CONSILIUM ACADEMIES

Online Safety

Policy

2025

EXCELLENCE AND EQUITY WITH INTEGRITY

Date of Approval:	October 2025
Approved by:	Trust Board
Date of next Review:	October 2026

Consilium Academies

Contents

Introduction

What is this policy?

Online safety is an integral part of safeguarding and requires a whole school, cross-curricular approach and collaboration between key school leads. Accordingly, this policy is written in line with 'Keeping Children Safe in Education' 2025 (KCSIE), 'Teaching Online Safety in Schools' 2019, statutory RSHE guidance 2025 and other statutory documents. It is cross-curricular (with relevance beyond Relationships, Health and Sex Education, Citizenship and Computing) and sits alongside the Trust statutory Child Protection and Safeguarding Policy. Any issues and concerns with online safety must always follow the school's safeguarding and child protection procedures.

Who is it for; when is it reviewed?

This policy is a living document, subject to full annual review but also amended where necessary during the year in response to developments in the school and local area. Any changes to this policy will be immediately disseminated to all stakeholders.

Who is in charge of online safety?

KCSIE 2025 makes clear that "the designated safeguarding lead should take **lead** responsibility for safeguarding and child protection (including online safety and understanding the filtering and monitoring systems and processes in place)." The DSL can delegate activities but not the responsibility for this area and whilst subject leads, e.g. for RSHE will plan the curriculum for their area, it is important that this ties into a whole-school approach.

What are the main online safety risks in 2025/2026?

In 2025-26, online safety risks will continue to evolve, with a growing focus on the impact of harmful algorithms, the misuse of AI, and the persistent dangers of cyberbullying, sextortion, and online grooming. The Online Safety Act 2025 will play a key role in addressing these issues by placing new obligations on platforms to tackle illegal and harmful content, particularly for children.

Social media and other platforms use algorithms to recommend content, but these algorithms can inadvertently expose users, especially children, to harmful content related to self-harm, suicide, eating disorders, and other dangerous activities. The Online Safety Act 2025 requires platforms to assess the impact of their algorithms on users and take steps to reduce the risk of harmful content being recommended, particularly to children. It also specifically targets content related to serious offenses like child sexual abuse, terrorism, and fraud, as well as content that promotes self-harm, suicide, and eating disorders.

AI-powered tools can be used to create deepfakes, which are realistic but fabricated videos and images, that can be used for blackmail, extortion, and spreading false information. Criminals are using AI-powered chatbots to lure children into dangerous situations and to identify vulnerabilities in online security measures to steal personal data. AI can be used to create fake social media accounts that are used to target and groom vulnerable children.

Cyberbullying continues to be a major concern, with new forms of harassment emerging as technology advances. This can include doxxing (revealing personal information), targeted harassment, and the spread of false information intended to cause harm. The Online Safety Act 2025 criminalises threatening communications, cyberflashing (sending unsolicited explicit images), and intimate image abuse. The act also addresses epilepsy trolling, which involves sending flashing images designed to trigger seizures.

Criminals use blackmail and coercion tactics to manipulate victims into sharing explicit content. Fraudulent schemes involving investments and cryptocurrencies are also a growing concern. The rapid development of new apps and online platforms can create new privacy risks for children, making it important to educate them about privacy settings and app permissions. Criminals continue to use online platforms to groom and exploit children.

In our schools over the past year, we have particularly noticed the impact in terms of device use and abuse and types of online/device-based incidents which affect the wellbeing and safeguarding of our pupils and subsequently, their mental health.

Nationally, some of the latest trends of the past twelve months are outlined below. These are reflected in this policy and the acceptable use agreements we use and seen in the context of the 4 Cs (see KCSIE for more details), a whole-school contextual safeguarding approach that incorporates policy and practice for curriculum, safeguarding and technical teams.

Self-generative artificial intelligence has become rapidly more accessible, with many pupils often having unfettered access to tools that generate text and images at home or in school. These tools not only represent a challenge in terms of accuracy when young people are genuinely looking for information (gen AI can be responsible for incorrect and sometime harmful information), but also in terms of plagiarism for teachers and above all safety - none of the mainstream tools have end-user safety settings, most have an age limit of 13 or even 18 and in spite of basic rude words not delivering results, will easily produce inappropriate material. Schools not only need to tackle this in terms of what comes into school but also educating young people and their parents on use of these tools in the home. Self-generative AI has also made it easier than ever to create sexualised images and deepfake videos. Whilst they may not be real, they have a devastating effect on a young person's emotional wellbeing and physical safety, and can also be used to blackmail, humiliate and abuse. The Internet Watch Foundation has reported AI-generated imagery of child sexual abuse progressing at such a worrying rate. Ofcom's 'Children and parents: media use and attitudes report 2024' has shown that YouTube remains the most used site or app among all under 18s and the reach of WhatsApp, TikTok and Snapchat increased yet further (especially with the minimum age for use of WhatsApp now 13). With children aged 3 - 17 spending an average 3 hours 5 minutes per day online, four in ten parents report finding it hard to control their child's screentime. Notably, 45% of 8-11s feel that their parents' screentime is too high, underlining the importance of modelling good behaviour.

Given the 13+ minimum age requirement on most social media platforms, it is notable that half (51%) of children under 13 use them. Despite age restrictions, four in ten admit to giving a fake age online, exposing them to content inappropriate for their age and increasing their risk of harm, with over a third (36%) of parents of all 3-17s saying they would allow their child to have a profile on sites or apps before they had reached the minimum age.

As a school we recognise that many of our children and young people are on these apps regardless of age limits, which are often misunderstood or ignored. We therefore will remind about best practice while remembering the reality for most of our pupils is quite different.

This is striking when you consider that over 95 percent of pupils have their own mobile phone by the end of Year 7, and the vast majority do not have safety controls or limitations to prevent harm of access to inappropriate material. This is particularly pertinent given that 141, cases of self-generated child sexual abuse material were found of 11–13-year-olds (Internet Watch Foundation Annual Report). These were predominantly (but importantly not only) girls; it is important also to recognise the increasing risk of sextortion, where older teenage boys have been financially exploited after being tricked into sharing intimate pictures online. This resulted in the National Crime Agency releasing an alert to all schools in Spring 2024.

Growing numbers of children and young people are using social media and apps such as Snapchat as their source of news and information, with little attention paid to the facts or veracity of influencers sharing news. The alarming speed and scale at which misinformation about the attack in Southport (August 2024) was shared, resulting in Islamophobic and racist violence, rioting and looting across England is particularly concerning, with much of it was fuelled by false online accusations about the assailant. Despite attempts by Police and national news to correct the misleading information, it racked up millions of views on social media sites like X and was actively promoted by several high-profile users with large followings.

