Online Safety Policy

Linked Documents
Anti-Bullying Policy
Child Protection and Safeguarding Policy
Children and Parents: Media Use and Attitudes Report 2023 (Ofcom)
Keeping Children Safe in Education 2024
Internet Watch Foundation Annual Report 2023
Positive Behaviour Policy
Personal, Social, Health and Economic Education Policy
Revealing-Reality: Anti-social-Media Report 2023
Teaching Online Safety in Schools (DfE 2023)

Date agreed by Governors	Autumn 2024
Next Review	Autumn 2025

The United Nations Convention on the Rights of the Child (UNCRC) articles which inform this policy are:

- Article 3: The best interest of the child must be top priority in all decisions and actions that affect children
- Article 12: Every child has the right to express their views, feelings and wishes in all matters affecting them, and to have their views considered and taken seriously.
- Article 28: Every child has the right to education. Discipline in schools must respect children's dignity and their rights.
- Article 29: Education must develop every child's personality, talents and abilities to the full. It must encourage the child's respect for human rights, as well as respect for their parents, their own and other cultures, and their environment.
- Article 31: Every child has the right to relax, play and take part in a wide range of cultural and artistic activities.

School's Purpose: To prepare pupils for lifelong success

School's Vision: At Godwin Junior School we:

- Value everyone
- Instil a love of learning
- Seek and encourage talent
- Inspire resilient learners
- Open minds to develop responsible global citizens
- Nurture confident, articulate individuals

Designated Safeguarding Lead (DSL), with lead responsibility for filtering and monitoring	Joanne Ince
Deputy Designated Safeguarding Leads / DSL Team Members	Sine Brown Tehira Aslam
Link governor for safeguarding	Ifeoma Ejuh
Curriculum leads with relevance to online safeguarding and their role	Celia Jones (PSHE Lead)

Online safety is an integral part of safeguarding and requires a whole school, cross-curricular approach and collaboration between key school leads.

This policy applies to all members of the school community (including staff, pupils, governors, volunteers, contractors, parents/carers, visitors and community users) who have access to and are users of our school IT systems, both in and out of the school.

KCSIE makes clear that "the Designated Safeguarding Lead (DSL) 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 will plan the curriculum for their area, it is important that this ties into a whole-school approach.

Current Online Safeguarding Risks

The main areas of risk for our school community can be summarised as follows:

Content:

- Exposure to inappropriate content
- Lifestyle websites promoting harmful behaviours
- Hate content and misinformation or fake news
- Content validation: how to check authenticity and accuracy of online content

Contact:

- Grooming [sexual exploitation, radicalisation, catfishing (creating a fake identity to target an individual for abuse or fraud) etc.]
- Online bullying in all forms
- Social or commercial identity theft, including passwords

Conduct:

- Aggressive behaviours (bullying)
- Privacy issues, including disclosure of personal information
- Digital footprint and online reputation
- Health and well-being (amount of time spent online, gambling, body image)
- Sexting
- Copyright and plagiarism (little care or consideration for intellectual property and ownership)

In our school, 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:

- outside of school, the use of instant messaging services between older pupils, between small groups of friends, and incidents of cyber-bullying resulting from this
- pupils watching live-streamer content (which is challenging to monitor and administrate live)
- use of video-sharing services such as TikTok which are not age-appropriate for pupils at Key Stage 2
- use of videogame systems such as Roblox and Fortnite which are not by default age-appropriate for use by pupils at Key Stage 2

Nationally, recent trends include:
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/carers 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.

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 are on these apps regardless of age limits, which are often misunderstood or ignored. We therefore remind about best practice, while remembering the reality for most of our pupils is quite different.

This is striking when you consider that 20% of 3-4 year olds have access to their OWN mobile phone, 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.

Recently, an increasing number of 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. This has coincided with the rise of misogynistic influencers such as Andrew Tate, which had a significant influence on many young boys, which schools have had to counter.

