St Austin's Catholic

Primary School

Laborare est Orare

To work is to pray

Online Safety Policy

Autumn (1) 2023

Policy agreed by the Full Governing Body of St Austin's Primary School:

On: ....18th October 2023…..... **Signed:......** (Chair of Governors)

To be reviewed:....... Autumn (1) 2025.........

"In our school, where everyone is special,
we will love and serve as Jesus taught"

"En nuestro colegio todos somos especiales.
Amaremos y serviremos como Jesús nos enseñó"

St Austin's Catholic Primary School
Online Safety Policy - 2023/4

Forward

In the light of changes to KCSIE – the most significant change relating to filtering and monitoring.

The DSL / DDSL will now take lead responsibility for web-filtering and monitoring. We will follow the new DfE standards as to the roles and responsibilities of all staff and DSLs and SLs. Our Tech teams; *Computeam* and *MGL* will work closely with DSL/ DDSLs. Technicians will be charged to carry out regular checks and feed back to SLT (DSL) teams. All staff need to be aware of the changes and renewed emphasis and play their part in feeding back about overblocking or gaps in the filtering provision.
We will constantly review our approaches to monitoring in line with the standards (note that filtering and monitoring are not the same – guidance can be found at https://safefiltering.lgfl.net).

Introduction

Key People and Dates

St Austin's Catholic Primary School	Designated Safeguarding Lead (DSL), with lead responsibility for filtering and monitoring	Mrs Colette Hickey
	Deputy Designated Safeguarding Leads / DSL Team Members	Mrs Jane Doyle and Mrs Alison Kelly
	Link governor for safeguarding	Mrs Ruth Culley
	Link governor for webfiltering	Mr Steven Tallant
	Curriculum leads with relevance to online safeguarding and their role (PSHE/RSHE/RSE/Computing)	Mrs Alison Kelly – Curriculum Lead Mr Jonathan Hughes – Computing Miss Ciara Sullivan – PSHE Miss Emma Vallely - RSHE
	Network manager an or other technical support	Mr Luke Edwards
	Date this policy was reviewed and by whom	FGB – October 2023
	Date of next review and by whom	FGB – October 2024

Online Safety Policy Rationale

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), online safety, PHSE policy and statutory RSHE guidance. It is cross-curricular (with relevance beyond Relationships, Health and Sex Education, Citizenship and Computing) and designed to sit alongside our Child Protection & Safeguarding Policy.

Any issues and concerns with online safety must always follow the school's safeguarding and child protection procedures.

Reviewed

A full annual review and or 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, St Austin's staff, governors, pupils and parents will be fully consulted when reviewing the policy.

Stakeholders understand the rules that are in place and why, and that the policy affects day-to-day practice. Acceptable Use Policies (see appendices) are available. These are reviewed alongside this overarching policy.

Accountability

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

Main online safety risks

Current Online Safeguarding Trends

In our school over the past year, we have particularly noticed the following in terms of device use and abuse and types of online/device-based incidents which affect the wellbeing and safeguarding of our students: In December 2022 we observed pupil messages using WhatsApp, snapchat and Instagram which we unacceptable. This led to workshops for pupils and parents.

Nationally, some of the latest trends of the past twelve months are outlined below. Acceptable use agreements are shared with children, parents and staff within the context of the **5 Cs** (KCSIE). Our aim, as a whole-school, is to approach safeguarding which 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 pupils having often unconstrained access to tools that generate text and images at home. These tools not only represent a challenge in terms of accuracy when pupils are genuinely looking for information, but also in terms of plagiarism for teachers: 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 inappropriate language, systems can produce inappropriate material. Schools not only need to tackle this in terms of what comes into school but also educating pupils and parents on use of these tools in the home. **SEE AUP STATEMENTS**

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 as staff, continue to teach best practice, while remembering the reality for most of our pupils is quite different.

Findings from the report found: *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: *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.*

Research has found 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.

Accessibility

This policy can only impact upon practice if it is a living document. It will be accessible by all stakeholders. It will be communicated in the following ways:

- Posted on the school website
- Displayed in the school office
- Part of school induction pack for <u>all</u> new staff (including temporary, supply and non-classroom)-
- Integral to safeguarding updates and training for all staff (September refreshers)
- Clearly reflected in the Acceptable Use Policies (AUPs) for staff, volunteers, contractors, governors, pupils and parents/carers on entry.

