St Paul with St Luke & St Saviour's C of E Primary School Federation

Online Safety Policy

(November 2024)

Approved by:	Federation Curriculum board	**Date:**	18th November 2024
Last reviewed on:	November 2024		
Next review due by:	November 2025		

What's different about this policy for September 2024?

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

Introduction

Key people / dates

St Paul with St Luke & St Saviour's C of E Primary School Federation	Designated Safeguarding Lead (DSL), with lead responsibility for filtering and monitoring	Tomas Hall
	Deputy Designated Safeguarding Leads / DSL Team Members	DSL Mark Ali - SPSL DSL Tomas Hall - StS DDSL Fahima Begum - SPSL DDSL Thomas Dunford - StS DDSL Jo Robin - StS DDSL Rachel Sablon - StS DDSL Fanoula Smith - Federation DDSL Dan French - Federation
	Link governor for safeguarding and web filtering	Aune Turkson-Jones

	Curriculum leads with relevance to online safeguarding and their role	**Computing:** Tomas Hall **PSHE:** Dan French, Thomas Dunford (StS) & Tahura Choudhury – (SPSL) **RSE:** Dan French, Thomas Dunford (StS) & Tahura Choudhury – (SPSL)
	Network manager / other technical support	Levetts Consultancy (StS) Connetix Ltd (SPSL)
	Date this policy was reviewed and by whom	November 2023 Full governing body
	Date of next review and by whom	November 2025 Full governing body

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

Who is it for; when is it reviewed?

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. Pupils could help to design a version in language their peers understand or help you to audit compliance. Acceptable Use Policies (see appendices) for different stakeholders help with this – ensure these are reviewed alongside this overarching policy. Any changes to this policy should be immediately disseminated to all the above stakeholders.

Who is in charge of online safety?

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 PSHE 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 schools 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: pupils accessing websites that have a suggested age limit of 13 such as Youtube, TikTok, Twitter (X) or Discord to socialise and view content some of which is not appropriate; parents and carers who are unaware of this and the risks posed to children and children messaging each other via mobile devices using inappropriate language.

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

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

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

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

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

This is striking when you consider that 20% of 3-4 year olds have access to their OWN mobile phone (let alone shared devices), rising to over 90 percent by the end of Primary School, and the vast majority have no safety controls or limitations to prevent harm or access to inappropriate material. At the same time, even 3 to 6 year olds are being tricked into 'self-generated' sexual content (Internet Watch Foundation Annual Report) while considered to be safely using devices in the home and the 7-10-year-old age group

is the fastest growing for this form of child sexual abuse material, up 60 percent within 12 months to represent over 60,000 cases found (of this same kind where the abuser is not present).

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

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

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

How will this policy be communicated?

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

- Posted on the school website
- Part of school induction pack for all new staff (including temporary, supply and non-classroom-based staff and those starting mid-year)
- Integral to safeguarding updates and training for all staff (especially in September refreshers)
- Clearly reflected in the Acceptable Use Policies (AUPs) for staff, volunteers, contractors, governors, pupils and parents/carers (which must be in accessible language appropriate to these groups), which will be issued to whole school community, on entry to the school, annually and whenever changed, plus displayed in school

Contents

Overview

Aims

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

- Setting out expectations for all St Saviour's 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. PSHE) 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 head of school will handle referrals to the LA designated officer (LADO). The local authority, academy trust or third-party support organisations you work with may also have advisors to offer general support.

Beyond this, **reporting.lgfl.net** has a list of curated links to external support and helplines for both pupils and staff, including the Professionals' Online-Safety Helpline from the UK Safer Internet Centre and the NSPCC 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 St Saviour's 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 2023/2024, it is vital that all members understand their responsibilities and those of others when it comes to filtering and monitoring. All staff have a key role to play in feeding back on potential issues

Education and curriculum

It is important that schools establish 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 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, new technology such as augmented reality, etc) in school or setting as homework tasks, all staff should encourage sensible use, monitor what pupils/students are doing and consider potential dangers and the age appropriateness of websites (ask your DSL what appropriate filtering and monitoring policies are in place). "Parents and carers are likely to find it helpful to understand what systems schools use to filter and monitor online use. It will be especially important for parents and carers to be aware of what their children are being asked to do online, including the sites they will be asked to access and be clear who from the school or college (if anyone) their child is going to be interacting with online" (KCSIE 2023).

Equally, all staff should carefully supervise and guide pupils when engaged in learning activities involving online technology (including, extra-curricular, extended school activities if relevant and remote teaching), supporting them with search skills, critical thinking (e.g. disinformation, misinformation and fake news), age appropriate materials and signposting, and legal issues such as copyright and data law. saferesources.lgfl.net has regularly updated theme-based resources, materials and signposting for teachers and parents.

At St Saviour's, 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 of Self-image and Identity, Online relationships, Online reputation, Online bullying, Managing online information, Health, Wellbeing and lifestyle, Privacy and security, and Copyright and ownership.

This is done within the context of an annual online safety audit, which is a collaborative effort led by the DSL and Computing lead.