Research conducted by the London Grid for Learning (LGfL) has revealed 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 pupils and also spread defamatory allegations about staff, and also for pupils, including where these are used to bully others

Aims

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

- Setting out expectations for all Godwin Junior School community members' online behaviour, attitudes and activities and use of digital technology (including when devices are offline).
- Helping the Senior Leadership Team 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 and learning, increase attainment and prepare children 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 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 our 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 Positive Behaviour Policy or Anti-Bullying Policy)

Roles and responsibilities

Godwin Junior 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. 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

Pupils

The education of pupils in online safety is an essential part of our school's online safety provision. Children need the help and support of the school to recognise and avoid online risks and build their resilience, and so at Godwin Junior School we adopt a whole-school approach to online safety.

Godwin Junior School:

- Has a clear, progressive online safety education programme, underpinned by the comprehensive Natterhub online safety learning delivery system and scheme of work, which are facilitated as part of the Computing curriculum. This covers a range of skills and behaviours appropriate to pupils' age and experience, and provides a logical progression from year group to year group
- Threads online safety learning through integrated curriculum areas, including lessons in PSHE
- Plans use of the World Wide Web and internet services carefully across all possible use cases to ensure that it is age-appropriate and supports the learning objectives for specific curriculum areas
- Will remind children about their responsibilities through the pupil Acceptable Use Agreement, as well as explicitly during lessons that make use of digital technologies
- Ensures staff are aware of their responsibility to model safe and responsible behaviour in their own use of technology, e.g. use of passwords, logging-off, use of content, research skills, obeying copyright
- Ensures that pupils understand the concept of plagiarism clearly; how to check copyright and also know that they must respect and acknowledge copyright/intellectual property rights
- Ensures pupils only use school-approved systems and publish within appropriately secure/ age-appropriate environments
- Identifies where pupils need extra support or intervention with keeping safe online through interviews, assessment of work and self-evaluations, to capture progress

Parents and Carers

Many parents and carers may have a limited understanding of online safety risks and issues, yet they play an essential role in the education of their children and in the monitoring of their child's online behaviour. Parents/carers may underestimate how often children and young people come across potentially harmful and inappropriate material on the Internet and may be unsure about how to respond. Parents and carers will be informed about the school's filtering and monitoring systems, and made 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 their child is going to be interacting with online where necessary.

The school will therefore seek to provide information and awareness to parents and carers through:

- Letters, newsletters, website
- Parent/Carer workshops
- High profile events e.g. Online Safety Week

Staff

All staff should carefully supervise and guide pupils when engaged in learning activities involving online technology (including extra-curricular, extended school activities and remote teaching). It is essential that **all** staff receive regular online safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- A programme of online safety training will be made available to staff. This will be regularly updated and reinforced.
- All staff read and sign the Acceptable Use Policy

- All new staff receive online safety training as part of their induction programme, ensuring that they fully understand the school Online Safety Policy and Acceptable Internet Use Agreement and sign to say that they have read the latter
- The Online Safety Leader will receive regular updates through attendance at external training events and by reviewing guidance documents released by relevant organisations
- This Online Safety Policy and its updates will be shared with staff

Governors
Governors are asked to develop their online safety awareness sessions through attendance at training provided by NPW or other relevant organisation. They are also invited to participate in school training sessions.

At Godwin Junior School, we recognise that online safety and broader digital resilience must be explicit 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), which is particularly demonstrated by our recent adoption of the Natterhub online safety curricular delivery system.

Annual reviews of curriculum plans 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.

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 and PSHE).

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 reporting concerns to contribute to the overall picture or highlight what might not yet be a problem.

School procedures for dealing with online safety will be mostly detailed in the following policies (primarily in the first key document):

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

Godwin Junior 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 must be reported to the 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 Teacher, unless the concern is about the Head Teacher 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.

We will inform parents/carers of online-safety incidents involving their children, and the police where staff or pupils engage in or are subject to behaviour which we consider is particularly concerning or breaks the law (particular procedures are in place for sexting and upskirting; see section below).

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.

Where pupils contravene these rules, our Positive Behaviour Policy will be applied; where staff contravene these rules, action will be taken as outlined in the staff Code of Conduct.

We reinforce these as usual at the beginning of any school year and will also remind pupils that the same applies for any home learning that may take place in future periods of absence/closure etc.

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

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 Godwin Junior School community. These are also governed by our school's Acceptable Use Policy.