Thank you for your cooperation in reading and adhering to the following policy

St Austin's Catholic Primary School
Online Safety Policy - 2023/4

Laborare est Orare

To work is to pray

Safeguarding Governor – Mrs R. Culley

Head teacher / DSL – Mrs Hickey

Deputy Head teacher / DDSL – Mrs Doyle

Assistant Head teacher – Mrs Kelly

Computing Lead – Mr Hughes

MGL Computer Teacher – Miss A. Rogan

IT Technician – Mr L. Edwards

Policy Review: October 2024

Contents

Overview

Aims

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

- Setting out expectations for all St Austin's Catholic School community members' online behaviour, attitudes and activities and use of digital technology (including when devices are offline)
- Helping safeguarding and senior leadership teams to have a better understanding and awareness of all elements of online safeguarding through effective collaboration and communication with technical colleagues (e.g. for filtering and monitoring), curriculum leads (e.g. RSHE) and beyond.
- Helping all stakeholders to recognise that online/digital behaviour standards (including social media activity) must be upheld beyond the confines of the school gates and school day, regardless of device or platform, and that the same standards of behaviour apply online and offline.
- Facilitating the safe, responsible, respectful and positive use of technology to support teaching & learning, increase attainment and prepare children and young people for the risks and opportunities of today's and tomorrow's digital world, to survive and thrive online
- Helping school staff working with children to understand their roles and responsibilities to work safely and responsibly with technology and the online world:
    - for the protection and benefit of the children and young people in their care
    - 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

Reporting and support should be followed as documented in all safeguarding and child protection policy documents, especially in response to incidents, which should be reported in line with our Child Protection & Safeguarding Policy. DSL / DDSLs will handle referrals (MARF) to local authority multi-agency safeguarding hubs (MASH) and will take charge of referrals to the LA designated officer (LADO).

Parents will be made aware that support is available at **reporting.lgfl.net** . This list of curated links to external support and helplines for both pupils, parents 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 will be useful for the school community and anonymous support for children and young people is also available.

Training is also available via **safetraining.lgfl.net**

Scope

This policy applies to all members of the St Austin's Catholic Primary 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.

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 is 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

In our school online safety builds on what pupils have already learned and identifies subject content that is appropriate for their stage of development.

As well as teaching the underpinning knowledge and behaviours that help pupils navigate the online world safely and confidently (regardless of the device) a whole school approach is undertaken by all . Teachers tailor teaching and support those with specific needs of pupils, including vulnerable pupils – safeguarding training and dedicate time (23/24) will support curriculum mapping for RSHE/PSHE and online safety leads to access training at safetraining.lgfl.net:

- RSHE
- PSHE
- Computing
- SEND

All staff will identify opportunities to thread online safety through all school activities, both outside the classroom and within the curriculum, supporting curriculum/phase/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.

At St Austin's Catholic Primary, we recognise that online safety and broader digital resilience must be thread throughout the curriculum through MGL scheme and specialist teacher (MGL)

Our Curriculum reviews allow leaders the opportunity to look at 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. See Computing curriculum

An online 23-24 annual online safety audit, a collaborative effort led by Curriculum lead, PSHE lead, Computing lead and MGL specialist teacher will ensure all pupils have the knowledge and skills to stay safe. This is part of our curriculum safeguarding offer in the School Development Plan. (SDP)

Handling safeguarding concerns and incidents

Online safety is a part of safeguarding as well as being a curriculum strand of Computing, PSHE/RSHE and Citizenship.

General concerns will be handled in the same way as any other safeguarding concern; all stakeholders should inform the online-safety lead / designated safeguarding lead to contribute to the overall picture or highlight even low-level concerns.

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). These concerns should be shared DSL/ DDSLs through CPOMS or verbally depending on severity.

School procedures for dealing with online safety will be mostly detailed in the online safety policy and the following policies

- Safeguarding and Child Protection Policy
- Anti-Bullying Policy
- Relationships and Behaviour Policy (including school sanctions)
- Acceptable Use Policies

- Prevent Risk Assessment / Policy
- LA Data Protection Policy, agreements and other documentation (e.g. privacy statement and consent forms for data sharing, image use etc)
- Cybersecurity

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 DSL/ DDSL 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. Reporting will then be followed up and recorded on CPOMS.

Any concern/allegation about staff misuse is always referred directly to the Headteacher, unless the concern is about the Headteacher in which case the complaint is referred to the Chair of Governors and the LADO (Local Authority's Designated Officer). Staff may also use the NSPCC Whistleblowing Helpline.

The school will actively seek support from other agencies as needed (i.e. the local authority, school improvement Liverpool, LGfL, UK Safer Internet Centre's Professionals' Online Safety Helpline (POSH), NCA CEOP, Prevent Officer, Police, IWF and Harmful Sexual Behaviour Support Service and FMU).

The DfE guidance Behaviour in Schools, advice for headteachers and school staff September 2023 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.)

