching and confiscation

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

The LA safeguarding team will be informed if school believes a device has sexual images, pornography, violence or bullying. Staff should not view these images without LA guidance.

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/Principal
- Designated Safeguarding Lead
- Governing Body, led by Online Safety / Safeguarding Link Governor
- PSHE / RSHE Lead/s
- Computing Lead
- Subject / aspect leaders
- Network Manager/technician
- Data Protection Officer (DPO)
- Volunteers and contractors (including tutor)
- Pupils
- 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 safeguarding policy, the code of conduct/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 safety lead as named in the AUP, maintaining an awareness of current online safety issues (see the start of this document for issues in 2024) 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 DfE standards and relevant changes to filtering and monitoring and play their part in feeding back to the DSL and Online Safety Officer about overblocking, gaps in provision or pupils bypassing protections. All staff are also responsible for the physical monitoring of pupils’ online devices during any session / class they are working within.

Headteacher – [Judy Knappett]

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 with technical colleagues and the Online Safety officer to complete an online safety audit in line with KCSIE (including technology in use in the school) – [see LGfL's template with suggested questions at onlinesafetyaudit.lgfl.net]
- 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 [LGfL's Safeguarding Training for School Governors is free to all governors at safetraining.lgfl.net]
- 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 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]
- 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 [see remotesafe.lgfl.net]
- 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 [websiterag.lgfl.net can help you with this]

Designated Safeguarding Lead / Online Safety Lead – [Judy Knappett supported by Alison Goodliffe, Nilufar Chowdhury]

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
- Ensure the school is complying with the DfE's standards on Filtering and Monitoring. [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]
- As part of this, DSLs will work with technical teams to carry out reviews and checks on filtering and monitoring, to complete the relevant documentation and ensure that safeguarding and technology work together. This will include a decision on relevant youTube mode and preferred search engine/s, etc.
- 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.
    - 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, [template you can use at safepolicies.lgl.net with provisions] and those hired by parents. [share the Online Tutors – Keeping Children Safe poster at parentsafe.lgfl.net to remind parents of key safeguarding principles]

Governing Body, led by Online Safety / Safeguarding Link Governor – [Emily Wright]

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." [NB – you may wish to refer to 'Teaching Online Safety in Schools 2019' and investigate/adopt the UKCIS cross-curricular framework 'Education for a Connected World – 2020 edition' to support a whole-school approach]

PSHE / RSHE Lead/s – [Moin Ahmed / Kelly Hitchins]

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" – [see LGfL's SafeSkills Online Safety Quiz and diagnostic teaching tool at safeskillsinfo.lgfl.net] 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 – [Ekram Ali]

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 / aspect 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 – [Afzaal Hussain - Connetix]

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.
- Support safeguarding teams to understand and manage filtering and monitoring systems and carry out regular reviews and annual checks.[e.g. schoolprotect.lgfl.net and monitoring.lgfl.net. There is a free template available for filtering checks here- safefiltering.lgfl.net].
- Support DSLs and SLT to carry out an annual online safety audit as now recommended in KCSIE. [LGfL has a free template you can use at https://onlinesafetyaudit.lgfl.net] 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, [we recommend you signpost them to LGfL's Safeguarding Shorts: Filtering for DSLs and SLT twilight at safetraining.lgfl.net which provides a quick overview to help build their understanding] protections for pupils in the home [e.g. LGfL HomeProtect filtering for the home – https://homeprotect.lgfl.net] and remote-learning. [see remotesafe.lgfl.net for guidance]
- Keep up to date with the school's online safety policy and technical information in order to effectively carry out their online safety role and to inform and update others as relevant.
- Work closely with the designated safeguarding lead / online safety lead / data protection officer / LGfL nominated contact / 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
- Ensure filtering and monitoring systems work on new devices and services before releasing them to students and staff.
- 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 [: Sophos Anti-Virus, Sophos, Sophos InterceptX, Sophos, Egress, Meraki Mobile Device Management. These solutions which are part of your package will help protect the network and users on it]
- 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 [see website audit tool at websiterag.lgfl.net]

Data Protection Officer (DPO) [Connetix]

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 (until pupil is aged 25 or older)'. However, some local authorities require record retention until 25 for all pupil records. An example of an LA safeguarding record retention policy can be read at safepolicies.lgfl.net, but you should check the rules in your area.
- 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 –