Breaches will be dealt with in line with our Positive Behaviour Policy (for pupils) or Code of Conduct (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, Godwin Junior School 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/carers are bound by the school's Data Protection Policy. It is important to remember that there is a close relationship between both data protection and cybersecurity and a school's ability to effectively safeguard children. Schools are reminded of this in KCSIE.

We are conscious that data protection does not prevent, or limit, the sharing of information for the purposes of keeping children safe. As outlined in Data Protection in Schools, 2023, "It's not usually necessary to ask for consent to share personal information for the purposes of safeguarding a child." And in KCSIE 2024, "The Data Protection Act 2018 and UK GDPR do not prevent the sharing of information for the purposes of keeping children safe. Fears about sharing information must not be allowed to stand in the way of the need to safeguard and promote the welfare and protect the safety of children."

Appropriate filtering and monitoring

Keeping Children Safe in Education has long asked schools to ensure "appropriate" webfiltering 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 DSL now has lead 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

The challenge for DSLs and SLT is to better understand, review and drive the rationale behind decisions in this area.

ALL STAFF need to be aware of the changes and renewed emphasis, as well as play their part in feeding back about areas of concern, potential for pupils to bypass systems and any potential overblocking. They can submit concerns at any point via email to the DSL and will be asked for feedback at the time of the regular checks which 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 Acceptable Usage Policies and regular training reminders in the light of the annual review and regular checks that will be carried out.

At Godwin Junior School:

- web filtering is provided by London Grid for Learning on our school site
- changes can be made by request to Head Teacher or DSL, who will inform the Education Space / NPW
- overall responsibility is held by the DSL, with further support from SLT
- technical support and advice, setup and configuration are from The Education Space
- regular checks are made half termly by the DSL to ensure filtering is still active and functioning everywhere
- an annual review is carried out as part of an online safety audit, in line with LGfL guidance found 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

At Godwin Junior School, we currently use physical monitoring by staff watching screens of users, but will be reviewing network monitoring solutions in dialogue with our service partners.

Messaging/commenting systems (including email and learning platforms)

Authorised systems

- Pupils at this school communicate with each other and with staff using Google Classroom and Natterhub. These platforms do not permit private messaging or commenting, and any comments left are freely visible by other pupils and staff, but not by the wider public. We do not encourage commenting or messaging on any other platforms, although we do use other services like Scratch which technically supply this facility.
- Staff at this school use the email system provided by LGfL through Outlook for all school emails. They never use a personal/private email account (or other messaging platform) to communicate with children or parents/carers, 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 internal and external individuals and teams relevant to their role.
- Staff at this school use Zoom, Google Meet and Microsoft Teams to carry out video-conferencing with groups of parents/carers and external individuals and teams, and may do so concerning school/child data when liaising with other professionals and professional bodies.

This is for the mutual protection and privacy of all staff, pupils and parents/carers, 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, including sign-off by the Head Teacher.

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 Teacher (if by a staff member).

Where devices have multiple accounts for the same app, mistakes can happen, such as an email being sent from or data being uploaded to the wrong account. If a private account is used for communication or to store data by mistake, the DSL/Head Teacher/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, Positive Behaviour Policy and staff Code of Conduct.
- Appropriate behaviour is expected at all times, and the system should not be used to send inappropriate materials or language which is or could be construed as bullying, aggressive, rude, insulting, illegal or otherwise inappropriate, or which (for staff) might bring the school into disrepute or compromise the professionalism of staff.
- Data protection principles will be followed at all times when it comes to all school communications, in line with the school Data Protection Policy and only using the authorised systems mentioned above.
- Staff are allowed to use the email system for reasonable (not excessive, not during lessons) personal use but should be aware that all use is monitored, their emails may be read and the same rules of appropriate behaviour apply at all times. Emails using inappropriate language, images, malware or to adult sites may be blocked and not arrive at their intended destination (and will be dealt with according to the appropriate policy and procedure).

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, we recognise that it is important to consider data protection and cybersecurity before adopting such a platform or service and at all times when using it. Godwin Junior School has a clear 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 our school community (both existing and prospective stakeholders) with a key reputational value.

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.

Digital images and video

When a pupil/student joins the school, parents/carers are asked if they give consent for their child's image to be captured in photographs or videos, for what purpose (beyond internal assessment, which does not require express consent) and for how long.