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
- Sexual Harassment / Child-on-Child Abuse Policy (if separate)
- Anti-Bullying Policy
- Behaviour Policy (including school sanctions)
- Acceptable Use Policies
- Prevent Risk Assessment / Policy
- Data Protection Policy, agreements and other documentation (e.g. privacy statement and consent forms for data sharing, image use etc)
- Cybersecurity : 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 Head of school, unless the concern is about the Head of school in which case the complaint is referred to the Executive Head or

Chair of Governors and the LADO (Local Authority's Designated Officer). Staff may also use the NSPCC Whistleblowing Helpline : helplines are displayed in the staff room

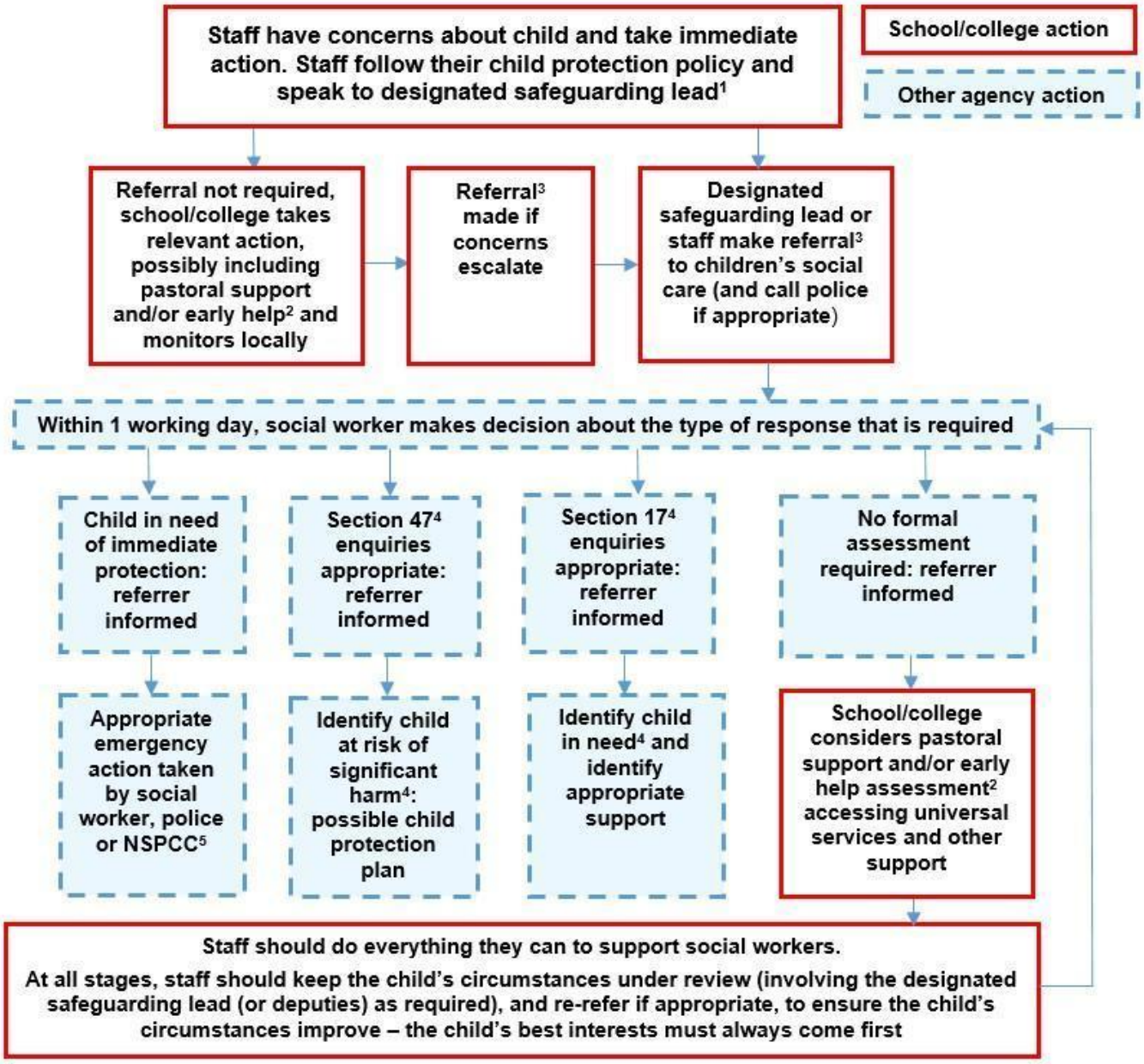
The school will actively seek support from other agencies as needed (i.e. the local authority, LGfL, UK Safer Internet Centre's Professionals' Online Safety Helpline (POSH), NCA CEOP, Prevent Officer, Police, IWF and Harmful Sexual Behaviour Support Service). The DfE guidance Behaviour in Schools, advice for headteachers and school staff September 2022 provides advice and related legal duties including support for pupils and powers of staff when responding to incidents – see pages 32-34 for guidance on child on child sexual violence and harassment, behaviour incidents online and mobile phones.

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

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

Actions where there are concerns about a child

The following flow chart (it cannot be edited) is taken from page 22 of Keeping Children Safe in Education 2024 as the key education safeguarding document. As outlined previously, online safety concerns are no different to any other safeguarding concern.