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

SHH Federation Acceptable Use Policy - AUP for KS1 Pupils

My name is _____ Date: _____

1. I only **USE** devices or apps, sites or games if a trusted adult says so.
2. I **ASK** for help if I'm stuck or not sure.
3. I **TELL** a trusted adult if I'm upset, worried, scared or confused.
4. If I get a **FUNNY FEELING** in my tummy, I talk to an adult.
5. I look out for my **FRIENDS** and tell someone if they need help.
6. I **KNOW** people online aren't always who they say they are and things I read online are not always **TRUE.**
7. Anything I do online can be shared and might stay online **FOREVER.**
8. **I don't keep SECRETS** unless they are a present or a nice surprise.
9. I don't have to do **DARES AND CHALLENGES** even if someone tells me I have to .
10. I don't change **CLOTHES** or get undressed in front of a camera **.**
11. I always **check before SHARING** personal information.
12. I am **KIND and polite** to everyone.

My trusted adults are:

_____ at school

_____ at home

SHH Federation Acceptable Use Policy (AUP) for KS2 Pupils

My name is _____ Year _____

These statements can keep me and others safe & happy at school and home

1.	**I learn online**	I use the school's internet, devices and logins for schoolwork, homework and other activities to learn and have fun.
2	**I behave the same way on devices as face to face in the classroom**.	I don't behave differently when I'm learning at home, so I don't say or do things I wouldn't do in the classroom, nor do teachers or tutors. If I get asked or told to do anything that I would find strange in school, I will tell another teacher.
3	**I ask permission**	At home or school, I only use the devices, apps, sites and games I am allowed to and when I am allowed to.
4	**I am creative online**	I don't just spend time on apps, sites and games looking at things from other people. I get creative to learn and make things, and I remember my Digital 5 A Day.
5	**I am a good friend online**	I won't share or say anything that I know would upset another person or they wouldn't want shared. If a friend is worried or needs help, I remind them to talk to an adult, or even do it for them.
6	**I am not a bully**	I do not post, make or share unkind, hurtful or rude messages or comments and if I see it happening I will tell my trusted adults.
7	**I am a secure online learne**r	I keep my passwords to myself and reset them if anyone finds them out. Friends don't share passwords!
8	**I am careful what I click on**	I don't click on unexpected links or popups, and only download or install things when I know it is safe or has been agreed by trusted adults. Sometimes app add-ons can cost money, so it is important I always check.
9	**I ask for help if I am scared or worried**	I will talk to a trusted adult if anything upsets me or worries me on an app, site or game – it often helps. If I get a funny feeling, I talk about it.
10	**I am honest**	I know it's not my fault if I see or someone sends me something bad – I won't get in trouble, but I mustn't share it. If I make a mistake, I don't try to hide it but ask a trusted adult for help.
11	**I communicate and collaborate online**	with people I already know and have met in real life or that a trusted adult knows about.
12	**I never pretend to be someone else online.**	It can be upsetting or even dangerous.
13	**I am careful when someone wants to be my friend online**	I know new online friends might not be who they say they are. Unless I have met them face to face, I can't be sure who they are.
14	**I check with a parent/carer before I meet an online friend the first time** I never go alone.	

15	**I don't do live videos on my own**	and always check if it is allowed. I check with a trusted adult before I video chat with anybody for the first time.
16	**I keep my body to myself online**	I never get changed or show what's under my clothes when using a device with a camera. I remember my body is mine and no-one should tell me what to do with it; I don't send any photos or videos without checking with a trusted adult.
17	**I don't take photos or videos of people without their permission.**	I never film fights or people when they are upset or angry. I always ask people's permission before sharing their image - they may not like the picture.
18	**I say no online if I need to**	I don't have to do something just because someone dares or challenges me to do it, or to keep a secret. If I get asked anything that makes me worried, upset or just confused, I should say no, stop chatting and tell a trusted adult immediately.
19	**I tell my parents/carers what I do online**	They might not know the app, site or game, but they can still help me when things go wrong, and they want to know what I'm doing.
20	**I follow age rules**	13+ games and apps aren't good for me so I don't use them – they may be scary, violent or unsuitable. 18+ games are not more difficult or skilled but very unsuitable.
21	**I am private online**	I only give out private information if a trusted adult says it's okay. This might be my address, phone number, location or anything else that could identify me or my family and friends; if I turn on my location, I will remember to turn it off again.
22	**I am careful what I share and protect my online reputation**	I know anything I do can be shared and might stay online forever (even on Snapchat or if I delete it).
23	**I am a rule-follower online**	I know that apps, sites and games have rules on how to behave, and some have age restrictions. I follow the rules, block bullies and report bad behaviour, at home and at school.
24	**I am part of a community**	I do not make fun of anyone or exclude them because they are different to me. If I see anyone doing this, I tell a trusted adult and/or report it.
25	**I respect people's work**	I only edit or delete my own digital work and only use words, pictures or videos from other people if I have their permission or if it is copyright free.
26	**I am a researcher online**	I use safe search tools approved by my trusted adults. I know I can't believe everything I see online. I know how to double check information I find. If I am not sure, I ask a trusted adult.