Whenever a photo or video is being considered to be used for a purpose outside of the school building, the member of staff responsible 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 Godwin Junior School, no member of staff will ever use their personal 'phone to capture photos or videos of pupils. Devices are provided on-site to support staff with capturing photos and videos that serve a purpose towards their learning and development.

Photos are stored in the local networked server or in the school's Google Drive cloud platform in line with the retention schedule of the school Data Protection Policy.

Staff 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 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/carers or younger children.

Pupils are advised to be very careful about placing any personal photos on social media as they grow. 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 express 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

Godwin Junior School works on the principle that if we don't manage our social media reputation, someone else will.

Online Reputation Management (ORM) is about understanding and managing our digital footprint (everything that can be seen or read about the school online). Few parents/carers 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.

Our Head Teacher is responsible for managing our X-Twitter and other social media accounts and checking our Google reviews and other mentions online.

Staff, pupils' and parents'/carers' social media 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/carers and staff will use it. While we strongly discourage pupil use, due to age ratings, we understand that in certain cases pupils might be given permission by their parents/carers to access social media. 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/carer chats, pages or groups.

If parents/carers 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's Complaints Procedure should be followed. Sharing complaints on social media is unlikely to help resolve the matter, but can cause upset to staff, pupils and parents/carers, also undermining staff morale and the reputation of the school (which is important for the pupils we serve).

Many social media platforms have a minimum age of 13 (note that WhatsApp is 16+), but the school occasionally deals with issues arising on social media involving pupils/students under this

age. We ask parents/carers to respect age ratings on social media platforms wherever possible and not encourage or condone under-age use.

However, the school has to strike a difficult balance of not encouraging under-age use at the same time as needing to acknowledge reality in order to best help our pupils 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/carers 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). The Digital Family Agreement may help to help establish shared expectations and the Top Tips for Parents poster, along with relevant items and support available from parentsafe.lgfl.net are useful resources, as is the Children's Commission Digital 5 A Day.

Although the school has an official X-Twitter account, this is used solely to post information and we ask parents/carers not to use these channels, especially not to communicate about their children.

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

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

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

* Exceptions may be made, e.g. for pre-existing family links, but these must be approved by the Head Teacher 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 Teacher (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 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 that 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.

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** must not bring personal devices to school. The Head Teacher may decide that exceptional circumstances (such as a child travelling a significant distance on public transport unaccompanied) merit an exception to this rule. In such a case, the pupil must leave any personal devices at the office at school reception and pick them up at the end of the school day before leaving. Any attempt to use a 'phone on school property without permission or to take illicit photographs or videos will lead to sanctions in line with our Positive Behaviour Policy.
- **All staff who work directly with children** should leave their mobile phones in their personal staff locker/in the school office and only use them in private staff areas, like the staff room. See also the 'Digital images and video' section of this document and the school Data Protection Policy. 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. In exceptional circumstances a member of staff may be granted permission by the Head Teacher or Deputy Head Teacher to keep their 'phone on their person for a short period of time during the school day, switched to silent.
- **Volunteers, contractors, governors** should leave their phones at the office. Under no circumstances should they be used in the presence of children or to take photographs or videos. If this is required (e.g. for contractors to take photos of equipment or buildings), permission of the Head Teacher or Deputy Head Teacher should be sought and this should be done in the presence of a member of staff.
- **Parents and carers** are asked to leave their device at the school office if they are attending a meeting/in the main part of the school building. They should ask permission before taking any photos, e.g. of displays in corridors or classrooms, and avoid capturing other children. When at school events, please refer to the Digital images and video section of this document.

Use of school devices

Staff and pupils are expected to follow the terms of the school Acceptable Use Policies for appropriate use and behaviour when on school devices, whether on site or at home.

School devices are not to be used in any way which contravenes AUPs, Positive Behaviour Policy / staff Code of Conduct.

WiFi is accessible to pupils via the Chromebook and iPad devices, with school-related internet use following the framework of the Acceptable Use Policy. All such use is filtered, and monitoring is carried out physically.