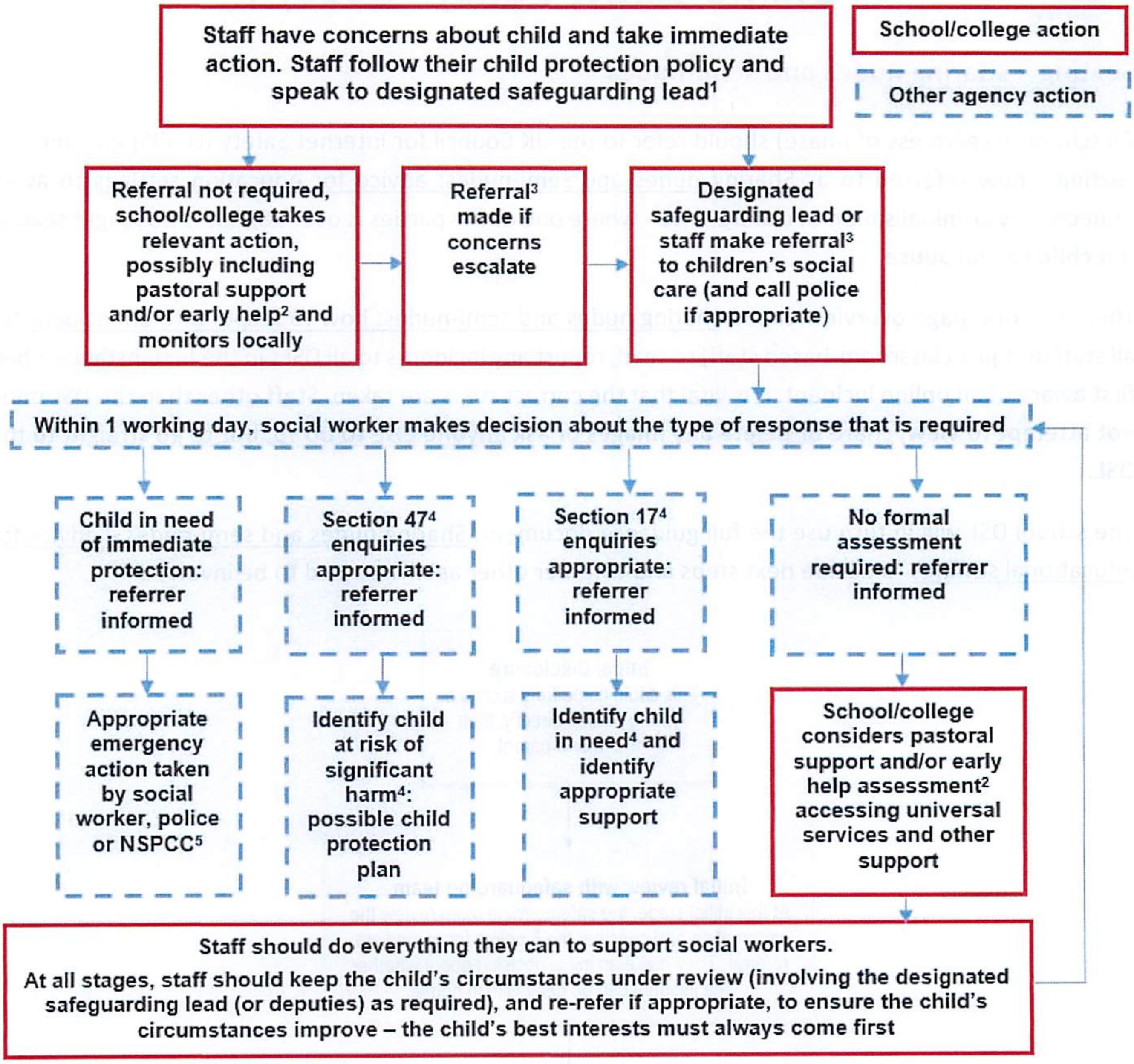
We will inform parents/carers of online-safety incidents involving their child, and the Police where staff or pupils engage in or are subject to behaviour which we considered criminal, is particular hate crime, sexting and upskirting.

St Austin's School, the DSL will evaluate whether reporting procedures are adequate for any future closures/lockdowns/isolations.

Actions where there are concerns about a child

The following flow chart is taken from Keeping Children Safe in Education 2023 as the key education safeguarding document.

As outlined previously, online safety concerns are no different to any other safeguarding concern.