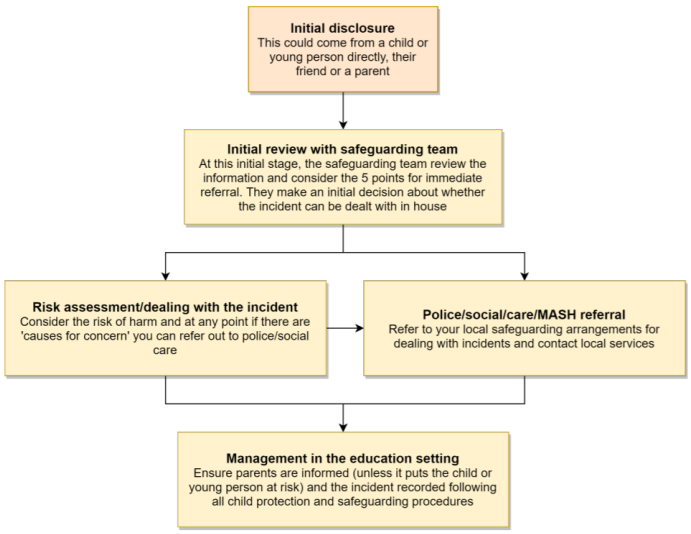

Staff have concerns about child and take immediate action. Staff follow their child protection policy and speak to designated safeguarding lead[1]
School/college action
Other agency action
Referral not required, school/college takes relevant action, possibly including pastoral support and/or early help[2]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

Sexting – sharing nudes and semi-nudes

All schools (regardless of phase) should refer to the UK Council for Internet Safety (UKCIS) guidance on sexting - now referred to as Sharing nudes and semi-nudes: advice for education settings to avoid unnecessary criminalisation of children. NB - where one of the parties is over 18, this is no longer sexting but child sexual abuse.

There is a one-page overview called Sharing nudes and semi-nudes: how to respond to an incident for all staff (not just classroom-based staff) to read, in recognition of the fact that it is mostly someone other than the designated safeguarding lead (DSL) or online safety lead to first become aware of an incident, and it is vital that the correct steps are taken. Staff other than the DSL must not attempt to view, share or delete the image or ask anyone else to do so, but to go straight to the DSL.

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



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

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

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

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

Up-skirting

It is important that everyone understands that up-skirting (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. See our Anti-Bullying policy for more information including procedures to follow when issues of this nature occur.

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

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

Child-on-child sexual violence and sexual harassment

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

Any incident of sexual harassment or violence (online or offline) should be reported to the DSL who will follow the full guidance. Staff should work to foster a zero-tolerance culture and maintain an attitude of 'it could happen here'. The guidance stresses that schools must take all forms of sexual violence and harassment seriously, explaining how it exists on a continuum and that behaviours incorrectly viewed as 'low level' are treated seriously and not allowed to perpetuate. The document makes specific reference to behaviours such as bra-strap flicking and the careless use of language.

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

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

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

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

Where pupils 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.

The new responsibilities for filtering and monitoring, led by the DSL and following the new DfE standards, may mean that more such incidents will be discovered in the coming year but the school will do its best to remind pupils and staff of this increased scrutiny at the start of the year.

Social media incidents

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

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, St Saviour's will request that the post be deleted and will expect this to be actioned promptly.

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

Data protection and cybersecurity

All pupils, staff, governors, volunteers, contractors and parents are bound by the school's data protection and cybersecurity policy which can be found here https://www.st-saviours.towerhamlets.sch.uk/wp-content/uploads/2021/07/GDPR-data-protection-Policy-St-2021-.pdf

It is important to remember that there is a close relationship between both data protection and cybersecurity and a school's ability to effectively safeguard children. Schools are reminded of this in KCSIE which also refers to the DfE Standards of Cybersecurity for the first time in 2023.

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

Appropriate filtering and monitoring

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

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

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

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

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

ALL STAFF need to be aware of the changes and renewed emphasis and play their part in feeding back about areas of concern, potential for students to bypass systems and any potential over blocking. They can submit concerns at any point to the DSL, Computing lead, SLT or administration team – this will be done via an email so a written record of concerns can be tracked. Staff will be asked for feedback at the time of the regular checks which will now take place.

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

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

At St Saviour's:

- web filtering is provided by LGFL on school site and for school devices used in the home
- changes can be made by the Levetts Consultancy
- overall responsibility is held by the DSL
- technical support and advice, setup and configuration are from Connectix
- Regular checks are made half termly by the Levetts Consultancy, and termly by the Safeguarding link governor, to ensure filtering is still active and functioning everywhere. This is evidenced in a report produced at the time of checking.
- an annual review is carried out as part of the online safety audit to ensure a whole school approach- using the template is available at onlinesafetyaudit.lgfl.net]
- guidance on how the system is 'appropriate' is available at appropriate.lgfl.net

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

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

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

Authorised systems

- Pupils at this school communicate with each other and with staff using Google Classroom and the Google Mail function within it.

- Staff at this school use the email system provided by LGFLMAIL for all school emails. They never use a personal/private email account (or other messaging platform) to communicate with children or parents, or to colleagues when relating to school/child data, using a non-school-administered system. Staff are permitted to use this email system to communicate with educational external organisations but not with under 18s.

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 and centrally managed.