There have also been significant safeguarding concerns where parents have filmed interactions with staff outside the school gates and posted this on social media, putting children and the wider school community at risk of harm. See nofilming.lgfl.net to find out more.

Cyber Security is an essential component in safeguarding children and now features within KCSIE. Sadly, the education sector remains a clear target for cyber-attacks, with the Cyber Security Breaches Survey 2024 highlighting an increase in school attacks nationally, with 71% of secondary schools reporting a breach or attack in the past year, and 52% of primary schools.

How will this policy be communicated?

It will be communicated in the following ways:

- Posted on the school website.
- Part of school induction pack for all new staff (including temporary, supply and non-classroom-based staff and those starting mid-year).
- Integral to safeguarding updates and training for all staff (especially in September refreshers).
- Clearly reflected in the Acceptable Use Policies (AUPs) for staff, volunteers, contractors, Local Academy Board members, Trust Board members, students and parents/carers.

Overview

Aims

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

- Setting out expectations for all school community members' online behaviour, attitudes and activities and use of digital technology (including when devices are offline).
- Helping safeguarding and senior leadership teams to have a better understanding and awareness of filtering and monitoring through effective collaboration and communication with technical colleagues.
- 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 todays 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 the Behaviour Policy).

Further Help and Support

Internal school channels should always be followed first for reporting and support, as documented in school policy documents, especially in response to incidents. The DSL will handle referrals to the local authority and with the Principal/Head of School will handle referrals to the Local Authority Designated Officer (LADO).

Beyond this, **reporting.lgfl.net** has a list of curated links to external support and helplines for both students and staff, including the Professionals' Online-Safety Helpline from the UK Safer Internet Centre and the NSPCC Report Abuse Helpline for sexual harassment or abuse, as well as hotlines for hate crime, terrorism and fraud which might be useful to share with parents, and anonymous support for children and young people.

Scope

This policy applies to all members of our community (including teaching and support staff, supply teachers and tutors engaged under the DfE National Tutoring Programme, LAB, volunteers, contractors, students, parents/carers, visitors and community users) who have access to our digital technology, networks and systems, whether on-site or remotely, and at any time, or who use technology in their school role.

Roles and responsibilities

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

Education and curriculum

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

As well as teaching about the underpinning knowledge and behaviours that can help students navigate the online world safely and confidently regardless of the device, platform or app, Teaching Online Safety in Schools recommends embedding teaching about online safety and harms through a whole school approach and provides an understanding of these risks to help tailor teaching and support to the specific needs of students, including vulnerable students – dedicated training around this with curriculum mapping for RSHE/PSHE and online safety leads is available at safetraining.lgfl.net

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

The following subjects have the clearest online safety links:

- Relationships education, relationships and sex education (RSE) and health (also known as RSHE or PSHE)
- Computing
- Citizenship

It is the role of all staff to identify opportunities to thread online safety through all school activities, both outside the classroom and within the curriculum, supporting curriculum/stage/subject leads, and making the most of unexpected learning opportunities as they arise (which have a unique value for students).

Whenever overseeing the use of technology (devices, the internet, new technology such as augmented reality, etc) in school or setting as homework tasks, all staff should encourage sensible use, monitor what students are doing and consider potential dangers and the age appropriateness of websites. "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 ask to access and be clear who from the school or college (if anyone) their child is going to be interacting with online."(KCSIE 2025).

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

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

Annual reviews of curriculum plans / schemes of work (including for SEND students) 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 online-safety concerns and incidents

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

General concerns must be handled in the same way as any other safeguarding concern; safeguarding is often referred to as a jigsaw puzzle, so all stakeholders should err on the side of talking to the online-safety lead / designated safeguarding lead, to contribute to the overall picture or highlight what might not yet be a problem.

Staff will often have a unique insight and opportunity to find out about issues first in the playground, corridors, toilets and other communal areas outside the classroom (particularly relating to bullying and sexual harassment and violence).

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

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

School commits to take all reasonable precautions to ensure online safety but recognises that incidents will occur both inside school and outside school (and that those from outside school will continue to impact students when they come into school or during extended periods away from school). All members of the school are encouraged to report issues swiftly to allow us to deal with them quickly and sensitively through the school's escalation processes.

Any suspected online risk or infringement should be reported to the online safety lead / designated safeguarding lead on the same day – where clearly urgent, it will be made by the end of the lesson.