School/college action

Other agency action

Staff have concerns about child and take immediate action. Staff follow their child protection policy and speak to designated safeguarding lead[1]

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

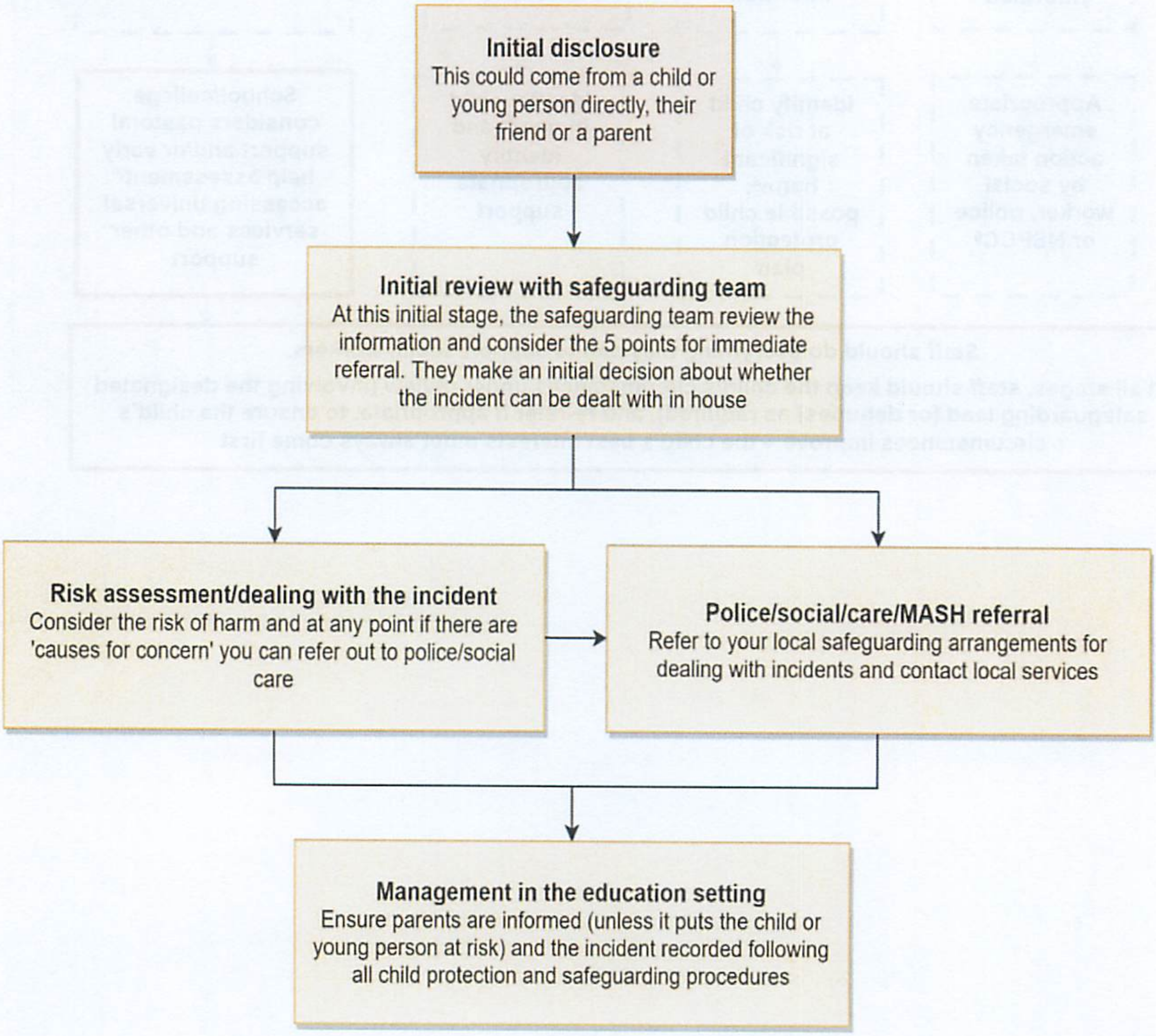
Staff should do everything they can to support social workers.
At all stages, staff should keep the child's circumstances under review (involving the designated safeguarding lead (or deputies) as required), and re-refer if appropriate, to ensure the child's circumstances improve – the child's best interests 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, report any incidents to all DSLs in the first instance when first aware of an online incident. It is vital that the correct steps are taken. **Staff other than the DSL must not attempt to view, share or delete any images 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.



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

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

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

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

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

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

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

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. Materials to support teaching about sexting can be found at sexting.lgfl.net

Upskirting

Upskirting (taking a photo of someone under their clothing, not necessarily a skirt) is now a criminal offence and constitutes a form of sexual harassment as highlighted in Keeping Children Safe in Education this is deemed child on child abuse.

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 anti-bullying policy should be followed for online bullying, which may also be referred to as cyberbullying, including issues arising from banter. School policies

When considering bullying, staff will be reminded of issues such as reports of fights being filmed and fake profiles being used to bully children in the name of others. Any homophobic, racist and sexist language used explicitly towards others is seen as hate crime. (Age of responsibility being 10)

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' Any incident of sexual harassment or violence (online or offline) should be reported to the DSL who will follow the full guidance.

