



Consilium
Academies



ONLINE SAFETY POLICY

September 2026



Date of Approval: 24.09.26

Approved by: Trust Board

Date of next Review: September 2027

Excellence and Equity with integrity

Contents

What is this policy?	4
Who is it for; when is it reviewed?	4
Who leads online safety?	4
What are the main online safety risks in 2026/2027?	4
Online Safeguarding Trends	4
How will this policy be communicated?	8
Overview	9
Aims	9
Scope	9
Roles and responsibilities	9
Education and curriculum	10
Handling safeguarding concerns and incidents	11
Nudes & Semi Nudes	13
Priority Areas	14
Upskirting	14
Bullying	15
Child-on-child sexual violence and sexual harassment	15
Misuse of school technology (devices, systems, networks or platforms)	15
Social media incidents	15
CCTV	16
Extremism	16
Data protection and cyber security	16
Appropriate filtering and monitoring	19
Messaging/commenting systems (incl. email, learning platforms & more)	20
Authorised systems	20
Behaviour/usage principles of messaging/commenting systems	20
Use of generative AI	21
Online storage or learning platforms	22
School website	22
Digital images and video	23
Social media	23
Our SM presence	23
Staff, pupils' and parents' social media presence	24
Device usage	25
Personal devices including wearable technology and bring your own device (BYOD)	25

All staff who work directly with children	25
Parents	26
Use of school devices	26
Trips / events away from school	26
Searching and confiscation	27
Appendix A – Roles	28
All staff	28
Key responsibilities:	28
Principal	29
Key responsibilities:	29
Designated Safeguarding Lead	30
Local Academy Board, led by Safeguarding Link Governor	32
Key responsibilities (quotes are taken from Keeping Children Safe in Education)	32
Key responsibilities (quotes are taken from Keeping Children Safe in Education)	32
PSHE / RSHE Lead/s	34
Key responsibilities:	34
Computing Lead	35
Key responsibilities:	35
Subject / aspect leaders	35
Key responsibilities:	35
Consilium Technical Services Team	35
Key responsibilities:	35
Data Protection Officer (DPO)	36
Key responsibilities:	36
Volunteers and contractors (including tutor)	36
Key responsibilities:	36
Pupils	37
Key responsibilities:	37
Parents/carers	37
Key responsibilities:	37
External groups (e.g. those hiring the premises) including parent associations	37
Key responsibilities:	37
Appendix B: The National Landscape of Online Safety	38
National Online Safeguarding Trends	38
1. MONITORING	38
2. OFCOM'S LATEST RESEARCH	38
3. IWF, CSAM CONCERNS	39

4. "COM NETWORKS"

39

5. CYBER ATTACKS

39

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

Who is it for; when is it reviewed?

This policy is a living document, subject to full annual review and amended where necessary during the year in response to developments in the school and local area. This document will help all stakeholders to understand the rules that are in place, why they are, and how the policy affects day-to-day practice. Acceptable Use for different stakeholders helps with this. Any changes to this policy will be immediately disseminated to all the above stakeholders.

Who leads online safety?

KCSIE 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 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 2026/2027?

There are 4 types of online safety risks outlined in KCSIE:

CONTENT: being exposed to illegal, inappropriate, or harmful content, for example: pornography, racism, misogyny, self-harm, suicide, antisemitism, radicalisation, extremism, extreme sexual or physical violence, misinformation, disinformation (including fake news) and conspiracy theories.

CONTACT: being subjected to harmful online interaction with other users or generative AI applications that simulate this; for example: peer to peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes.

CONDUCT: online behaviour that increases the likelihood of, or causes, harm; for example, making, sending and receiving explicit images, including those generated using AI and online bullying, and

COMMERCE: risks such as online gambling, inappropriate advertising, phishing and or financial scams.

It is the responsibility of all staff to understand the above, recognise when a child may be experiencing harm related to the above, and report to the DSL.

Online Safeguarding Trends

In our school over the past year, we have 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 pupils.

In 2026-27, 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?