I have read and understood this agreement. If I have any questions, I will speak to a trusted adult:

My trusted adults are: _____

Signed: _____ Date: _____

SHH Federation Acceptable Use Policy - AUP for Parents / Carers

We ask all adults in school and all children in KS2 to read and sign an Acceptable Use Policy (AUP) to outline how we expect them to behave when they are online or using school devices both in school and at home.

We tell your children that **they should not behave any differently when they are out of school or using their own device or on a home network.** What we tell pupils about behaviour and respect applies to all members of the school community, whether they are at home or school. We seek the support of parents and carers to reinforce this message and help children to behave in a safe way when online:

"Treat yourself and others with respect at all times; treat people in the same way when you are online or on a device as you would face to face."

Where can I find out more?

You can read Stewart Headlam and Hague's Federation full Online Safety Policy on our websites. If you have any questions about this AUP or our approach to online safety, please speak to Alison Goodliffe or Nilufar Chowdhury.

What am I agreeing to?

1. I understand that SHH Federation uses technology as part of the daily life of the school when it is appropriate to support teaching & learning and the smooth running of the school, and to help prepare the children and young people in our care for their future lives.
2. I understand that the school takes every reasonable precaution to keep pupils safe and to prevent pupils from accessing inappropriate materials, including through behaviour policies and agreements, physical and technical monitoring, education and support and web filtering to restrict inappropriate material.
3. School network protections will be superior to most home filtering. However, please note that accessing the internet always involves an element of risk and the school cannot be held responsible for the nature and content of materials accessed through the internet and mobile technologies. Schools are asked not to overblock or provide an experience which is so locked down as to block educational content or not train pupils for life in an online world.

4. I understand that internet and device use in school, and use of school-owned devices, networks and cloud platforms out of school is subject to filtering and monitoring. More detail of this can be found in our online safety policy.
5. I understand and will help my child to use any devices at home in the same manner as when in school, including during any remote learning periods.
6. I understand that my child might be contacted online on Google classroom by teachers or TAs who work in their class about their learning, wellbeing or behaviour. If they are contacted by someone else or staff ask them to use a different app to chat, they will tell another teacher.
7. I will promote positive online safety and model safe, responsible and positive behaviours in my 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.
8. The impact of social media use is often felt strongly in schools, which is why we expect certain behaviours from pupils when using social media. I will support the school's social media policy and not encourage my child to join any platform where they are below the minimum age.
9. I will follow the school's guidance on when I can capture and/or share images/videos. I will not share images of other people's children on social media and understand that there may be cultural or legal reasons why this would be inappropriate or even dangerous. The school sometimes uses images/video of my child for internal purposes such as recording attainment, but it will only do so publicly if I have given my consent on the relevant form.
10. I will not covertly film or make recordings or any interactions with pupils or adults in schools. If I wish to make any recording, I will obtain permission from the Head of School.
11. I understand that for my child to grow up safe online, s/he will need positive input from school and home, so I will talk to my child about online safety and refer to parentsafe.lgfl.net for advice and support on safe settings, parental controls, apps and games, talking to them about life online, screentime and relevant topics from bullying to accessing pornography, extremism and gangs, sharing inappropriate content etc...
12. I understand that my child needs a safe and appropriate place to do home learning, whether for homework or during times of school closure. When on any video calls with school, my child will be fully dressed and not in bed, and the camera angle will point away from beds/bedding/personal information etc. Where it is possible to blur or change the background, I will help my child to do so.
13. If my child has online tuition, I will refer to the Online Tutors – Keeping children Safe poster and undertake necessary checks where I have arranged this privately, ensuring they are registered/safe and reliable, and for any tuition to remain in the room where possible, ensuring my child knows that tutors should not arrange new sessions or online chats directly with them.