As a whole school approach, we instil a zero-tolerance culture and maintain an attitude of ***'it could happen here'.*** Our school takes 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. Specific reference to behaviours such as bra-strap flicking and the careless use of language will be dealt with immediately.

Children are aware, though online safety teaching, of the negative online environment and the mental health impact this can have on others. Through internet safety day, mental health days, wellbeing week and computer clubs we offer opportunities for children to discuss.

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

Clear and well communicated rules and procedures 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 Safeguarding Policies for pupils, parents and staff.

Where pupils breach 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/safer working practices.

These documents are sent to all staff at the beginning of each school year. /During computer lessons we ensure that the pupils are aware that **the same rules apply 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 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 incidents will be discovered in the coming year. Our school will ensure that pupils and staff will increase scrutiny at the start of the year.

Social media incidents

These incidents / breaches will be dealt with in line with the school behaviour policy (for pupils) or code of conduct/safer working practices (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 Austin's will request that the post be deleted. Disciplinary procedures will be undertaken.

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 GDPR LA policy. Data protection and cybersecurity and a school's ability to effectively safeguard children and families can be found in KCSIE (2023) which also refers to the DfE Standards of Cybersecurity for the first time in 2023.

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 states that "appropriate" web - filtering and monitoring systems which keep children safe online but do not "overblock" should be in place.

Since KCSIE 2023, in recognition of the importance of these systems to keeping children safe, the DSL/ DDSLs are responsible for filtering and monitoring (see page 1 for the DSL name and the named governor with responsibility for filtering and monitoring).

St Austin's will follow, alongside *Compteam*, the new DfE filtering and monitoring standards, we will

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

As a school we will work closely with *Computeam* and MGL and relevant safeguarding teams. Our IT Development technician will be charged in carrying out regular checks to feed back to DSL/ DDLS.

ALL STAFF need to play their part in responding to online areas of concern, potential for pupils who can bypass systems and any potential overblocking. They can submit concerns at any point via CPOMS and IT email. Regular checks will then immediately follow, either internally or externally, depending on the nature of the concern. Guidance at (safefiltering.lgfl.net)

Staff induction will indicate systems in place and staff responsibilities regarding safeguarding as well as via AUPs. Termly staff safeguarding training will highlight regular checks that will be carried out. These will carried out by St Austin's IT development team, including DSL and *Compute am.* Information will be shared with staff and governors at FGB meeting and directed times.

Staff will be aware of the differences between filtering and monitoring, the meaning of *over blocking* and other terminology. Training for all staff, safeguarding teams and technical teams as available through guidance videos and flyers using. https://safefiltering.lgfl.net and safetraining.lgfl.net

At St Austin's Catholic primary school

- web filtering is provided by National Grid for Learning (NGfL) on school site alongside LCC and computeam
- Changes can be made by Mrs Hickey, Mr Tallant, Miss Waldron and Mr Edwards.
- Overall responsibility is held by the DSL / Mrs Hickey with further SLT support from computeam
- Technical support and advice, setup and configuration are from LCC and Computeam
- Regular checks are made half termly by Computeam to ensure filtering is still active and functioning everywhere.
- An annual review is carried out, in October, as part of the online safety audit to ensure a whole school approach – a template is available at onlinesafetyaudit.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 (air server)
- network monitoring using log files of internet traffic and web access by NgFL
- individual device monitoring through software or third-party services NgFL

At St Austin's Catholic Primary, we use

We use all the above strategies alongside the support of NgFL, Computeam and LCC

All devices linked to the school network and Wi-Fi are filtered and monitored

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

Authorised systems

- Pupils at this school do not communicate with each other using any of our internal platforms. Children in Ks2 use Google Classroom, for homework task which are directly linked to the class teacher. In Ks1 children can access Purple Mash.
- My Maths and numbots are learning platforms for children to access however no communication systems are open allowing children to message each other.
- Teachers only, have access to use/send/view/respond.
- Staff at St Austin's use the email system provided by Gmail for all school emails. Staff will not use personal/private email account (or other messaging platform) Staff will not communicate with children or parents using personal email or personal school email address – all communication is through enquiries@st-austins.co.uk
- Staff at St Austin's also use CPOMS to communicate any concerns internally.
- Any systems above are centrally managed and administered by the school or authorised IT provider (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 (other than google classroom, purple mash, twitter) with communication facilities or any child login or storing school/child data must be approved in advance by the school and centrally managed by the Head teacher supported by our IT technician and IT external provider.
- Any unauthorised attempt to use a different system may be a safeguarding concern or disciplinary matter. DSL should be notified immediately.
- Where devices have multiple accounts for the same app, mistakes can happen, such as an email being sent from or data being uploaded to the wrong account. If this a private account is used for communication or to store data by mistake, the DSL/Headteacher/DPO (the particular circumstances of the incident will determine whose remit this is) should be informed immediately.