Any unauthorised attempt to use a different system may be a safeguarding concern or disciplinary matter and should be notified to the DSL (if by a child) or to the Head of school (if by a staff member).

Where devices have multiple accounts for the same app, mistakes can happen, such as an email being sent from or data being uploaded to the wrong account. If this private account is used for communication or to store data by mistake, the DSL/Executive 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 http://www.st-saviours.towerhamlets.sch.uk/wp-content/uploads/2021/07/GDPR-data-protection-Policy-St-2021-.pdf and only using the authorised systems mentioned above.
- Pupils and staff are allowed to use the email systems: Hotmail and Google Mail 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).

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. St Saviour's has a clear cybersecurity and data protection policy which staff, governors and volunteers must follow at all times.

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 Head and Governors have delegated the day-to-day responsibility of updating the content of the website and ensuring compliance with DfE stipulations to John Ward.

The site is managed by / hosted by John Ward.

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 Bridget Clark– School Business Manager or the DPO John Pearson-Hicks

Digital images and video – see Appendix 1

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:

[Ensure these are the options on your consent form and check they still meet all school needs]

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

- Etc.]

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

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

All staff are governed by their contract of employment and the school's Acceptable Use Policy, which covers the use of mobile phones/personal equipment for taking pictures of pupils, and where these are stored. At St Saviour's, only members of staff with permission 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).]

Photos are stored in the school's Google Drive in line with the retention schedule of the school Data Protection Policy.

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

St Saviour's 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. [If your school has no SM accounts, you may wish to add to this paragraph "…even there are no official/active school social media accounts."]

Fanoula Smith is responsible for managing our X-Twitter and Facebook accounts and for 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 policy should be followed. Sharing complaints on social media is unlikely to help resolve the matter, but can cause upset to staff, pupils and parents, also undermining staff morale and the reputation of the school (which is important for the pupils we serve).

Many social media platforms have a minimum age of 13 (note that WhatsApp is 16+), but on occasion the school has dealt with issues arising on social media involving pupils/students under the age of 13. We ask parents to respect age ratings on social media platforms wherever possible and not encourage

or condone underage use. It is worth noting that Online Harms regulation is likely to require more stringent age verification measures over the coming years.

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

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

Although the school has an official Facebook and 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 such communication/ school use. [Reference any other relevant platforms here also, or edit if social media contact is allowed, and what controls are in place]

[Edit the following for exceptions and alternative rules if social media is more widely used as part of school life, adding the restrictions and controls if it is, e.g. if a Facebook class group is allowed, then at least a second unrelated teacher must be part of the group to monitor activity between the teacher and students]

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 Head of school, 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 Head of school (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 [this links to the section in this document; provide other link if you have this as a separate document] and permission is sought before uploading photographs, videos or any other information about other people.

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

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)

[There are too many variants to give examples to select from here; instead we have given one or two examples of the many possibilities that you can easily edit, add the word 'not' or otherwise amend]

- **Pupils/students** in Years 5 and 6 who come to school by themselves or who are home alone are allowed to bring mobile phones in but these must be handed to the school office upon arrival and collected only at the end of the school day. Mobile phones are not allowed in class. Any attempt to use a phone in lessons without permission or to take illicit photographs or videos will be a major beach of the behaviour policy. 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 the staff toom 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 of school should be sought (the head of school 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 on page . [parentfilming.lgfl.net may provide further useful guidance]. Parents are asked not to call pupils on their mobile phones during the school day; urgent messages can be passed via the school office.

Use of school devices – see Appendix 1

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.

Wifi is accessible to staff and visitors for [insert here any allowed use of BYOD and/guest networks and any restrictions for personal devices] school-related internet use / limited personal use within the framework of the acceptable use policy. All such use is monitored.

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.

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 issued a school duty phone and this number used for any authorised or emergency communications with pupils/students and parents. Any deviation from this policy (e.g. by mistake or because the school phone will not work) will be notified immediately to the Head of school. 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.

[Ensure that the authorised systems you use to communicate with parents as outlined within this document include any systems used in exceptional circumstances such as on trips if you notify parents of trip updates or status of arriving back at school and that these are DP compliant. You may wish to name them also here]

Searching and confiscation

In line with the DfE guidance 'Searching, screening and confiscation: advice for schools', the Head of School, Executive Head 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.

Full details of the school's search procedures are available in the school Behaviour Policy [Insert link].

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 (see Appendix 1) 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 2023) and guidance (such as KCSIE), modelling safe, responsible and professional behaviours in their own use of technology at school and beyond and avoiding scaring, victim-blaming language.