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

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

Overview

Aims

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

- Setting out expectations for all Consilium Academies community members' online behaviour, attitudes and activities and use of digital technology (including when devices are offline).
- Helping safeguarding and senior leadership teams to have a better understanding and awareness of all elements of online safeguarding through effective collaboration and communication with technical colleagues (e.g. for filtering and monitoring), curriculum leads (e.g. RSHE) and beyond.
- Helping all stakeholders to recognise that online/digital behaviour standards (including social media activity) must be upheld beyond the confines of the school gates and school day, regardless of device or platform, and that the same standards of behaviour apply online and offline.
- Facilitating the safe, responsible, respectful and positive use of technology to support teaching and learning, increase attainment and prepare children and young people for the risks and opportunities of today's and tomorrow's digital world, to survive and thrive online.
- Helping school staff working with children to understand their roles and responsibilities to work safely and responsibly with technology and the online world:
 - for the protection and benefit of the children and young people in their care, and
 - for their own protection, minimising misplaced or malicious allegations and to better understand their own standards and practice.
 - for the benefit of the school, supporting the school ethos, aims, and objectives, and protecting the reputation of the school and profession.
- Establishing clear structures by which online misdemeanours will be treated, and procedures to follow where there are doubts or concerns (with reference to other school policies such as Behaviour Policy).

Scope

This policy applies to all members of the Consilium Academies community (including teaching, supply and support staff, trainee teachers, Trustees, LAB members, volunteers, contractors, pupils, parents/carers, visitors and community users) who have access to our digital technology, networks and systems, whether on-site or remotely, and at any time, or who use technology in their school role. It applies primarily to their usage of Trust owned IT equipment and systems but can in some instances impact the use of personal devices where the activity is work related.

Roles and responsibilities

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

All members of the school community should **read the relevant section in Appendix A of this document** that describes individual roles and responsibilities. Please note that there is one for 'All Staff' that must be read by all staff, including those who have a named role in another section. There are also role descriptions in the Appendix A, e.g. pupil, staff, etc. All staff have a key role to play in feeding back on potential issues.

Education and curriculum

Despite the risks associated with being online, Consilium Academies recognises the opportunities and benefits for children too. Technology is a fundamental part of adult life and so developing the competencies to understand and use it, is critical to children's later positive outcomes. The choice to use technology in school will always be driven by pedagogy and inclusion.

At Consilium Academies, we engage our pupils in discussions about online safety and technology use. This helps us to ensure that our teaching of online safety is up to date and responsive to children's experiences and needs.

As well as teaching about the underpinning knowledge and behaviours that can help pupils navigate the online world responsibly, safely and confidently regardless of the device, platform or app, [Teaching Online Safety in Schools](#) recommends embedding teaching about online safety and harms through a whole school approach and provides an understanding of these risks to help tailor teaching and support to the specific needs of pupils, including vulnerable pupils.

RSHE guidance also recommends that schools assess teaching to "The curriculum should build knowledge and skills sequentially, with regular feedback provided on pupil progress. Lessons should ensure that all pupils are challenged, and assessments should identify where pupils need extra support or intervention."

The teaching of online safety, features in these particular areas of curriculum delivery:

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

However, it is the role of ALL staff to identify opportunities to thread online safety through all school activities, both outside the classroom and making the most of unexpected learning opportunities as they arise.

Whenever overseeing the use of technology in school or setting as homework tasks, all staff will encourage sensible use, monitor what pupils are doing and consider potential risks and the age appropriateness of tasks. This includes supporting them with search skills, reporting and accessing help, critical thinking (e.g. bias, disinformation, misinformation, and conspiracy theories), access to 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.

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

We utilise data from our safeguarding reports, filtering logs, monitoring captures, parental complaints and other stakeholder feedback to inform our curriculum, so that we are constantly learning from concerns and being reflexive and responsive to the needs of our children.

We recognise that nationally, children with SEND are less likely to receive effective online safety teaching but are more at risk of being a victim of harm caused online. Therefore, at Consilium Academies, we will ensure that we adapt our curriculum and teaching of online safety for all children, especially those with SEND. We will also consider whether specific filtering policies are required for particular children to afford more protection from online harms. We will also consider targeted and individual interventions that children need to protect them from harm and prevent future online harm.