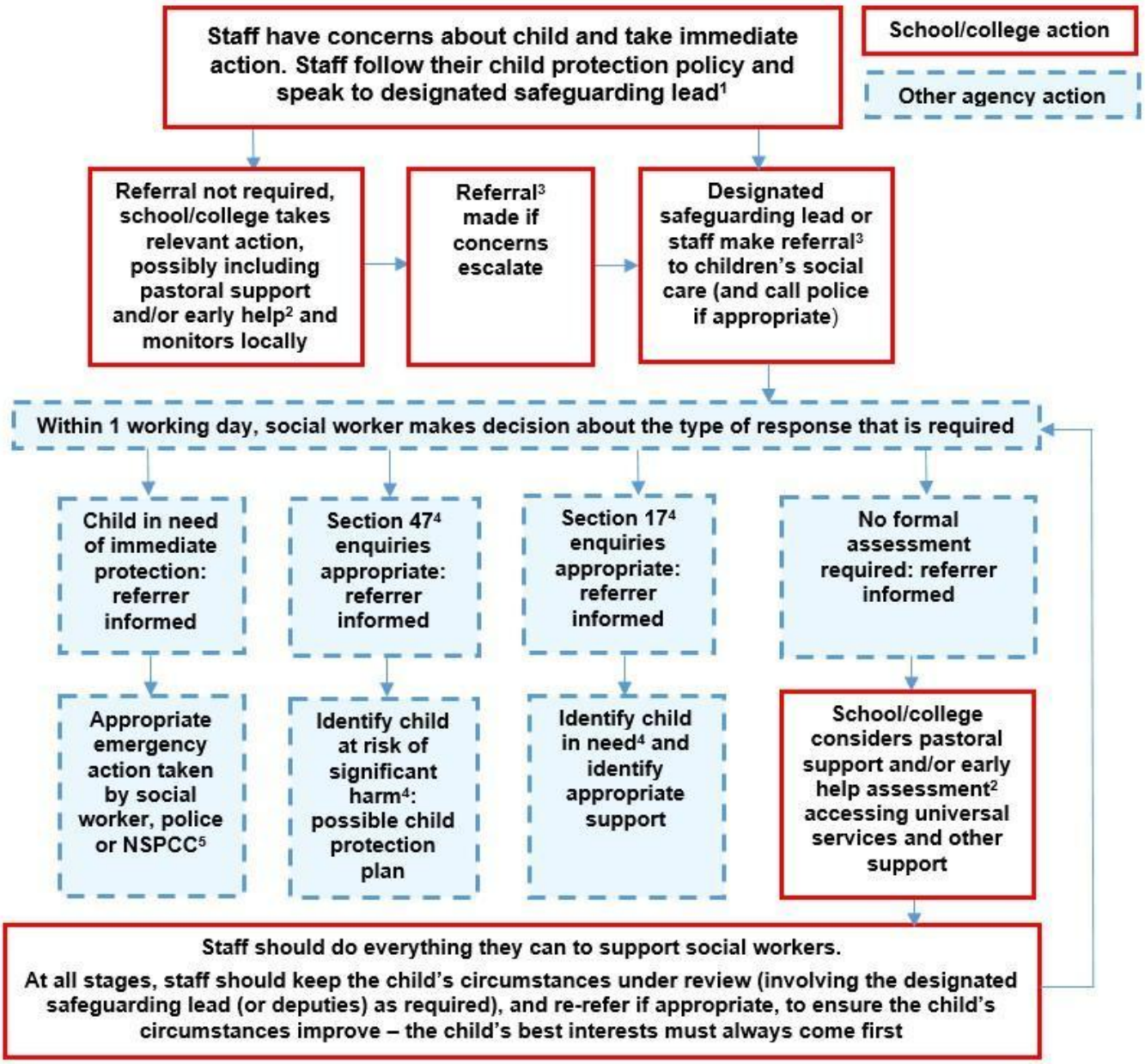
Any concern/allegation about staff misuse is always referred directly to the Principal/Head of School unless the concern is about the Principal/Head of School in which case the complaint is referred to the Hub Director for the region and where appropriate the LADO (Local Authority's Designated Officer). Staff may also use the NSPCC Whistleblowing Helpline.

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

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

Actions where there are concerns about a child

The following flow chart is taken from page 24 of Keeping Children Safe in Education 2025 as the key education safeguarding document. As outlined previously, online safety concerns are no different to any other safeguarding concern.

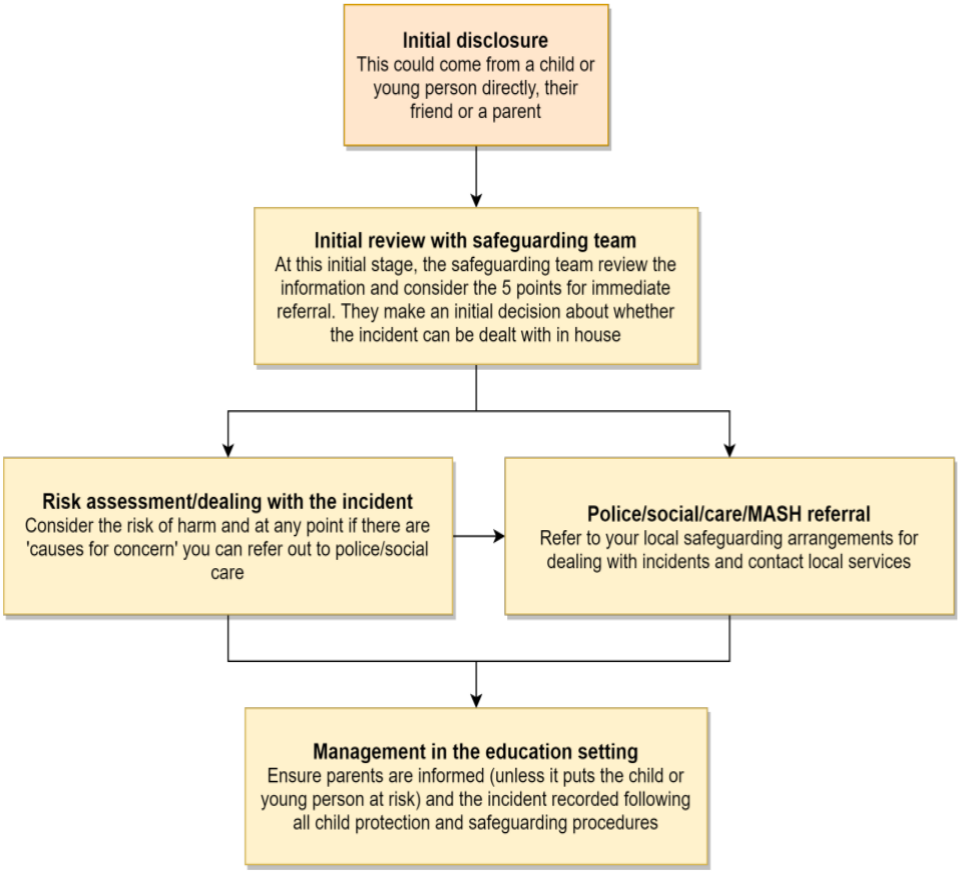


Sexting – sharing nudes and semi-nudes

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

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

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



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

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

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

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

Upskirting

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

Bullying

Online bullying, including incidents that take place outside school or from home should be treated like any other form of bullying and the school bullying policy should be followed for online bullying, which may also be referred to as cyberbullying, including issues arising from banter.

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

Sexual violence and harassment

Part 5 of Keeping Children Safe in Education covers the immediate response to a report, providing reassurance and confidentiality which is highly relevant for all staff; the case studies section provides a helpful overview of some of the issues which may arise.

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

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

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

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

Where students contravene these rules, the school behaviour policy will be applied; where staff contravene these rules, action will be taken as outlined in the staff code of conduct.

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

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

Social media incidents

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

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

CCTV

CCTV is used across the school for the protection and safety of the school community. Please refer to the Trust's CCTV Policy for more information.

Extremism

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

Data protection and data security

GDPR information on the relationship between the school and LGfL can be found at gdpr.lgfl.net; there are useful links and documents to support schools with data protection in the 'Resources for Schools' section of that page.