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

Executive Headteacher – Fanoula Smith

Key responsibilities:

- Foster a culture of safeguarding where online-safety is fully integrated into whole-school safeguarding
- Oversee and support the activities of the designated safeguarding lead team and ensure they work technical colleagues to complete an online safety audit in line with KCSIE (including technology in use in the school) – [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 new DfE standards—through regular liaison with technical colleagues and the DSL– in particular understand what is blocked or allowed for whom, when, and how as per KCSIE. [LGfL's Safeguarding Shorts: Filtering for DSLs and SLT twilight provides an overview]
    - In 2023/4 this will involve starting regular checks and annual reviews, upskilling the DSL and appointing a filtering and monitoring governor
- Liaise with the designated safeguarding lead on all online-safety issues which might arise and receive regular updates on school issues and broader policy and practice information
- Support safeguarding leads and technical staff as they review protections for pupils in the home and remote-learning procedures, rules and safeguards [see remotesafe.lgfl.net for policy guidance and an infographic overview of safeguarding considerations for remote teaching technology]
- 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 – Tomas Hall

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

- The DSL should "take **lead responsibility** for safeguarding and child protection (**including online safety and understanding the filtering and monitoring** systems and processes in place).
- Ensure "An effective whole school approach to online safety as per KCSIE
- In 2023/4 working to take up the new responsibility for filtering and monitoring by working closely with technical colleagues, SLT and the new filtering governor to learn more about this area, better understand, review and drive the rationale behind systems in place and initiate regular checks and annual reviews, including support for devices in the home. [LGfL's Safeguarding Shorts: Filtering for DSLs and SLT twilight provides a quick overview and there is lots of information for DSLs at safefiltering.lgfl.net and appropriate.lgfl.net]
- Where online-safety duties are delegated and in areas of the curriculum where the DSL is not directly responsible but which cover areas of online safety (e.g. RSHE), ensure there is regular review and open communication and that the DSL's clear overarching responsibility for online safety is not compromised or messaging to pupils confused
- Ensure ALL staff and supply staff undergo safeguarding and child protection training (including online-safety) at induction and that this is regularly updated.
    - In 2023/4 this must include filtering and monitoring and help them to understand their roles
    - all staff must read KCSIE Part 1 and all those working with children also Annex B – translations are available in 13 community languages at kcsietranslate.lgfl.net (B the condensed Annex A can be provided instead to staff who do not directly work with children if this is better)
    - cascade knowledge of risks and opportunities throughout the organisation
    - safecpd.lgfl.net has helpful CPD materials including PowerPoints, videos and more
- Ensure that ALL governors and trustees undergo safeguarding and child protection training (including online-safety) at induction to enable them to provide strategic challenge and oversight into policy and practice and that this is regularly updated –[LGfL's Safeguarding Training for school governors is free to all governors at safetraining.lgfl.net]

- Take day-to-day responsibility for safeguarding issues and be aware of the potential for serious child protection concerns
- Be mindful of using appropriate language and terminology around children when managing concerns, including avoiding victim-blaming language [see spotlight.lgfl.net for a resource to use with staff on how framing things linguistically can have a safeguarding impact, and some expressions we use might be unhelpful]
- Remind staff of safeguarding considerations as part of a review of remote learning procedures and technology, including that the same principles of online-safety and behaviour apply
- Work closely with SLT, staff and technical colleagues to complete an online safety audit (including technology in use in the school) – [see LGfL's template with questions to use at onlinesafetyaudit.lgfl.net]
- Work with the Executive 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 – Aune Turkson - Jones

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 / RHE Lead/s – Dan French

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 – Tomas Hall

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 – Connectix

Key responsibilities:

- As listed in the 'all staff' section, plus:
- Collaborate regularly with the DSL and leadership team to help them make key strategic decisions around the safeguarding elements of technology.
- Note that KCSIE changes expect a great understanding of technology and its role in safeguarding when it comes to filtering and monitoring and in 2023/4 you will be required to support safeguarding teams to understand and manage these systems and carry out regular reviews and annual checks.
- Support DSLs and SLT to carry out an annual online safety audit as now recommended in KCSIE. [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
- 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 [Network managers/technicians at LGfL schools may want to ensure that you take advantage of the following solutions which are part of your package: Sophos Anti-Virus, Sophos Anti-Phish, Sophos InterceptX, Sophos Server Advance, Malware Bytes, Egress, Meraki Mobile Device Management and CloudReady/NeverWare. 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 [move this requirement to a different role outline as appropriate] and that any misuse/attempted misuse is identified and reported in line with school policy
- Work with the Executive Headteacher to ensure the school website meets statutory DfE requirements [see website audit tool at websiterag.lgfl.net / this may well be part of someone else's role, but the technical team is likely to play at least some role in working with the web team – move this bullet point as appropriate]

Data Protection Officer (DPO) – John Pearson-Hicks

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 – N/A

Key responsibilities:

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

APPENDIX 1 – FROM STAFF HANDBOOK

Staff Acceptable Use Policy

Staying Safe Whilst Using the Computer:

I will only use the school's digital technology resources and systems for professional purposes or for uses deemed 'reasonable' by the Head of School and Governing Body. I agree and accept that any computer, laptop or tablet loaned to me by the school is provided solely to support my professional responsibilities.

Accessing Computer Systems

I will not reveal my password(s) to anyone and will not record it in a place where it could be easily discovered (such as the back page of a diary). If my password is compromised, I will ensure I change it. I will not use anyone else's password if theyreveal it to me and will advise them to change it. I will not allow unauthorised individuals to access email / Internet / intranet / network, or other school / LA systems.