Behaviour / usage principles

- More detail for all the points below are given in the Social media section of this policy as well as our acceptable use agreements, behaviour policy and staff code of conduct. School Policies
- 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 Local authority Data Protection Policy – which includes notices to; *password hygiene, cybersecurity, data protection best practice, privacy statements, collaboration with your DPO, file sharing permissions and procedures, use of two-factor authentication, parental permissions, consent to pupil work being displayed, the differences between consumer and education products (e.g. a private Gmail account or Google Drive and those belonging to a managed educational domain*) and only using the authorised systems mentioned above.
- All staff are allowed to use the email system for reasonable (not excessive, not during lessons) personal use but should be aware that all use is monitored, their emails may be read and the same rules of appropriate behaviour apply at all times. Emails using inappropriate language, images, malware or to adult sites may be blocked and not arrive at their intended destination (and will be dealt with according to the appropriate policy and procedure through the LA)
- Pupils access Google Classroom, Purple Mash, My Maths and TT Rockstars).

Online storage or learning platforms

All the principles outlined above also apply to any system to which staff log in online to conduct school business, whether it is to simply store files or data on the server or cloud or collaborate, learn, teach, etc.

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 Headteacher and Governors have delegated the day-to-day responsibility of updating the content of the website and ensuring compliance with DfE stipulations to Website lead and IT technician.

The site is managed by / hosted by ParentAPP owned by Community Brands Ltd.

All staff submitting information on our website, will remember we have the same duty as any person or organisation to respect and uphold copyright law. Staff must always credit where material has been found and only used with permission. When necessary open-access libraries of public-domain images/sounds will be used. Finding something on Google or YouTube does not mean that copyright has been respected. If in doubt, check with IT technical team.

Digital images and video

At St Austin's school, parents/carers are requested to give consent for their child's image to be captured in photographs or videos, which is needed beyond internal use (e.g. Twitter, school website)

Parents will answer as follows: These options, on our consent form, check the following

- For displays around the school
- For filming school plays
- For the newspaper
- For the school websites
- For social media (Twitter)
- For a specific high-profile image for display

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. This register is held centrally for staff to access

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 Austin's Catholic School, no member of staff will ever use their personal phone to capture photos or videos of pupils.

Photos are stored in the **digital content** folder on the school server in line with the retention schedule of the school Data Protection Policy.

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

We encourage pupils to think about their online reputation and digital footprint, so we, as adults are role models by not oversharing and behaving appropriately online.

Through our safeguarding curriculum, pupils are taught about how images can be manipulated and 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 Austin's Catholic Primary 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. Mr J. Hughes is responsible for managing our X-Twitter and other social media accounts by 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. We expect the same standards from our pupils and parents.

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 the profession into disrepute. This applies both to public pages and to private posts, e.g. parent chats, pages or groups.

If parents have a concern about the school, we would urge them to contact us directly and in private to resolve the matter. If an issue cannot be resolved in this way, the school complaints procedure which can be found on the school website 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+) however, our staff regularly deal with issues arising on social media involving pupils/students under the age of 11. 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 with whom, for how long, and when **(late at night / in bedrooms is not helpful for a good night's sleep and productive teaching and learning at school the next day).** You may wish to refer to the Digital Family Agreement to help establish shared expectations and the Top Tips for Parents poster along with relevant items and support available from parentsafe.lgfl.net and introduce the Children's Commission Digital 5 A Day.

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

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

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

Parents/ pupils are discouraged from 'following' staff, governor, volunteer or contractor public accounts as laid out in the AUPs. However, we accept that this can be hard to control (but this highlights the need for staff to remain professional in their private lives). In the reverse situation, however, staff must not follow such public pupil accounts.

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

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

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

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

All members of the school community are reminded that particularly in the context of social media, it is important to comply with the school policy on Digital images and video and permission is sought before uploading photographs, videos or any other information about other people. (SEE LETTER TO PARENTS)

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

Device usage

AUPs remind those with access to school devices about rules on the misuse of school technology – devices used at home should be used just like if they were in full view of a teacher or colleague. Please read the following in conjunction with those AUPs and the sections of this document which impact upon device usage, e.g. copyright, data protection, social media, misuse of technology, and digital images and video.