There are references to the relationship between data protection and safeguarding in key Department for Education documents 'Keeping Children Safe in Education' and 'Data protection: a toolkit for schools' (August 2018), which the DPO and DSL will seek to apply. This quote from the latter document is useful for all staff – note the red and purple highlights:

"**GDPR does not prevent, or limit, the sharing of information for the purposes of keeping children safe.** Lawful and secure information sharing between schools, Children's Social Care, and other local agencies, is essential for keeping children safe and ensuring they get the support they need. **The Data Protection Act 2018 introduced 'safeguarding' as a reason to be able to process sensitive, personal information, even without consent** (DPA, Part 2,18; Schedule 8, 4) When Designated Safeguarding Leads in schools are considering whether, or not, to share safeguarding information (especially with other agencies) **it is considered best practice for them to record who they are sharing that information with and for what reason. If they have taken a decision not to seek consent from the data subject and/or parent/carer that should also be recorded within the safeguarding file. All relevant information can be shared without consent if to gain consent would place a child at risk. Fears about sharing information must not be allowed to stand in the way of promoting the welfare and protecting the safety of children**."

All students, staff, LAB members, volunteers, contractors and parents are bound by the school's data protection policy and agreements, which can be found on our website or shared areas.

Rigorous controls on the network, sign-on for technical services, firewalls and filtering all support data protection. The following data security products are also used to protect the integrity of data, which in turn supports data protection: Sophos Anti-Virus, Sophos Anti-Phish, Sophos InterceptX, Sophos Server Advance, Malware Bytes, Egress, Intune Device Management.

School ensures a GDPR-compliant framework for storing data, but which ensures that child protection is always put first and data-protection processes support careful and legal sharing of information.

Staff are reminded that all safeguarding data is highly sensitive and should be treated with the strictest confidentiality at all times and only shared via approved channels to colleagues or agencies with appropriate permissions. The use of Microsoft Rights Management System to encrypt all non-internal emails is compulsory for sharing student data. If this is not possible, the DPO and DSL should be informed in advance.

Data protection and data security are critical aspects of safeguarding our staff and students.

- **Use of personal vs school devices**

As outlined in the Acceptable Use policy, staff are reminded that they must not download work related files to their personal device. Accessing online cloud-based services is however permitted.

- **Password policy / two-factor authentication**

The Trust operates a strict password policy – all staff are forced to choose a suitably complex password when they setup their account and will be regularly prompted to change them. All staff must use multi-factor authentication to access their accounts.

- **Reminders to lock devices when leaving unattended**

All staff must lock their devices when they are away from their desk. The Trust has implemented an automatic timer that will lockout the device after 1 hour of inactivity. In an ideal world this timer would be 15 minutes, however it is

recognised that this would cause issues for lesson delivery. It is therefore critical that staff support the safeguarding and security of our students by carrying out this manual process if they are leaving their device unattended.

- **Device encryption**

All portable devices (e.g., laptops, tablets) are encrypted with BitLocker Drive Encryption. Where possible all desktop devices that have the required security hardware are also encrypted for additional protection. The Trust enforces write protection onto all USB devices via BitLocker Policy. Members of staff are encouraged to use the Trust's cloud-based storage in favour of removable media wherever possible.

- **Access to and access audit logs for school systems**

The Trust records all logon attempts to any of the accounts associated with the organisation. All activity on Trust owned devices or accounts if logged and can be reviewed at any time. Staff and students are reminded that their activity is monitored by the DSL at each site; they must therefore ensure they are complaint with the acceptable usage policy at all times.

- **Security processes and policies**

The Trust has a detailed Cyber Security Policy which outlines the preventative measures taken to keep our school's safe. This includes a disaster recovery plan in the event of an incident. Investment has been made into backups systems for critical data to keep our schools operational.

- **Access by third parties, e.g. IT support agencies**

Third parties must not be allowed unattended access to any IT system on the Trust's internal network. The Trust's IT team will supervise any remote connection to a device to ensure that the usage is in line with our expectations.

- **Wireless access / BYOD**

Staff, students, and visitors are able to access the 'guest' wireless network with their personal devices. The base level student web filtering policy is applied to this network to keep all members of our community safe. Only Trust owned devices can connect to our internal network in line with the security policy.

- **File sharing**

All file sharing must be undertaken on the Office 365 platform. Internal sharing should be completed using the pre-defined SharePoint or Teams sites wherever possible.

- **Cloud platform use, access and sharing protocols**

The Trust uses Office 365 as its primary cloud-based platform. All sensitive data should be saved into this platform, which includes OneDrive, SharePoint and Teams amongst other services. Sharing of data from Office 365 is restricted to approved companies to prevent data leakage. Staff should not upload data relating to any member of the school community to any personal cloud storage – only the trust's own Microsoft 365 environment can be used.

Appropriate filtering and monitoring

Keeping Children Safe in Education obliges schools to "ensure appropriate filters and appropriate monitoring systems are in place [and] not be able to access harmful or inappropriate material [but at the same time] be careful that "over blocking" does not lead to unreasonable restrictions as to what children can be taught with regards to online teaching and safeguarding." The filtering and monitoring systems will be informed in part, by the risk assessment required by

the Prevent Duty. School's can use the DfE's 'plan technology for your school service' to self-assess against the filtering and monitoring standards and receive personalised recommendations on how to meet them.

Across the Trust, the web filtering and firewall provision is provided by Wave 9. This means we have a dedicated and secure connection that is protected with firewalls and multiple layers of security, including a web filtering system called Sophos XG, which is made specifically to protect children in schools. You can read more about why this system is appropriate on the UK Safer Internet Centre's appropriate filtering submission pages here.

There are three types of appropriate monitoring identified by the Safer Internet Centre. These are:

1. Physical monitoring (adult supervision in the classroom, at all times)
2. Internet and web access
3. Active/Pro-active technology monitoring services

Across Consilium Academies, we utilise a combination of all three approaches to keep our children safe. In the classroom, teachers utilise Netsupport monitoring technology to ensure they have visibility of the activities as they occur. This software also reports any concerns to the DSL on site via e-mail notifications. Our firewall and web filtering solution also blocks a number of inappropriate categories.

At home, school devices are monitored by the NetSupport client which provides the same functionality as if the device were in school. We also provide a basic level of filtering onto each device from our Sophos client.

When users log into any school system on a personal device, activity may also be monitored.

The designated safeguarding lead (DSL) has lead responsibility for filtering and monitoring and works closely with the Director of IT Services and school level IT staff to implement the DfE filtering and monitoring standards, which require schools to:

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

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

Technical and safeguarding colleagues work together closely to carry out annual reviews and check and also to ensure that the school responds to issues and integrates with the curriculum.

We carry out half-termly checks to ensure all systems are in operation, functioning as expected, etc and an annual review as part of an online safety audit of strategy, approach etc.