We communicate with parents and carers about how we support pupils with their online safety learning, including what their children are being asked to do online and the sites they will be asked to access.

Handling safeguarding concerns and incidents

Online safety concerns are safeguarding concerns. They 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 speak to the safeguarding lead with any concerns (no matter how small they seem) to contribute to the overall picture or highlight what might not yet be a problem.

Support staff will often have unique insight and opportunity to find out about issues first in the playground, corridors, toilets and other communal areas outside the classroom.

School procedures for dealing with recognition and response to online safety will be mostly detailed in the following policies:

- Child Protection & Safeguarding 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
- Artificial Intelligence Policy

This Trust commits to taking all reasonable precautions to safeguard pupils online, but the internet can never be 100% safe (as stated in KCSIE), and we recognise 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).

Any suspected online risk or infringement should be reported to the DSL as soon as possible on the same day. The reporting member of staff will ensure that a record is made of the concern on CPOMS - this includes any concerns raised by the filtering and monitoring systems (see section further on in this policy for more information).

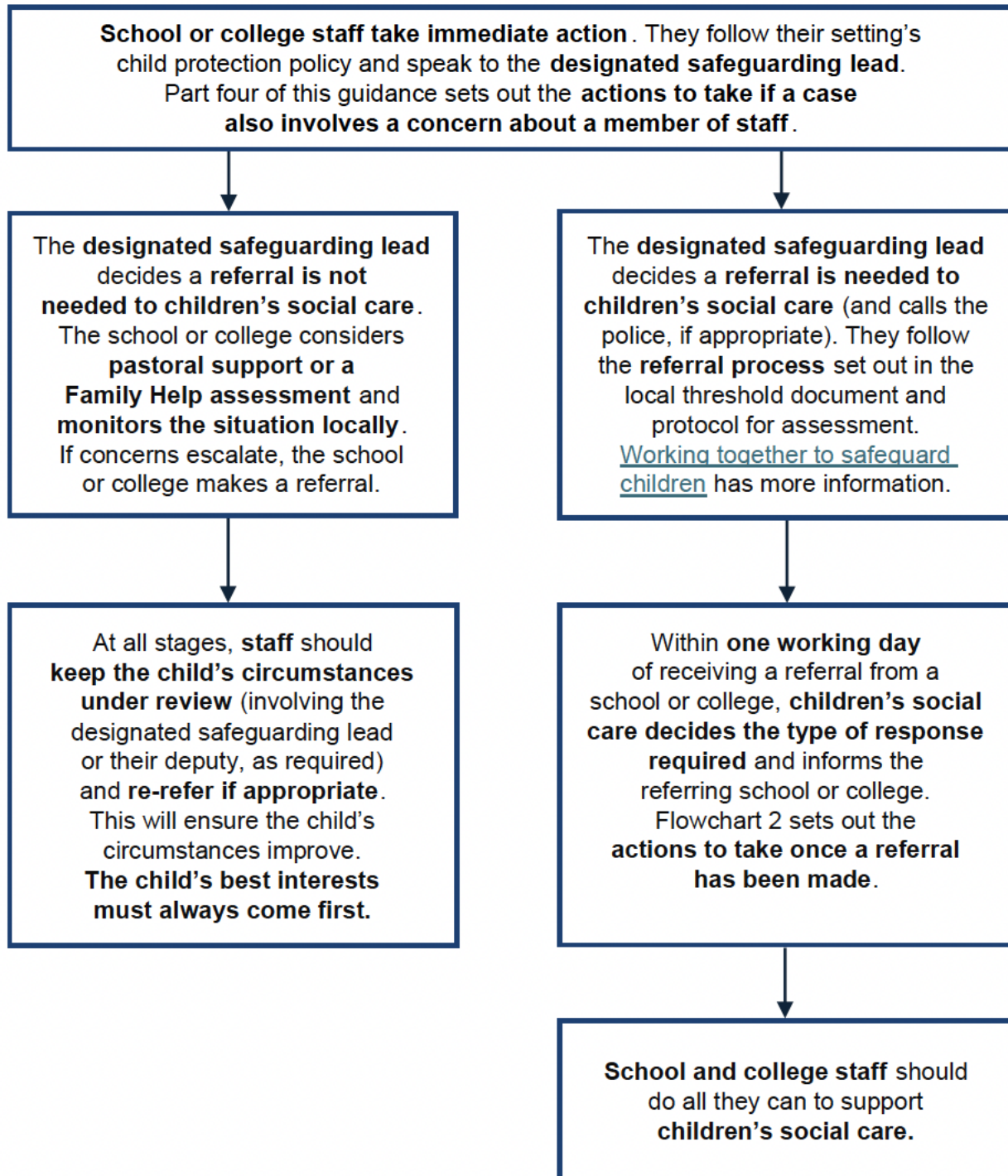
As per the Children's Wellbeing and Schools Act (2026), there is now a mandatory duty for teachers to report any concerns of child sexual abuse, which includes sexual abuse that is facilitated by and/or takes place online (including non-contact abuse such as image sharing). Therefore, all staff must report such concerns without delay to the DSL.