14. I understand that whilst home networks are much less secure than school ones, I can apply child safety settings to my home internet and to various devices, operating systems, consoles, apps and games. There are also child-safe search engines e.g. swiggle.org.uk and YouTube Kids is an alternative to YouTube with age appropriate content. Find out more at parentsafe.lgfl.net
15. I understand that it can be hard to stop using technology sometimes, and I will talk about this to my child, and refer to the principles of the Digital 5 A Day: childrenscommissioner.gov.uk/our-work/digital/5-a-day/
16. I understand and support the commitments made by my child in the Acceptable Use Policy (AUP) which s/he has signed, and I understand that s/he will be subject to sanctions if s/he does not follow these rules.
17. I can find out more about online safety at SHH Federation by reading the full Online Safety Policy on the website and can talk to class teachers if I have any concerns about my child/ren's use of technology, or about that of others in the community, or if I have questions about online safety or technology use in school.

~~~~~~~~~~~~~~~~~~~~

I/we have read, understood and agreed to this policy.

Signature/s: _____

Name/s of parent / guardian: _____

Parent / guardian of: _____

Date: _____

What is an AUP?

We ask all children, young people and adults involved in the life of Stewart Headlam and Hague Federation to sign an Acceptable Use* Policy (AUP), which outlines how we expect them to behave when they are online, and/or using school networks, connections, internet connectivity and devices, cloud platforms and social media (both when on school site and outside of school).

This AUP is reviewed annually, and I will be asked to sign it upon entry to the school and every time changes are made.

Why do we need an AUP?

All staff, governors and volunteers have particular legal / professional obligations and it is imperative that all parties understand that online safety is part of safeguarding as well as part of the curriculum, and it is everybody's responsibility to uphold the school's approaches, strategy and policy as detailed in the full Online Safety Policy.

Where can I find out more?

All staff, governors and volunteers should read Stewart Headlam and Hague Federation's full Online Safety Policy for more detail on our approach to online safety and links to other relevant policies (e.g. Safeguarding Policy, Behaviour Policy, etc).

If you have any questions about this AUP or our approach to online safety, please speak to Alison Goodliffe or Nilufar Chowdhury.

What am I agreeing to?

1. **(This point is for staff and governors):** I have read and understood Hague and Stewart Headlam's full Online Safety policy and agree to uphold the spirit and letter of the approaches outlined there, both for my behaviour as an adult and enforcing the rules for pupils/students. I will report any breaches or suspicions (by adults or children) in line with the policy without delay as outlined in the Online Safety Policy.

2. I understand online safety is a core part of safeguarding and part of everyone's job. It is my duty to support a whole-school safeguarding approach and to learn more each year about best-practice in this area. I have noted the section in our online safety policy which describes trends over the past year at a national level and in this school.

3. I will report any behaviour which I believe may be inappropriate or concerning in any way to the Designated Safeguarding Lead (if by a child) or Headteacher/Principal (if by an adult) and make them aware of new trends and patterns that I identify.

4. I will follow the guidance in the Safeguarding and Online Safety policies for reporting incidents (including for handling incidents and concerns about a child in general, sharing nudes and semi-nudes, upskirting, bullying, sexual violence and harassment, misuse of technology and social media)

5. I understand the principle of 'safeguarding as a jigsaw' where my concern or professional curiosity might complete the picture; online-safety issues (particularly relating to bullying and sexual harassment and violence) are most likely to be overheard in the playground, corridors, toilets and other communal areas outside the classroom. understand the sections on.

1. I will take a zero-tolerance approach to all forms of child-on-child abuse (not dismissing it as banter), including bullying and sexual violence & harassment – know that 'it could happen here'!
2. I will be mindful of using appropriate language and terminology around children when addressing concerns, including avoiding victim-blaming language.

3. I will identify opportunities to thread online safety through all school activities as part of a whole school approach in line with the RSHE curriculum, 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).

4. When overseeing the use of technology in school or for homework or remote teaching, I will encourage and talk with pupils about appropriate behaviour and how to get help and consider potential risks and the age-appropriateness of websites (find out what appropriate filtering and monitoring systems are in place and how they keep children safe).

5. I will check with a DSL if I want to use any new platform of app that has not already been approved by the school, to ensure this is quality assured.

6. I will follow best-practice pedagogy for online safety education, avoiding scaring and other unhelpful prevention methods. [onlinesafetyprinciples.lgfl.net]

7. I will prepare and check all online sources and classroom resources **before** using them, for accuracy and appropriateness. I will flag any concerns about "overblocking" to the DSL.

8. I will carefully supervise and guide pupils when engaged in learning activities involving online technology, supporting them with search skills, critical thinking, age-appropriate materials and signposting, and legal issues such as copyright and data protection.

9. I will physically monitor pupils using online devices in the classroom to ensure appropriate and safe use.

10. During any periods of remote learning, I will not behave any differently towards students compared to when I am in school and will follow the same safeguarding principles as outlined in the main child protection and safeguarding policy when it comes to behaviour, ways to contact and the relevant systems and behaviours.

11. I understand that school systems and users are protected by security, monitoring and filtering services, and that my use of school devices, systems and logins on my own devices and at home (regardless of time, location or connection), including encrypted content, can be monitored/captured/viewed by the relevant authorised staff members.
12. I know the filtering and monitoring systems used within school and the types of content blocked and am aware of the increased focus on these areas in KCSIE. If I discover pupils or

adults may be bypassing blocks or accessing inappropriate material, I will report this to the DSL without delay. Equally, if I feel that we are overblocking, I shall notify the school to inform regular checks and annual review of these systems.

13. I understand that I am a role model and will promote positive online safety and model safe, responsible and positive behaviours in my own use of technology both in and outside school, including on social media, e.g. by not sharing other's images or details without permission and refraining from posting negative, threatening or violent comments about others, regardless of whether they are members of the school community or not.