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

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

Electronic communications

This section only covers electronic communications, but the same principles of transparency, appropriate conduct and audit trail apply.

Office 365

- Staff and students across Consilium use Office e-mail communication.

These systems are linked to our Arbor systems and are fully auditable, trackable and managed by the Consilium Technical Services Team. This is for the mutual protection and privacy of all staff, students and parents, as well as to support data protection.

General principles for email use are as follows:

- Email/Teams chat is the only means of electronic communication to be used between staff and students / staff and parents (in both directions). Some schools may utilise Parent messaging / text messaging apps to such as Classcharts/Arbor to communicate with parents. Use of a different platform must be approved in advance by the data-protection officer and Head of Technical Services. 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 Principal/Head of School (if by a staff member).
- Email may only be sent using the email systems above. There should be no circumstances where a private email is used; if this happens by mistake, the DSL/Headteacher/DPO (the particular circumstances of the incident will determine whose remit this is) should be informed immediately.
- Staff or student personal data should never be sent/shared/stored on email.
    - If data needs to be shared with external agencies, Microsoft Rights Management or OneDrive sharing are available and must be used.
    - Internally, staff should use the school network, including when working from home.
- Students in our schools are restricted to emailing within the school and cannot email external accounts Some exceptions have been made for careers/college related activities.
- 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
- Students and staff are NOT allowed to use the email system for personal use and 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.

See also the social media section of this policy.

Use of generative AI

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

- We will talk about the use of these tools with students, staff and parents – their practical use as well as their ethical pros and cons.
- We are aware that there will be use of these apps and exposure to AI creations on devices at home for some students – these experiences may be both positive/creative and also negative (inappropriate data use, misinformation, bullying, deepfakes, undressing apps).
- The use of any generative AI in Exams, or to plagiarise and cheat is prohibited, and the Behaviour Policy will be used for any student found doing so.

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. Each school has nominated members of staff to ensure the content is up to date. This is supervised by the Marketing Team. The site is managed by / hosted by E4Education (Juniper).

The DfE has determined information which must be available on a school website. LGfL has compiled RAG (red-amber-green) audits at safepolicies.lgfl.net to help schools to ensure that are requirements are met (see appendices).

Where other staff submit information for the website, they are asked to remember:

- 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. If in doubt, check with Claudia Ireland, Head of Marketing. There are many open-access libraries of high-quality public-domain images that can be used (e.g. pixabay.com for marketing materials – beware some adult content on this site). Students and staff at LGfL schools also have access to licences for music, sound effects, art collection images and other at curriculum.lgfl.net
- Where student's work, images or videos are published on the website, their identities are protected, and full names are not published (remember also not to save images with a filename that includes a student's full name).

Cloud platforms

It is important to consider data protection before adopting a cloud platform or service – see our Data Protection policy here. Where possible Office 365 should be used as the cloud platform or identity service.

For online safety, basic rules of good password hygiene ("Treat your password like your toothbrush –never share it with anyone!"), expert administration and training can help to keep staff and students safe, and to avoid incidents. The data protection officer and Head of Technical Services analyse and document systems and procedures before they are implemented and regularly review them.

The following principles apply:

- Privacy statements inform parents and children (13+) when and what sort of data is stored in the cloud.
- The DPO approves new cloud systems, what may or may not be stored in them and by whom. This is noted in a DPIA (data-protection impact statement) and parental permission is sought.
- Regular training ensures all staff understand sharing functionality and this is audited to ensure that student data is not shared by mistake. Open access or widely shared folders are clearly marked as such.
- Students and staff are only given access and/or sharing rights when they can demonstrate an understanding of what data may be stored and how it can be seen.
- Two-factor authentication is used for access to staff or student data.
- Student images/videos are only made public with parental permission.
- Only school-approved platforms are used by students or staff to store student's work.
- All stakeholders understand the difference between consumer and education products (e.g. a private Gmail account or Google Drive and those belonging to a managed educational domain)

Digital images and video

When a 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 taken/made, the member of staff taking it will check the latest database before using it for any purpose.

Any students 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 students, and where these are stored. In our Trust, no member of staff will ever use their personal phone to capture photos or videos of students.

Photos are stored on the school network or Office 365 are stored in line with the retention schedule of the school Data Protection Policy.

Staff and parents are reminded annually about the importance of not sharing photos without permission, due to reasons of child protection (e.g., cared for children often have restrictions for their own protection), data protection, religious or cultural reasons, or simply for reasons of personal privacy. Further detail on this subject and a sample letter to parents for taking photos or videos at school events can be found at parentfilming.lgfl.net

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

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

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

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

Social media

Our social media presence

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

Online Reputation Management (ORM) is about understanding and managing our digital footprint (everything that can be seen or read about the school online). Few parents will apply for a school place without first 'googling' the school, and the Ofsted pre-inspection check includes monitoring what is being said online (Mumsnet is a favourite).

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.

Claudia Ireland, Head of Marketing and Communications, is responsible for managing our Twitter/Facebook/and other social media accounts and checking our Wikipedia and Google reviews. S/he follows the guidance in the LGfL / Safer Internet Centre online-reputation management document here.

Staff, students' and parents' SM presence

Social media (including here 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 students will use it. However, as stated in the acceptable use policies which all members of the school community sign, we expect everybody to behave in a positive manner, engaging respectfully with the school and each other on social media, in the same way as they would face to face.

This positive behaviour can be summarised as not making any posts which are or could be construed as bullying, aggressive, rude, insulting, illegal or otherwise inappropriate, or which might bring the school or (particularly for staff)

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

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

Many social media platforms have a minimum age of 13 (note that WhatsApp is 16+), but the school regularly deals with issues arising on social media with students under the age of 13. We ask parents to respect age ratings on social media platforms wherever possible and not encourage or condone underage use. It is worth noting that Online Harms regulation is likely to require more stringent age verification measures over the coming years.

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

Parents can best support this by talking to their children about the apps, sites and games they use (you don't need to know them – ask your child to explain it to you), with whom, for how long, and when (late at night / in bedrooms is not helpful for a good night's sleep and productive teaching and learning at school the next day).

The Trust and its schools may utilise an official Facebook / Twitter / Instagram account (managed by Claudia Ireland, Head of Marketing and Communications) and will respond to general enquiries about the school but asks parents/carers not to use these channels to communicate about their children.

Email is the official electronic communication channel between parents and the school, and between staff and students.

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

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

* Exceptions may be made, e.g. for pre-existing family links, but these must be approved by the Principal/Head of School and should be declared upon entry of the student 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 Principal/Head of School (if by a staff member).