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

- **Pupils** are not allowed to bring mobile phones in to school. Those children who do are to leave their devices, including wearable technology at the school office were these can be locked away. Any attempt to use a phone in lessons without permission or to take illicit photographs or videos will lead to sanctions. Safeguarding Policies
- Important messages and phone calls to or from parents can be made at the school office, which will also pass on messages from parents to pupils in emergencies.
- **All staff who work directly with children** should leave their mobile phones on silent and only use them in private staff areas during school hours. See also the 'Digital images and video' section of this document and the school data protection cybersecurity policies. Child/staff data should never be downloaded onto a private phone. If a staff member is expecting an important personal call when teaching or otherwise on duty, they must ask for permission from DSL/ DDSL.
- **Volunteers, contractors, governors** should leave their phones in their pockets and turned off. Under no circumstances should they be used in the presence of children or to take photographs or videos. If this is required (e.g. for contractors to take photos of equipment or buildings), permission of the headteacher should be sought 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. Parents are not permitted to take photographs of any event which compromises others children's safety. 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

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 members for 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 pupils 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 Headteacher. Teachers using their personal phone in an emergency will ensure that the number is hidden to avoid a parent or student accessing a teacher's private phone number.

Searching and confiscation

In line with the DfE guidance 'Searching, screening and confiscation: advice for schools', the Headteacher 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.

Appendix – Roles

Relevant roles & responsibilities:

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

Roles:

- All Staff
- Headteacher – Mrs Hickey
- Designated Safeguarding Lead – Mrs Hickey and Mrs Doyle
- Governing Body, led by Online Safety / Safeguarding Link Governor - Mrs Culley & Mr Tallant
- PSHE / RSHE Lead/s – Miss Sullivan, Mrs Vallely, Mrs Hughes
- Computing Lead – Mr Hughes
- Subject Leaders – all staff
- Network Manager
- External provider – Simon Jobe, Computeam
- Data Protection Officer (DPO)
- Volunteers and contractors
- 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 Safeguarding Policies and relevant parts of Keeping Children Safe in Education Part one 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 and guidance (such as KCSIE), modelling safe, responsible and professional behaviours in their own use of technology at school and beyond and avoiding scaring, victim-blaming language.

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

Headteacher – Mrs C. Hickey

Key responsibilities:

- Foster a culture of safeguarding where online-safety is fully integrated into whole-school safeguarding
- Oversee and support the activities of the designated safeguarding lead team and ensure they work technical colleagues to complete an online safety audit in line with KCSIE (including technology in use in the school)
- Undertake training in offline and online safeguarding, in accordance with statutory guidance and Local Safeguarding Children Partnership support and guidance
- Ensure ALL staff undergo safeguarding training (including online-safety) at induction and with regular updates and that they agree and adhere to policies and procedures
- Ensure ALL governors and trustees undergo safeguarding and child protection training and updates (including online-safety) to provide strategic challenge and oversight into policy and practice and that governors are regularly updated on the nature and effectiveness of the school's arrangements
- 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.
- In 2023/4, in line with new additional advice, regular checks and annual reviews, upskilling the DSL and appointing a filtering and monitoring governor will be actioned

- Liaise with the designated safeguarding lead on all online-safety issues which might arise and receive regular updates on school issues and broader policy and practice information
- Support safeguarding leads and technical staff as they review protections for pupils in the home and remote-learning procedures, rules and safeguards
- Take overall responsibility for data management and information security ensuring the school's provision follows best practice in information handling; work with the DPO at LCC, DSL and governors to ensure a compliant framework for storing data, but helping to ensure that child protection is always put first and data-protection processes support careful and legal sharing of information
- Understand and make all staff aware of procedures to be followed in the event of a serious online safeguarding incident
- Ensure suitable risk assessments are undertaken so the curriculum meets needs of pupils, including risk of children being radicalised
- Ensure the school website meets statutory requirements

Designated Safeguarding Lead / Online Safety Lead – Mrs C. Hickey and Mrs J Doyle

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
- 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
- Ensure ALL staff and supply staff undergo safeguarding and child protection training (including online-safety) at induction and that this is regularly updated.
- all staff must read KCSIE Part 1 and all those working with children also Annex B –
- 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