14. I will not contact or attempt to contact any pupil or to access their contact details (including their usernames/handles on different platforms) in any way other than school-approved and school-monitored ways, which are detailed in the school's Online Safety Policy. I will report any breach of this by others or attempts by pupils to do the same to the headteacher.
15. If I already have a personal relationship to a pupil or their family, I will inform the DSL/Headteacher of this as soon as possible.
16. Details on social media behaviour, the general capture of digital images/video and on my use of personal devices is stated in the full Online Safety policy. If I am ever not sure, I will ask first.
17. I will not use any new technology or download any apps without agreement from DSL.
18. I will not use a mobile hotspot to provide internet to any device I use in school.
19. I agree to adhere to all provisions of the school's Cybersecurity and Data Protection Policies at all times, whether or not I am on site or using a school device, platform or network.
20. I will never use school devices and networks/internet/platforms/other technologies to access material that is illegal or in any way inappropriate for an education setting. I will not attempt to bypass security or monitoring and will look after devices loaned to me.
21. I will not support or promote extremist organisations, messages or individuals, nor give them a voice or opportunity to visit the school. I will not browse, download or send material that is considered offensive or of an extremist nature. I understand that any breach of this AUP and/or of the school's full Online Safety Policy here may lead to appropriate staff disciplinary action or termination of my relationship with the school and where appropriate, referral to the relevant authorities.
22. I will only use gen AI platforms that have been authorised for use, and I will ensure that any use of these platforms is transparent, appropriate, legal and ethical. I will also ensure that I abide by all data protection legislation in relation to using these platforms.

To be completed by the user

I have read, understood and agreed to this policy. I understand that it is my responsibility to ensure I remain up to date and read and understand the school's most recent online safety / safeguarding policies. I understand that failure to comply with this agreement could lead to disciplinary action.

Signature: _____

Name: _____

Role: _____

Date: _____

To be completed by a member of SMT:

I approve this user to be allocated credentials for school systems as relevant to their role.

Systems (delete or add as appropriate): School network, School GSuite, RM Inetgris, ActiveLearn (bug club), Accelerated Reader, Pixel,

Additional permissions (e.g. admin) _____

Signature: _____

Name: _____

Role: _____

Date: _____

Acceptable Use Policy for Contractors or Visitors who have access to school IT equipment and networks.

Background

We ask all children, young people and adults involved in the life of SHH Federation to sign an Acceptable Use* Policy (AUP), which outlines how we expect them to behave when they are online, and/or using school networks, connections, internet connectivity and devices, cloud platforms and

Visitors and contractors are asked to sign this document before they are allowed access to the school or its pupils. Many of these rules are common sense – if you are in any doubt or have questions, please ask the DSL Judy Knappett, Sue Walsh or Nilufar Chowdhury

Further details of our approach to online safety can be found in the overall school Online Safety Policy.

If you have any questions during your visit, you must ask the person accompanying you.

If questions arise after your visit, contact the school.

What am I agreeing to?

1. I understand that any activity on a school device or using school networks, platforms, internet and logins may be captured by one of the school's security, monitoring and filtering systems and/or viewed by an appropriate member of staff.

2. I will never attempt to arrange any meeting with a pupil, 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.

3. I will leave my phone in my pocket and turned off. Under no circumstances will I use it (or other capture device) in the presence of children or to take photographs or audio/visual recordings of the school, its site, staff or pupils/students. If required (e.g. to take photos of equipment or buildings), I will have the prior permission of the headteacher (this may be delegated to other staff) and it will be done in the presence of a member staff.

4. If I am given access to school-owned devices, networks, cloud platforms or other technology:

- I will use them exclusively for the purposes to which they have been assigned to me, and not for any personal use
- I will not attempt to access any pupil / staff / general school data unless expressly instructed/allowed to do so as part of my role
- I will not attempt to make contact with any pupils/students or to gain any contact details under any circumstances
- I will protect my username/password and notify the school of any concerns
- I will abide by the terms of the school Data Protection Policy protections.
- I understand that my online activity will be subject to the school's filtering and monitoring systems, and that any attempts to access content which is illegal or inappropriate for a school setting, may result in further action as per the safeguarding procedures and may result in termination of contract.

5. I will not share any information about the school or members of its community that I gain as a result of my visit in any way or on any platform except where relevant to the purpose of my visit and agreed in advance with the school.

6. I will not reveal any information on social media or in private which shows the school in a bad light or could be perceived to do so.

7. I will not do or say anything to undermine the positive online safety messages that the school disseminates to pupils/students and will not give any advice on online safety issues unless this is the purpose of my visit and this is pre-agreed by the school. NB – if this is the case, the school will ask me to complete Annex A and consider Annex B of 'Using External Visitors to Support Online Safety' from the UK Council for Child Internet Safety (UKCIS).

8. I understand that children can be abused and harmed when using devices and I will report any behaviour (no matter how small) which I believe may be inappropriate or concerning in any way to the Designated Safeguarding Lead (if by a child) or Headteacher/Principal (if by an adult).

9. I will only use any technology during my visit, whether provided by the school or my personal/work devices, including offline or using mobile data, for professional purposes and/or those linked to my visit and agreed in advance. I will not view material which is or could be perceived to be inappropriate for children or an educational setting.

10. I will behave in a professional and responsible manner at all times and understand that failure to do so may result in further action being taken and could result in the termination of my contract.