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

The serious consequences of inappropriate behaviour on social media are underlined by the fact that during the last 6 years, there have been over 300 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.

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

Devices used at home should be used just like if they were in full view of a teacher or colleague.

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

- **Students** during the school day, phones must remain turned off at all times, unless the teacher has given express permission as part of the lesson. Any attempt to use a phone in lessons without permission or to take illicit photographs or videos will lead to sanctions from the school behaviour policy. Important messages and phone calls to or from parents can be made at the school office, which will also pass on messages from parents to pupils in emergencies.
- **All staff who work directly with children** should leave their mobile phones on silent and only use them in private staff areas during school hours. Child/staff data should never be downloaded onto a private phone. If a staff member is expecting an important personal call when teaching or otherwise on duty, they may leave their phone with the school office to answer on their behalf or ask for the message to be left with the school office.
- **Volunteers, contractors, governors** should leave their phones in their pockets and turned off. Under no circumstances should they be used in the presence of children or to take photographs or videos. If this is required (e.g. for contractors to take photos of equipment or buildings), permission of should be sought from a member of school staff and all photos must be taken 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. When at school events, please refer to the Digital images and video section of this document on page. Parents are asked not to call students on their mobile phones during the school day; urgent messages can be passed via the school office.

Network / internet access on school devices

- **Staff and students** are not allowed internal network access via personal devices. However, they are allowed to access the school guest wireless internet network for school-related internet use / limited personal use within the framework of the acceptable use policy. All such use is monitored.
- **Home devices** are issued to some students. These are restricted to the apps/software installed by the school and may be used for learning - all usage may be tracked. The devices are protected and monitored by Impero and Sophos systems. Students who breach the acceptable usage policy may have their device revoked.
- **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. Child/staff data should never be downloaded onto a private phone.
- **Volunteers, contractors, governors** have no access to the school network but can access the guest wireless network which has no access to networked files/drives or systems and is subject to the acceptable use policy. All internet traffic is monitored.
- **Parents** can access the guest wireless network but have no access to networked files/drives, subject to the acceptable use policy. All internet traffic is monitored.

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 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 Principal/Head of School. Teachers using their personal phone in an emergency will ensure that the number is hidden to avoid a parent or student accessing a teacher's private phone number.

Searching and confiscation

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

Appendix 1 – Roles

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

School staff – note that you may need to read two sections – if your role is reflected here, you should still read the "All Staff" section.

Roles:

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

All staff

Key responsibilities:

- Read and follow this policy in conjunction with the child protection and safeguarding policy and the relevant parts of Keeping Children Safe in Education 2025. Understand the expectations, applicable roles and responsibilities in relation to filtering and monitoring.
- Understand that online safety is a core part of safeguarding and part of everyone's job – never think that someone else will pick it up. Safeguarding is often referred to as a jigsaw puzzle – you may have the missing piece, so do not keep anything to yourself. Record online-safety incidents in the same way as any safeguarding incident; report in accordance with school procedures.
- Know who the Designated Safeguarding Lead (DSL) and Online Safety Lead (OSL) are; notify them not just of concerns but also of trends and general issues you may identify. Also speak to them if policy does not reflect practice and follow escalation procedures if concerns are not promptly acted upon.
- Sign and follow the staff acceptable use policy and code of conduct.
- Identify opportunities to thread online safety through all school activities as part of a whole school approach in line with the RSHE curriculum, both outside the classroom and within the curriculum, supporting curriculum/stage/subject leads, and making the most of unexpected learning opportunities as they arise (which have a unique value for students).
- Whenever overseeing the use of technology in school or for homework or remote teaching, encourage and talk about appropriate behaviour and how to get help and consider potential risks and the age-appropriateness of websites (find out what appropriate filtering and monitoring systems are in place and how they keep children safe).
- Follow best-practice pedagogy for online-safety education, avoiding scaring, victim-blaming language and other unhelpful prevention methods.
- When supporting students remotely, be mindful of additional safeguarding considerations – refer to the remotesafe.lgfl.net infographic which applies to all online learning.
- Carefully supervise and guide students when engaged in learning activities involving online technology, supporting them with search skills, critical thinking, age-appropriate materials and signposting, and legal issues such as copyright and GDPR.
- Be aware of security best-practice at all times, including password hygiene and phishing strategies.
- Prepare and check all online sources and classroom resources before using for accuracy and appropriateness.
- Encourage students to follow their acceptable use policy at home as well as at school, remind them about it and enforce school sanctions.
- Take a zero-tolerance approach to all forms of child-on-child abuse, not dismissing it as banter - this includes bullying, sexual violence, and harassment.
- Be aware that you are often most likely to see or overhear online-safety issues (particularly relating to bullying and sexual harassment and violence) in the playground, corridors, toilets, and other communal areas outside the classroom – let the DSL/OSL know.
- Receive regular updates from the DSL/OSL and have a healthy curiosity for online safeguarding issues.
- Model safe, responsible, and professional behaviours in your own use of technology. This includes outside school hours and site, and on social media, in all aspects upholding the reputation of the school and of the professional reputation of all staff. More guidance on this point can be found in this Online Reputation guidance for schools.

Principal/Head of School

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.

- 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 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.
- Liaise with technical colleagues on a regular basis to have an understanding and awareness of filtering and monitoring provisions and manage them effectively – in particular understand what is blocked or allowed for whom, when, and how. Note that KCSIE 2025 strengthens the wording for this. [LGfL's Safeguarding Shorts: Filtering for DSLs and SLT twilight provides an overview].
- Liaise with the designated safeguarding lead on all online-safety issues which might arise and receive regular updates on school issues and broader policy and practice information.
- Support safeguarding leads and technical staff as they review protections for students in the home and remote-learning procedures, rules and safeguards [see remotesafe.lgfl.net for policy guidance and an infographic overview of safeguarding considerations for remote teaching technology].
- Take overall responsibility for data management and information security ensuring the school's provision follows best practice in information handling; work with the DPO and DSL to ensure a GDPR-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 students, including risk of children being radicalised.
- Ensure the school website meets statutory requirements.