GDPR

I will adhere to the school's General Data Protection and Access Control Policy and Procedures. I will ensure a clear desk in agreement with school policy. I accept that Ihave been granted rights defined in GDPR agreement information and acknowledge the training I have received. I know that breaches will lead to my personal liability. Contact us If you have any questions, concerns or would like more information about anything mentioned GDPR and the privacy notices. Do contact either our School Data Protection Lead, Bridget Clark, School Business Manager at St Saviour's, first or our independent Data Protection Officer, John Pearson-Hicks @ GROW Education / LDBS john.pearson-hicks@london.anglican.org.

Keeping Children Safe

I will embed the school's e-safety curriculum into my teaching and teach children in my care about the e-safety and anti-cyberbullying rules. I will be vigilant about e-safety risks and incidents (including cyber-bullying) that children in my charge might experience and respond promptly by following the agreed procedures and communicating concerns to the Computing co-ordinator or nominated child protection officer as appropriate. https://www.st-saviours.towerhamlets.sch.uk/

Digital Images

I will use school devices to take photographs and videos, rather than my own device. If I use personal digital cameras or camera phones for taking and transferring images of pupils or staff for professional purposes, I will save the photos on the school network and delete them from my equipment at the first available opportunity. I will not store images or photos of children or staff at home without permission. I will ensure that I do not photograph or video children for which release consent has not been granted. Consent needs to be clearly granted that fits the purpose. I will follow the school's guidance document on publication of photographs and videos.

Communication

I will only use the approved, secure email system(s) for any school business. (This is currently the LGfL provided StaffMail system.) I will only use the approved school email, or other school approved communication systems with pupils or parents/carers, and only communicate with them on appropriate school business. Secure information on pupils is transferred via USO-FX and Egress. We use Google Sheets to communicate remotely and add working documents during lockdown.

Inappropriate Material

I will not browse, download or send material that could be considered offensive. This could include (but does not exclusively include) materials that are pornographic, hateful, racist, sexist, abusive, obscene or

discriminatory. I will report any accidental access to, or receipt of inappropriate materials, or filtering breach to the ICT Coordinator. I understand that all Internet and network usage can be logged and this information could be made available to my manager onrequest.

Copyright

I will not publish or distribute work that is protected by copyright. This includes protected images available online. Use Cornerstones & Jigsaw images for classwork that already has intellectual property agreements.

Protecting the Network and Antivirus

I will not connect a computer, laptop or other device (including USB flash drive), to the network / Internet if it does not have up-to-date anti-virus software (or been scanned first for USB flash drives), and I will keep any 'loaned' equipment up-todate, using the school's recommended anti-virus, firewall and other ICT 'defence' systems. I will not download any software or resources from the Internet that can compromise the network or are not adequately licensed.

Personal Use of Online Publishing Systems

I will not engage in any online activity that may compromise my professional responsibilities. This includes posting on social networking sites about school. I will not contact children known to me through school on any social networking site. (Facebook, Instagram, Twitter, WhatsApp). I will ensure that any private social networking sites / blogs etc. that I create or actively contribute to are not confused with my professional role. This policy is to be read in conjunction with our Online Safety Policy – both are available on the staff Intranet and the website. Staff must sign each year that they have read and will abide by the acceptable use policy. Full colour poster versions of the Early years, ks1 &2 acceptable use versions of the policy are available via the full policy and should be displayed in the appropriate classroom and regularly discussed with children. Where safeguarding duty changes throughout the year please ensure you are updated. Referral telephone numbers may change during the year. Please change this in your handbook as required.

Online safeguarding is becoming a significant concern with peer abuse rising. Staff need to be mindful especially if remote teaching. When using zoom for blended learning please ensure you follow protection protocols on using passwords, locking rooms, muting, disabling tools and others as appropriate. Recording can only happen with permission. Staff need to be in pairs whilst leading lessons using zoom. Etiquette and behaviour online have the same high expectations as in person. Please do not say or accept online behaviour which would harm you in person. Blended learning will be delivered with additional training and good practice guidance from INSET onwards to ensure all our pupils are ready for a potential new lockdown.

What You Need To Do As A Classroom Educator-GDPR For Teachers: At A Glance

Introduction

St Saviour's Primary School aims to ensure that personal information is treated lawfully and correctly. The lawful and correct treatment of personal information is extremely important in maintaining the

confidence of those with whom the school deals and in achieving its objectives. This policy sets out the basis on which the school shall process any personal data from the students, their parents/carers, staff and other parties from whom data is collected. The school, and therefore
any person who handles personal data on behalf of the school, fully endorses and adheres to the data protection principles set out in Article 5 of the GDPR and sections 83-89 DPA 2018 as below and shall be responsible for and be able to demonstrate compliance with the principles outlined below:

The Six Data Protection Principles

Personal Information shall be:

• processed lawfully, fairly and in a transparent manner (lawfulness, fairness and transparency)

• collected for specified explicit and legitimate purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes; (purpose limitation)

• adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed; (data minimisation)

• accurate and where necessary kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay (accuracy)

• kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods in so far as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required to safeguard the rights and freedoms of the data subject (storage limitation)

• processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures (integrity and confidentiality)

Definitions

• Personal data: Means any information relating to an identified or identifiable natural person (data subject). An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

• Personal data breach: Means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, access to personal data transmitted, stored or otherwise processed.

• Consent: Means any freely given, specific, informed and unambiguous indication of wishes, by a statement or clear affirmative action which signifies agreement to the processing of data.