- 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. Staff will work to frame conversations linguistically reducing any 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
- Work with the headteacher, DPO and governors to ensure a compliant framework for storing data, but helping to ensure that child protection is always put first and data-protection processes support careful and legal sharing of information
- Stay up to date with the latest trends in online safeguarding and "undertake Prevent awareness training." – see safetraining.lgfl.net and prevent.lgfl.net
- Review and update this policy, other online safety documents (e.g. Acceptable Use Policies) and the strategy on which they are based (in harmony with policies for behaviour, safeguarding, Prevent and others) and submit for review to the governors/trustees.
- Receive regular updates in online-safety issues and legislation, be aware of local and school trends – see safeblog.lgfl.net for examples or sign up to the LGfL safeguarding newsletter
- Ensure that online-safety education is embedded across the curriculum in line with the statutory RSHE guidance (e.g. by use of the updated UKCIS framework 'Education for a Connected World – 2020 edition') and beyond, in wider school life
- Promote an awareness of and commitment to online-safety throughout the school community, with a strong focus on parents, including hard-to-reach parents – dedicated resources at parentsafe.lgfl.net
- Communicate regularly with SLT and the safeguarding governor/committee to discuss current issues (anonymised), review incident logs and filtering/change control logs and discuss how filtering and monitoring work and have been functioning/helping.
- Ensure all staff are aware of the procedures that need to be followed in the event of an online safety incident, and that these are logged in the same way as any other safeguarding incident.
- Ensure adequate provision for staff to flag issues when not in school and for pupils to disclose issues when off site, especially when in isolation/quarantine, e.g. a survey to facilitate disclosures and an online form on the school home page about 'something that worrying me' that gets mailed securely to the DSL inbox
- Ensure staff adopt a zero-tolerance, whole school approach to all forms of child-on-child abuse, and don't dismiss it as banter (including bullying).
- Pay particular attention to **online tutors**, both those engaged by the school as part of the DfE scheme who can be asked to sign the contractor AUP and those hired by parents. **CHECK** the Online Tutors – Keeping Children Safe poster at parentsafe.lgfl.net . This can remind parents of key safeguarding principles

Governing Body, led by Online Safety / Safeguarding Link Governor – Mrs R Culley

Key responsibilities are to

- Approve this policy and strategy and subsequently review its effectiveness using Online safety in schools and colleges: Questions from the Governing Board
- Undergo safeguarding and child protection training (including online safety) at induction to provide strategic challenge, ensuring this is regularly updated
- 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
- 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 approach to online safety with a clear policy on the use of mobile technology.

PSHE / RSHE Lead/s – Miss C Sullivan and Miss E Vallely

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 personal, social, health and economic (PSHE) curriculum and relationships, sex and health education (RSHE). "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.

- We focus on the underpinning knowledge and behaviours outlined in Teaching Online Safety in Schools in an age appropriate way to help pupils navigate the online world safely and confidently regardless of their device, platform or app.
- Assess teaching to "identify where pupils need extra support or intervention through tests, written assignments or self evaluations, to capture progress" to complement the computing curriculum.
- Work closely with the DSL 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 – Mr J Hughes

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, PSHE leads and MGL outreach provider to avoid overlap but ensure a complementary whole-school approach
- Work closely with the DSL/DDSL and all other staff to ensure an understanding of the issues, approaches and messaging within Computing
- Collaborate with technical staff and others responsible for ICT use in school to ensure a common and consistent approach, in line with acceptable-use agreements

Subject Leaders

Key responsibilities:

- As listed in the 'all staff' section, plus:
- Look for opportunities to embed online safety in your subject or aspect, especially as part of the RSHE, PHSE curriculum, and model positive attitudes and approaches
- Consider how Teaching Online Safety in Schools can be applied in any context within your subject area
- Work closely with the DSL/DDSL and all other staff to ensure an understanding of the issues, approaches and messaging within technologies used as an educational tool
- Ensure subject specific action plans also have an online-safety element

Network Manager/other technical support roles – Computeam and Mr L Edwards

Key responsibilities:

- As listed in the 'all staff' section, plus:
- Collaborate regularly with the DSL and leadership team to help them make key strategic decisions around the safeguarding elements of technology.
- Note that KCSIE changes expect a great understanding of technology and its role in safeguarding when it comes to filtering and monitoring and in 2023/4 you will be required to support safeguarding teams to understand and manage these systems and carry out regular reviews and annual checks.
- Support DSLs and SLT to carry out an annual online safety audit as now recommended in KCSIE. This should also include a review of technology, including filtering and monitoring systems (what is allowed, blocked and why and how 'over blocking' is avoided as per KCSIE) to support their role as per the new DfE standards, protections for pupils in the home and remote-learning.
- Keep up to date with the school's online safety policy and technical information in order to effectively carry out their online safety role and to inform and update others as relevant
- Work closely with the designated safeguarding lead / online safety lead / data protection officer / 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
- As part of a team, monitor the use of school technology, online platforms and social media presence and that any misuse/attempted misuse is identified and reported in line with school policy
- Work with the Headteacher to ensure the school website meets statutory DfE requirements

Data Protection Officer (DPO) – Mr M Jones

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 mentors, students and tutors)

Key responsibilities:

- Read, understand, sign and adhere to an acceptable use policy (AUP)
- Report any concerns, no matter how small, to the designated safeguarding 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 our school, and will never do so directly with a pupil. The same applies to any private/direct communication with a pupils.

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 – etc SAPTA

Key responsibilities:

- SAPTA, Governing Body, Spanish lead and external curriculum club lead will sign an acceptable use policy prior to using technology or the internet within our school.
- External groups will support our 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