Designated Safeguarding Lead / Online Safety Lead

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

- "The designated safeguarding lead should take **lead responsibility** for safeguarding and child protection [including online safety and understanding the filtering and monitoring systems and processes in place] … this **lead** responsibility should not be delegated".
- Work with the Principal/Head of School and technical staff to review protections for **students in the home** and **remote-learning** procedures, rules and safeguards [there is guidance at remotesafe.lgfl.net].
- Where the online-safety coordinator is not the named DSL or deputy DSL, ensure there is regular review and open communication between these roles and that the DSL's clear overarching responsibility for online safety is not compromised.
- Ensure "An effective whole school approach to online safety [that] empowers a school or college to protect and educate the whole school or college community in their use of technology and establishes mechanisms to identify, intervene in and escalate any incident where appropriate.".
- Ensure ALL staff undergo safeguarding and child protection training (including online safety) at induction and that this is regularly updated.
- Take day-to-day responsibility for online safety issues and be aware of the potential for serious child protection concerns.
- Be mindful of using appropriate language and terminology around children when managing concerns, including avoiding victim-blaming language [see spotlight.lgfl.net for a resource to use with staff on how framing things linguistically can have a safeguarding impact, and some expressions we use might be unhelpful].
- Remind staff of safeguarding considerations as part of a review of remote learning procedures and technology, including that the same principles of online safety and behaviour apply.

- Work with the Principal/Head of School and DPO to ensure a GDPR-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.
- 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, but also including hard-to-reach parents – dedicated resources at parentsafe.lgfl.net.
- Communicate regularly with the Senior Leadership Team 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 students to disclose issues when off site, especially when in isolation/quarantine/lockdown.
- Liaise with technical teams and ensure they are implementing not taking the strategic decisions on what is allowed and blocked and why. Also, as per KCSIE "be careful that 'over blocking' does not lead to unreasonable restrictions". [LGfL's Safeguarding Shorts: Filtering for DSLs and SLT twilight provides a quick overview and the LGfL the appropriate filtering statement is here.]
- Ensure KCSIE 'Part 5: Sexual Violence & Sexual Harassment' is understood and followed throughout the school and that 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).
- Facilitate training and advice for all staff, including supply teachers:
    - 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
    - Annex A is now a condensed version of Part one and can be provided (instead of Part one) to those staff who do not directly work with children, if the governing body or proprietor think it will provide a better basis for those staff to promote the welfare and safeguard children.
    - cascade knowledge of risks and opportunities throughout the organisation
    - cpd.lgfl.net has helpful CPD materials including PowerPoints, videos and more
- Pay particular attention to **online tutors**, both those engaged by the school as part of the DfE scheme who can be asked to sign the contractor AUP, [template you can use at safepolicies.lgl.net with provisions] and those hired by parents. [share the Online Tutors – Keeping Children Safe poster at parentsafe.lgfl.net to remind parents of key safeguarding principles].

Local Academy Board, led by Safeguarding Link Governor

Key responsibilities (quotes are taken from Keeping Children Safe in Education)

- Adopt this policy and strategy and subsequently review its effectiveness, e.g. by asking the questions in the helpful document from the UK Council for Child Internet Safety (UKCIS) Online safety in schools and colleges: Questions from the Governing Board .
- Undergo (and signpost all other governors and Trustees to attend) safeguarding and child protection training (including online safety) at induction to provide strategic challenge and into policy and practice, ensuring this is regularly updated – [LGfL's Safeguarding Training for school governors is free to all governors at safetraining.lgfl.net].

- Ensure that all staff also receive appropriate safeguarding and child protection (including online safety which, amongst other things, includes an understanding of the expectations, applicable roles and responsibilities in relation to filtering and monitoring) training at induction and that this is updated.
- "Ensure appropriate filters and appropriate monitoring systems are in place [but…] be careful that 'overblocking' does not lead to unreasonable restrictions as to what children can be taught with regard to online teaching and safeguarding".
- Ask about how the school has reviewed protections for **students in the home** (including when with online tutors) and **remote-learning** procedures, rules and safeguards [see remotesafe.lgfl.net for guidance].
- Support the school in encouraging parents and the wider community to become engaged in online safety activities.
- Have regular strategic reviews with the DSL and incorporate online safety into standing discussions of safeguarding at LAB meetings.
- Where the online-safety coordinator is not the named DSL or deputy DSL, ensure that there is regular review and open communication between these roles and that the DSL's clear overarching responsibility for online safety is not compromised.
- Work with the DPO, DSL and the Principal/Head of School to ensure a GDPR-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) at induction. The training should be regularly updated […] in line with advice from the local three safeguarding partners […] integrated, aligned and considered as part of the overarching safeguarding approach." There is further support for this at cpd.lgfl.net
- "Ensure that children are taught about safeguarding, including online safety […] as part of providing a broad and balanced curriculum […] Consider a whole school or college approach to online safety [with] a clear policy on the use of mobile technology." [NB – you may wish to refer to 'Teaching Online Safety in Schools 2019' and investigate/adopt the UKCIS cross-curricular framework 'Education for a Connected World – 2020 edition' to support a whole-school approach].

PSHE / RSHE Lead

Key responsibilities:

- As listed in the 'all staff' section, plus:
- Embed consent, mental wellbeing, healthy relationships and staying safe 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 students' lives." [dedicated training with curriculum mapping for RSHE/PSHE and online safety leads is available at safetraining.lgfl.net].
- Focus on the underpinning knowledge and behaviours outlined in Teaching Online Safety in Schools in an age appropriate way to help students to navigate the online world safely and confidently regardless of their device, platform or app.
- Assess teaching to "identify where students need extra support or intervention [through] tests, written assignments or self-evaluations, to capture progress" – [see LGfL's SafeSkills Online Safety Quiz and diagnostic teaching tool at safeskillsinfo.lgfl.net]
- This complements the computing curriculum, which covers the principles of online safety at all key stages, with progression in the content to reflect the different and escalating risks that students face. This includes how to use technology safely, responsibly, respectfully and securely, and where to go for help and support when they have concerns about content or contact on the internet or other online technologies.

- 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 new RSHE curriculum, and model positive attitudes and approaches to staff and students alike.
- Consider how the UKCIS framework Education for a Connected World and Teaching Online Safety in Schools can be applied in your context.
- Work closely with the DSL/OSL and all other staff to ensure an understanding of the issues, approaches, and messaging within Computing.
- Ensure subject specific action plans also have an online safety element.