~~~~~~~~~~~~~~~~~~~~

To be completed by the visitor/contractor:

I have read, understood and agreed to this policy.

Signature/s: _____

Name: _____

Organisation: _____

Visiting / accompanied by: _____

Date / time: _____

Chrome Book or Laptop device loan agreement for Pupil Home Learning Use

Device on loan: Chrome Book Asset Register No:_____

Full name of child the loan is for: _____ Year Gp _____

The above device is owned by: Tick which school

● **Hague Primary School**	
● **Stewart Headlam School**	

Loan Agreement:

- I agree to take full responsibility for the loan equipment.
- **I will ensure the device is used in a safe way to prevent damage:**
    - Keep the device in a secure place when not in use
    - Don't leave the device in a car or on show at home
    - Don't eat or drink around the device
    - Don't lend the device to non Hague or Stewart Headlam siblings or friends

    - Don’t leave the equipment unsupervised in unsecured areas
- The equipment **is to be used by my child to enable them to complete their school work** and access online meetings or lessons run by the school.
- I will **return the equipment in the same condition** that it was loaned to me when asked to by the school.
- I will **supervise my child’s use of the equipment** to ensure they are using it appropriately and safely.
- I am responsible for ensuring the online safety of my child. **I will set parental controls on my home broadband. (***Details on how to do this can be accessed here: https://www.saferinternet.org.uk/advice-centre/parents-and-carers/parental-controls-offered-your-home-internet-provider)*
- **I will not install new software** on the device without school permission.
- I will ensure that **my child follows the Pupil Acceptable Use Agreement** when using the equipment at home, just as they would at school.
- **If the device is damaged, lost or stolen I will inform the school immediately. If it is stolen I will also inform the police and get a crime reference number.**

The school is not responsible for any damage to person or property resulting from the loaned device/computer, or for any costs resulting from the use of the computer including electricity, printer cartridges, paper or any cost occurring from an internet service.