• Special categories of personal data: Is personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purposes of uniquely identifying a natural person, data concerning health or data concerning a natural persons sex life or sexual orientation.
• Processing: Includes any operation or set of operations, whether or not by automated means such as collection, recording, organisation, structuring, storage, adaption or alteration, retrieval, use, disclosure, erasure or destruction.
• Educational records: The right of access to any record of information which relates to a pupil and therefore includes any education, health and care plan and any personal education plan. Educational records do not include information which is processed by a teacher solely for the teacher's own use such as lesson plans.
• Subject Access Request: Right to access to the personal data by the pupil or parent/carer of the pupil.
• Data subject: This will be the person that we collect the data from. This will include pupils, family members and staff.

Processing of Information

The school, through appropriate management controls will, when processing personal information about any individual:
Observe fully the conditions regarding the collection and use of information and meet the school's legal obligations under the GDPR and the Data Protection Act 2018.
Collect and process appropriate information only to the extent that it is needed tofulfil operational needs or to comply with any legal requirement.
Ensure that the individual about whom information is held can exercise their rights under the Act unless an exemption applies for example in relation to education data,
including the right:
• to be informed that processing is being undertaken
• to prevent processing in certain circumstances
• to correct, rectify, block or erase information, which is regarded as incorrect information
• of access to personal information
• to erasure
• to portability where applicable

What Counts as Personal Information?

This is any information held by the school about a living individual, from which that individual can be identified. For example, this includes:
• A name and address or contact details held about pupils, parents and staff and their families
• information attached to a reference number that could be used to identify someone
• a pupil's school record
• photographs of a child
• records of sickness absence
• financial records relating to a child's parent

Processing of Special Categories of Personal Information

The school, through appropriate management controls will, when processing special categories of personal information about any individual:

• Observe fully the conditions regarding the processing of special categories of information as outlined in Article 9 and meet the school's legal obligations underthe GDPR and the Data protection Act 2018. In particular, Schedule 1 Part 4 of the DPA 2018 states that the school must have this policy document in place which explains as below, the procedures for securing compliance with the principles in Article 5 as outlined above.

• Collect and process special categories of data only to the extent that it is needed to fulfil operational needs or to comply with any legal requirement.

• Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs data, data concerning health or data concerning a natural person or trade union membership and the processing of genetic data biometric data for the purpose of uniquely identifying a natural person.

Access to Personal Information

The school will process requests for access to personal information in line with the relevant sections of the GDPR and the Data Protection Act 2018.

Subject Access Requests

Individuals can request a copy of the personal data the school holds about them. Any staff member who receives a valid data protection request must forward it to the Data Protection Officer for the school.

• if more information is required this will be requested from the requester;

• if all information has been received, and the request is a valid subject access request, the school will acknowledge the request and process the request within one month from receipt; unless the request is particularly large and complex in which case the time can be extended for two months.

Access to Educational Records

The Education (Pupil Information) (England) Regulations 2005 allow parents access to the official education records of their children. The school must make a pupil's educational record available for inspection or provide a copy of the record within 15 days of a valid written request by a parent. Any charges for copying will not exceed the cost of supply.

The school may refuse to disclose information under the Pupil Information Regulations where:

• The school would have no right to disclose the information to the pupil under the GDPR and DPA 2018.

• This may be where the information might cause serious harm to the physical or mental health of the pupil or another individual.When providing information to an individual, it is most important that the individual's identity is verified. If in doubt, questions should be asked of the individual, to which only he/she is likely to know the answers. School staff should disclose information in line with the school's Personal Information Request Policy.

The school should not disclose anything on a pupil's record that would be likely to cause serious harm to their physical or mental health or that of anyone else. Therefore, those creating such records should make sure this kind of information is kept separate from the pupil's other records. Where there is a doubt or statutory requirements conflict staff should seek advice in the first instance from the Data

Protection Officer.

Requests From Other Agencies for Personal Information

• Requests from any external agency will be processed in accordance with the GDPR 2017 and Data Protection Act 2018.

• The staff member responsible for dealing with such requests will ensure that any disclosure made without the consent of the pupil is done in accordance with the data protection and other relevant legislation, taking account of an individual's rights as enshrined in the Human Rights Act 1998. Relevant, confidential information should only be disclosed to:

• other members of staff on a need to know basis;

• relevant Parents/Guardians;

• other authorities if it is necessary in the public interest, e.g. prevention of crime;

• other authorities, such as the LEA and schools to which a pupil may move, where there are legitimate requirements (DfEE leaflet 0015/2000 entitled "Pupil Records and Reports" issued in March 2000 covers Data Protection issues and how and what information should be transferred to other schools. DfES/0268/2002 provides further information).