Technical Services Team

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, so help DSLs and SLT to understand systems, settings and implications.
- Support DSLs and SLT to carry out an annual online safety audit as now recommended in KCSIE. [LGfL has a free template you can use at https://onlinesafetyaudit.lgfl.net] This should also include a review of technology, including filtering and monitoring systems (what is allowed, blocked and why and how 'over blocking' is avoided as per KCSIE), [we recommend you signpost them to LGfL's Safeguarding Shorts: Filtering for DSLs and SLT twilight at safetraining.lgfl.net which provides a quick overview to help build their understanding] protections for students in the home [e.g. LGfL HomeProtect filtering for the home – https://homeprotect.lgfl.net] and remote-learning. [see remotesafe.lgfl.net for guidance]
- Keep up to date with the school's online safety policy and technical information in order to effectively carry out their online safety role and to inform and update others as relevant.
- Work closely with the designated safeguarding lead / online safety lead / data protection officer / LGfL nominated contact / RSHE lead to ensure that school systems and networks reflect school policy and there are no conflicts between educational messages and practice.

- Ensure the above stakeholders understand the consequences of existing services and of any changes to these systems (especially in terms of access to personal and sensitive records / data and to systems such as YouTube mode, web filtering settings, sharing permissions for files on cloud platforms etc.
- Maintain up-to-date documentation of the school's online security and technical procedures.
- To report online-safety related issues that come to their attention in line with school policy.
- Manage the school's systems, networks and devices, according to a strict password policy, with systems in place for detection of misuse and malicious attack, with adequate protection, encryption and backup for data, including disaster recovery plans, and auditable access controls.
- Monitor the use of school technology, online platforms and social media and that any misuse/attempted misuse is identified and reported in line with school policy.

Data Protection Officer (DPO)

Key responsibilities:

- Be aware that of references to the relationship between data protection and safeguarding in key Department for Education documents 'Keeping Children Safe in Education' and 'Data protection: a toolkit for schools' (August 2018), especially this quote from the latter document:
- "GDPR does not prevent, or limit, the sharing of information for the purposes of keeping children safe. Lawful and secure information sharing between schools, Children's Social Care, and other local agencies, is essential for keeping children safe and ensuring they get the support they need. **The Data Protection Act 2018 introduced 'safeguarding' as a reason to be able to process sensitive, personal information, even without consent** (DPA, Part 2,18; Schedule 8, 4) When Designated Safeguarding Leads in schools are considering whether, or not, to share safeguarding information (especially with other agencies) it is considered best practice for them to record who they are sharing that information with and for what reason. If they have taken a decision not to seek consent from the data subject and/or parent/carer that should also be recorded within the safeguarding file. All relevant information can be shared without consent if to gain consent would place a child at risk. Fears about sharing information **must not be allowed** to stand in the way of promoting the welfare and protecting the safety of children."

The same document states that the retention schedule 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 student 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.

- Work with the DSL and the Principal/Head of School to ensure frameworks are in place for the protection of data and of safeguarding information sharing as outlined above.
- Ensure that all access to safeguarding data is limited as appropriate, and also monitored and audited.

Volunteers and contractors (including tutor)

Key responsibilities:

- Read, understand, sign and adhere to an acceptable use policy (AUP).
- Report any concerns, no matter how small, to the designated safety lead / online safety coordinator as named in the AUP.
- Maintain an awareness of current online safety issues and guidance.
- Model safe, responsible and professional behaviours in their own use of technology at school and as part of remote teaching or any online communications.
- Note that as per AUP agreement a contractor will never attempt to arrange any meeting, **including tutoring session,** without the full prior knowledge and approval of the school, and will never do so directly with a student. The same applies to any private/direct communication with a student.

Students

Key responsibilities:

- Read, understand, sign and adhere to the student acceptable use policy and review this annually.
- Treat **home learning during any isolation/quarantine or bubble/school lockdown** in the same way as regular learning in school and behave as if a teacher or parent were watching the screen.
- Avoid any private communication or use of personal logins/systems to communicate with or arrange meetings with school staff or tutors.
- Understand the importance of reporting abuse, misuse or access to inappropriate materials, including any concerns about a member of school staff or supply teacher or online tutor.
- Know what action to take if they or someone they know feels worried or vulnerable when using online technology, at school, home or anywhere else.
- To understand the importance of adopting safe and responsible behaviours and good online safety practice when using digital technologies outside of school and realise that the school's acceptable use policies cover actions out of school, including on social media.
- Remember the rules on the misuse of school technology – devices and logins used at home should be used just like if they were in full view of a teacher.
- Understand the benefits/opportunities and risks/dangers of the online world and know who to talk to at school or outside school if there are problems.

Parents/carers

Key responsibilities:

- Read, sign, and promote the school's parental acceptable use policy (AUP) and read the student AUP and encourage their children to follow it.
- Talk to the school if they have any concerns about their children's and others' use of technology.
- Promote positive online safety and 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.
- Encourage children to engage fully in home-learning, whether for homework or during any school closures or isolation and flag any concerns.
- Support the child during any home learning to avoid video calls in a bedroom if possible and if not, to ensure the child is fully dressed and not in bed, with the camera pointing away from beds/bedding/personal information etc. and the background blurred or changed where possible.
- If organising private online tuition, remain in the room, if possible, ensure the child knows tutors should not arrange new sessions directly with the child or attempt to communicate privately. Further advice available in the Online Tutors – Guidance for Parents and Carers poster at parentsafe.lgfl.net, which is a dedicated parent portal offering updated advice and resources to help parents keep children safe online.

External groups including parent associations

Key responsibilities:

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

Appendix 2 – Related Policies and Documents

1. Child Protection and Safeguarding Policy
2. Behaviour Policy / Anti-Bullying Policy
3. Staff Code of Conduct
4. *Acceptable Use Policies (AUPs) for:
    - *Pupils [Symbolised Version / KS1 / KS2 / KS3 / KS4]
    - *Staff, Volunteers Governors & Contractors
    - *Parents
5. *Online-Safety Questions from the Governing Board (UKCIS)
6. *Education for a Connected World cross-curricular digital resilience framework (UKCIS)
7. *Safer working practice for those working with children & young people in education (Safer Recruitment Consortium)
8. *Working together to safeguard children (DfE)
9. *Searching, screening and confiscation advice (DfE)
10. *Sharing nudes and semi-nudes guidance from UKCIS:
    - *How to respond to an incident - overview for all staff
    - *Full guidance for school DSLs
    - *Online Safety Audit for Trainee (ITT) & Newly Qualified Teachers (NQT)
11. *Prevent Duty Guidance for Schools (DfE and Home Office documents)
12. Data protection policy
13. *Cyber security advice, procedures etc
14. *Preventing and tackling bullying (DfE)
15. Cyber bullying: advice for headteachers and school staff (DfE) – find this at bullying.lgfl.net
16. *RAG (red-amber-green) audits for statutory requirements of school websites
17. *Ofsted Review of sexual abuse in schools and colleges