Any concern/allegation about staff misuse is always (as per any safeguarding allegation) referred directly to the Principal, unless the concern is about the Principal, 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.

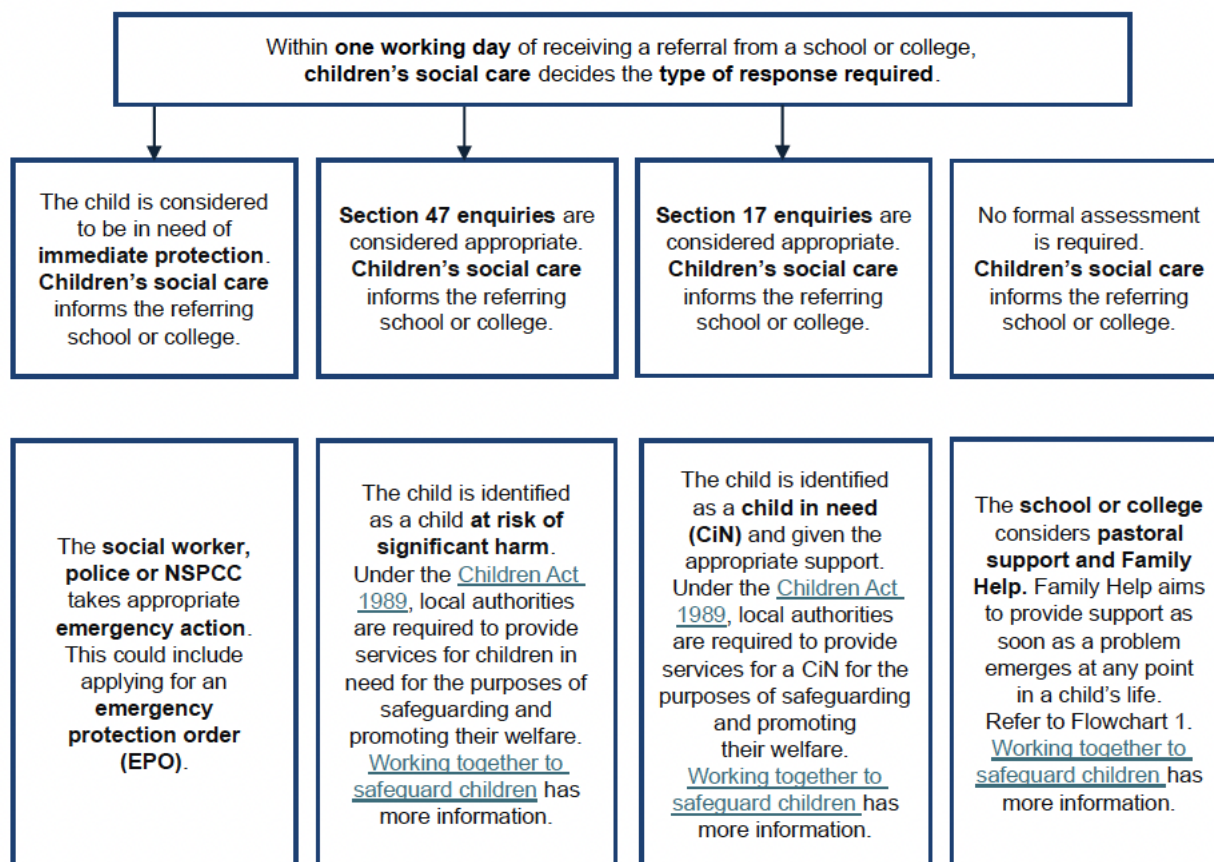
The school will actively seek support from other agencies as needed (i.e. the local authority, LGfL, UK Safer Internet Centre's Professionals' Online Safety Helpline (POSH), NCA CEOP, Prevent Officer, Police, IWF and Harmful Sexual Behaviour Support Service).