Data Uses and Purposes

All processing of personal data must be for a purpose that is necessary to enable the school to perform its duties and services. Personal information should only be processed in line with those notified purposes. All personal data should be regarded as confidential and its security protected accordingly. This also applies when school information is being processed at members of staff's homes. Information held by the school must not be used for unauthorised non-school purposes. If you become aware of any potential data breach, please refer to section 9 below, and follow the designated procedures accordingly. Personal Information should only be disclosed to persons (internal and external) where their authority to receive it has been explicitly established, e.g. where the information is required by the police for the prevention and detection of crime, or a relevant Information Sharing Agreement is in place. Purposes will include the following:

• Providing education and pastoral care

• Providing activities for pupils including school trips and after school clubs and activities

• Safeguarding and promoting the welfare of children

• Providing references for pupils and staff

• Providing human resources function for staff

• Ancillary purposes to education including completing contractual obligations

• Fundraising

Data Incident Reporting / Data Breach

Staff members must notify Asma Bibi, Data Protection Officer, of any potential data incidents as soon as the incident occurs and in any event within 24 consecutive hours after occurrence. Any reported data incident will be investigated appropriately and actions taken as necessary. If a member of the public reports a potential incident, they can do this by contacting the Data Protection Officer directly by phone on 0207 987 4624 or by e-mail: abibi34.211@lgflmail.org.sch.uk

Personal data breaches will be notified to the Information Commissioner's Office within 72 hours of the incident. All staff members will follow the school's Data Breach guidance manual with associated templates and procedures and the Information Commissioner's Office guidance.

Clear Desk Policy

Classrooms will be tidy, desks should be cleared and resources clearly organised, accessible and labelled. Staff must abide by the following practice points when handling personal data.

Leaving a Room

Whenever a room is unoccupied for an extended period of time you should do the following:

• Remove all sensitive and confidential paperwork from plain sight and lock it in a drawer or filing cabinet. This includes mass storage devices such as USB drives and hard drives, or laptops and iPads.

• Draws should be locked and keys for accessing drawers or filing cabinets should not be left unattended at or near a desk.

• Devices should be screen locked and locked away.

Confidential Waste

• All waste paper which contains sensitive or confidential information must be disposed of either by using the confidential waste bags around school.

• Under no circumstances should this information be placed in regular waste paper bins.

• If the school destroy large scale files such as pupil files or HR records, they should be recorded on the data destruction log.

Computer Screens

• Devices such as iPads/laptops/Chromebooks/tablets/USBs must be locked away at the end of the day.

• Computer workstations must be locked when the desk is unoccupied and completely shut down at the end of the work day.

• Computer / laptop screens to be locked when left unattended.

• An appropriate passcode/password must be set for all accounts. Passwords must be complex (a mix of letters, numbers and special characters) and must not be shared with others.

• Devices are configured to automatically lock after a period of inactivity.

Displays

• Passwords should not be left in open areas which are visible to others.

• Sensitive or confidential personal data displayed in class rooms should not be left visible or displayed to unauthorised persons.

• Personal data (including but not limited to seating plans, allergy details and student lists) shall be stored in folders or in secure places.

• When sharing screen to the class, the school will ensure that no personal data is shared on the projector.

• Before displaying any names and photos, the school will ensure that the student/parent has provided consent.

• The School will limit the amount of data on displays. If names are necessary, only first names will be used.

Taking Data Off-Site

• You are responsible for security of the data in your possession and when transporting it off site you must always take steps to keep it secure.

• Paper documents are not removed from the School without the prior permission of SLT. When such permission is given reasonable steps must be taken to ensure the confidentiality of the information is maintained during transit. In particular, the information is not to be transported in see-through bags or other un-secured storage containers.

• Paper documents should not be used in public spaces and not left unattended in any place where it is at risk (e.g. in car boots, in a luggage rack on public transport).

• Paper documents taken home or printed at home containing personal information, sensitive data and confidential information are not left around where they can be seen, accessed or removed.

• Paper documents are collected from printers as soon as they are produced and not left where they can be casually read.

• The master copy of the data is not to be removed from School premises.

• Paper documents containing personal data are locked away in suitable facilities such as secure filing cabinets in the home just as they would be in School.

• Documents containing confidential personal information are not pinned to noticeboards where other members of the household may be able to view them.

• Paper documents are disposed of securely by shredding and should not be disposed of with the ordinary waste unless it has been shredded first.

Printing

• Any print jobs containing personal information should be retrieved immediately.

• To release printing the school will use Quick Print release button on the screen.

• All print jobs will be wiped from the system at the end of each week.

Compliance

If you have misplaced any information, then you must let SLT know as quickly as possible.

Lone Working

Staff are encouraged not to work alone in school. Work carried out unaccompanied or without immediate access to assistance should be risk assessed to determine if the activity is necessary. Work involving potentially significant risks (for example work at height) should not be undertaken whilst working alone.

Where lone working cannot be avoided staff should:

• Obtain the Head of School's permission and notify Asma Bibi on each occasion when lone working will occur.

• Ensure they do not put themselves or others at risk.

• Ensure they have means to summon help in an emergency e.g. access to a telephone or mobile telephone etc.

• When working off site notify a colleague of their whereabouts and the estimated time of return. Staff undertaking home visits to obtain as much background information as possible about the child/family being visited. In most circumstances visits should be done by two staff.
• Key holders attending empty premises where there has been an incident or suspected crime should do so with a colleague if possible. They should not enter the premises unless they are sure it is safe to do so.
• Report any incidents or situations where they may have felt “uncomfortable”.

Home and Unaccompanied Visits

No lone home visits to be undertaken by staff. All home visits need to have prior SLT agreement.