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 educational visits, teachers share their personal 'phone numbers with one another and the school – these are recorded on the Risk Assessment document. School staff will not usually have any direct contact with parents and carers – this will be done via the school. In exceptional circumstances, such as if a child falls unwell during a residential visit, a staff member may need to contact a parent/carer directly after confirming this course of action with the Head Teacher. Staff using their personal phone in this type of situation will ensure that the number is hidden to avoid a parent/carer accessing a staff member's private 'phone number.

Searching and confiscation

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

Appendix A – Roles

Please read the relevant roles and 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
- Head Teacher
- Designated Safeguarding Lead
- Governing Board, led by Safeguarding Link Governor
- PSHE / RSHE Lead
- Computing Lead
- Subject Leaders
- Network Manager/technician
- Data Protection Officer (DPO)
- Volunteers and contractors
- Pupils
- Parents/carers
- External groups, including The Friends of Godwin – our PTA

All staff

All staff should sign and follow the staff acceptable use policy in conjunction with this Policy, the school's Child Protection and Safeguarding Policy, the Code of Conduct and relevant parts of Keeping Children Safe in Education to support a whole-school safeguarding approach.

This includes reporting any concerns, no matter how small, to the Designated Safeguarding Lead as named in the AUP, maintaining an awareness of current online safety issues 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.

Head Teacher

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

Designated Safeguarding Lead / Online Safety Lead

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
- Working closely with technical colleagues and SLT to learn more about filtering and monitoring, 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 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.
- 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 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
- 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 Head Teacher, 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/carers, including harder-to-reach parents/carers – dedicated resources at parentsafe.lgfl.net
- Communicate regularly with SLT and the safeguarding governor 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).

Governing Board, led by Safeguarding Link Governor

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 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
- Ensure that all staff also receive appropriate safeguarding and child protection (including online) training at induction and that this is updated
- Support the school in encouraging parents/carers 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 Head Teacher to ensure a compliant framework for storing data, but helping to ensure that child protection is always put first and data-protection processes support careful and legal sharing of information
- Check all school staff have read Part 1 of KCSIE; SLT and all working directly with children have read Annex B
- Ensure that all staff undergo safeguarding and child protection training (including online safety and now also reminders about filtering and monitoring
- "Ensure that children are taught about safeguarding, including online safety […] as part of providing a broad and balanced curriculum […] Consider a whole school or college approach to online safety [with] a clear policy on the use of mobile technology."

PSHE / RSHE Lead

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."
- 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

Key responsibilities:

- As listed in the 'all staff' section, plus:
- Oversee the delivery of the online safety element of the Computing curriculum in accordance with the national curriculum
- Work closely with the RSHE lead to avoid overlap but ensure a complementary whole-school approach
- Work closely with the DSL/OSL and all other staff to ensure an understanding of the issues, approaches and messaging within Computing
- Collaborate with technical staff and others responsible for ICT use in school to ensure a common and consistent approach, in line with acceptable-use agreements

Subject Leaders

Key responsibilities:

- As listed in the 'all staff' section, plus:
- Look for opportunities to embed online safety in your subject or aspect, especially as part of the RSHE curriculum, and model positive attitudes and approaches to staff and pupils alike
- Consider how the UKCIS framework Education for a Connected World and Teaching Online Safety in Schools can be applied in your context
- Work closely with the DSL/OSL and all other staff to ensure an understanding of the issues, approaches and messaging within Computing

Network Manager/other technical support roles – The Education Space/NPW

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 from 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 is up to date, easy to follow and practicable
- Monitor the use of school technology, online platforms and social media presence and that any misuse/attempted misuse is identified and reported in line with school policy

Data Protection Officer (DPO) – Rafaela Kettle

Key responsibilities:

- Alongside those of other staff, provide data protection expertise and training and support the DP and Online Safety 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 2024, "The Data Protection Act 2018 and UK GDPR do not prevent the sharing of information for the purposes of keeping children safe. Fears about sharing information must not be allowed to stand in the way of the need to safeguard and promote the welfare and protect the safety of children."
- 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)'.
- Ensure that all access to safeguarding data is limited as appropriate, and also monitored and audited

Volunteers and contractors

Key responsibilities:

- 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

Pupils

Key responsibilities:

- Read, understand, sign and adhere to the student/pupil Acceptable Use Policy

Parents/carers

Key responsibilities:

- Model safe and responsible behaviours in their own use of technology

External groups including parent associations – Friends of Godwin

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