I, the parent/carer, have read or had explained and understand the terms and conditions in the home loan agreement.

I understand that I am liable for the cost of the Chromebook if I fail to return it when asked or its repair costs if damaged due to mis-use.

Parent Name: _____

Parent Signature: _____ Date loan started: _____

E-Security Policy 2024-2025

E-Security Policy:

Schools hold personal data on learners, staff and others to help them conduct their day-to-day activities. Some of this information is sensitive and could be used by another person or criminal organisation to cause harm or distress to an individual. The loss of sensitive information can result in media coverage, and potentially damage the reputation of the school. This can make it more difficult for our school to use technology to benefit learners. A list of personal sensitive data held is included in appendix 6.

Everybody in the school community has a shared responsibility to secure any sensitive information used in their day to day professional duties and even staff not directly involved in data handling should be made aware of the risks and threats and how to minimise them.

Strategic and operational practices

At this school:

- The Executive Head Teacher is the Senior Information Risk Officer (SIRO).
- Louise Manthorpe from Connetix is our Data protection Officer with responsibility for data protection compliance.
- Staff are clear who are the key contact(s) for key school information (the Information Asset Owners) are. We have listed the information and information asset owners in a spreadsheet stored in Planning and curriculum\Policies\HPS Non statutory
- Any incidents where data protection may have been compromised, such as when passwords for sensitive systems or devices have been lost or stolen, must be reported to the head teacher so that appropriate action can be taken.
- All staff are DBS checked and records are held in one central record in RM Integris.
- We ensure ALL the following school stakeholders sign an Acceptable Use Agreement form. We have a system so we know who has signed. staff, governors, pupils, parents, volunteers. This makes clear staffs' responsibilities with regard to data security, passwords and access.
- We have approved educational web filtering across our wired and wireless networks. Where concerns are raised we maintain the right to monitor the content of school emails.
- We follow LA guidelines for the transfer of any data, such as MIS data or reports of children, to professionals working in the Local Authority or their partners in Children's Services / Family Services, Health, Welfare and Social Services.
- We require that any Sensitive material must be encrypted if the material is to be removed from the school and limit such data removal. We have an approved remote access solution so staff can access sensitive and other data from home, without need to take data home.
- Sensitive / Special Category data must not be downloaded or stored onto personal devices not owned by the school.
- School staff with access to setting-up usernames and passwords for email, network access and Learning Platform access are working within the approved system and follow the security processes required by those systems.
- All staff have their own unique username and private passwords to access school systems. Staff are responsible for keeping their passwords private and ensuring they are strong passwords.

- We require staff to use strong passwords for access into our MIS system. These are changed every 90 days.
- Guest accounts with restricted access are used for external or short term visitors.
- We ask staff to undertake at least annual house-keeping to review, remove and destroy any digital materials and documents which need no longer be stored.

Technical Solutions

- Staff have a secure area on the network to store sensitive documents or photographs.
- We require staff to log-out of systems when leaving their computer, but also enforce lock-out after 10 minutes idle time.
- If any member of staff has to take any sensitive / special category information off site they should do so by accessing the shared staff google drives or by using an encrypted flash drive.
- We use the DfE S2S site to securely transfer CTF pupil data files to other schools.
- We use the Pan-London Admissions system (based on USO FX) to transfer admissions data.
- We use Freedom2Roam with its 2-factor authentication for remote access into our systems.
- We use LGfL's USO FX to transfer other data to schools in London, such as references, reports of children.
- We use Egress to transfer sensitive / personal data where USOFx cannot be used.
- We use the LGfL secure data transfer system, USOAutoUpdate, for creation of online user accounts for access to broadband services and the London content
- We use Google Apps for Education for online documentation storage.
- We store any Sensitive / Special Category written material in lockable storage cabinets in a lockable storage area.
- All servers are kept in lockable locations and are managed by DBS-checked staff.
- We use LGfL's GridStore remote secure back-up for disaster recovery on our network.
- We comply with the WEEE directive on equipment disposal by using an approved or recommended disposal company for disposal of equipment where any protected or restricted data has been held and get a certificate of secure deletion for any server that once contained personal data.
- Portable equipment loaned by the school (for use by staff at home), where used for any protected data, is disposed of through the same procedure.
- Paper based sensitive information is shredded, using cross cut shredder.

Mobile Devices:

Staff should take extra care when using mobile devices to access sensitive data eg I pads or personal mobile phones.

All phones and I pads used to access the sensitive data / school emails should be secured with a 4 digit code, finger print or pattern to access the device. These codes should be secure (not 1234 or 0000).

If pupils or other people are using your mobile device, ensure that they cannot access the sensitive data. Check your device is not automatically remembering passwords for sites containing sensitive data such as emails or class assessments.

Report the loss of any device used to access personal data to Judy or Alison so we can assess any potential risk to school data and take appropriate action.

Password Security Policy

Introduction

The school holds a lot of personal data about children. All adults working in school need to take responsibility for ensuring the security of the data they have access to through the use of secure passwords and passcodes.

The main electronic data areas that the majority of staff have access to are:

- RM Integris (our MIS system)
- The sensitive or admin areas of the school network (pupil data, SEN records, reports, behaviour data, photos, pupil passwords, etc) The more sensitive data stored on the sensitive or admin area of the school network should be password protected.
- Gmail (school emails and staff google drives may contain information about staff or pupils).
- Pixl (pupil assessment data)
- Accelerated Reader (pupil assessment data)
- Pearson Bug Club
- Pearson Power Maths
- Exaat EYFS tracking system (pupil data and photos).
- LGfl (pupil data for cyberpass).

All staff need to make sure that their passwords for these and any other sources of sensitive data are secure.

Responsibilities

The management of the password security policy will be the responsibility of the IT Technician and ICT Coordinator.

The school will be responsible for ensuring that the school network is as safe and secure as is reasonably possible and that:

- users can only access data to which they have right of access
- no user should be able to access another's files, without permission (or as allowed for monitoring purposes within the school's policies).
- access to personal data is securely controlled in line with the school's personal data policy
- keeping secure records of access rights of different user groups which are reviewed regularly.

All users will have responsibility for the security of their username and passwords, must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security.

Pupil Passwords:

- EYFS and Year 1 have a class login to the network and will be closely supervised whilst using IT.

- All users (from year 2 and above) will be provided with a username and password for the network, lgfl and for gmail by the IT Technician/Co-ordinator who will keep an up to date record of users and their usernames.

Pupils will be taught about the importance of keeping passwords secure through:

- ICT and / or e-safety lessons
- the Acceptable Use Agreement Policy Statements

Staff Passwords:

Members of staff will be made aware of the school's password policy at induction and through regular review of the school's e-safety policy and password security policy and Internet Use Agreement

Passwords should:

- *Be long (at least 8 characters)*
- *Contain a mixture of upper and lower case letters, numbers and/ or symbols.*
- *Not be easy to guess names or words eg class names, school name, DFE number, password, consecutive numbers eg 123.*
- *Be kept private (not shared with other members of staff or written down and left by computers).*
- *Changed at least annually.*

Users are encouraged to check the strength of their password using a password meter.

• temporary passwords for staff e.g. used with new user accounts or when users have forgotten or need to change their passwords, shall be enforced to change immediately upon the next account log-on

• passwords shall not be displayed on screen, and shall be securely hashed (use of one-way encryption)

The "master / administrator" passwords for the school ICT system, used by the IT Technician and ICT Co-ordinator are also available to the Headteacher.

Mobile Devices:

Staff should take extra care when using mobile devices to access sensitive data eg I pads or personal mobile phones.

All phones and I pads used to access the sensitive data / school emails should be secured with a 4 digit code, finger print or pattern to access the device. These codes should be secure (not 1234 or 0000).

If pupils or other people are using your mobile device, ensure that they cannot access the sensitive data. Check your device is not automatically remembering passwords for sites containing sensitive data.

Report the loss of any device used to access personal data to Judy, Nilufar or Alison so we can assess any potential risk to school data and take appropriate action.

Audit / Monitoring / Reporting / Review

In the event of a serious security incident, the police may request and will be allowed access to passwords used for encryption. The Local Authority Auditors also have the right of access to passwords for audit investigation purposes.

User lists, IDs and other security related information is given the highest security classification and stored in a secure manner.