We will inform parents/carers of online safety incidents involving their children, Children's Services and the Police where staff or pupils engage in or are subject to behaviour which we consider is particularly concerning or breaks the law.

The following flow charts are taken from page 27/28 of Keeping Children Safe in Education 2026 as the key education safeguarding document. As outlined previously, online safety concerns are no different to any other safeguarding concern.



Flowchart 2: actions taken once a referral has been made to children's social care



The following sub-sections provide details on managing particular types of concern.

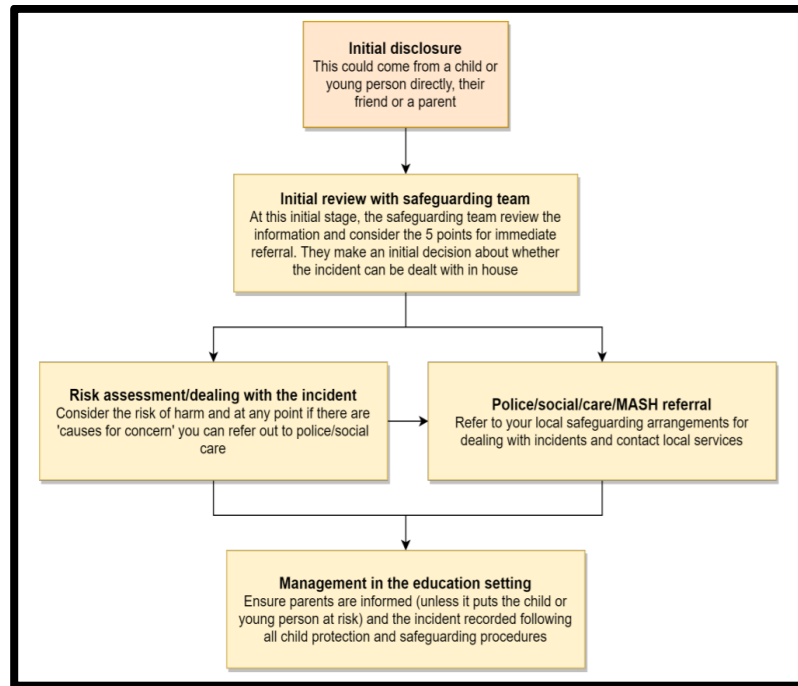
Nudes & Semi Nudes

All schools (regardless of phase) should refer to the UK Council for Internet Safety (UKCIS) guidance - [Sharing nudes and semi-nudes: advice for education settings](#).

There is a one-page overview called [Sharing nudes and semi-nudes: how to respond to an incident](#) for all staff (not just classroom-based staff) to read, in recognition of the fact that it is mostly someone other than the Designated Safeguarding Lead (DSL) 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 go straight to the DSL.**

Everyone must understand that whilst the sharing of intimate or sexual images involving children (created via AI or otherwise) is illegal, pupils should be encouraged and supported to talk to members of staff if they have made a mistake or had a problem in this area. The UKCIS guidance seeks to avoid unnecessary criminalisation of children.

The school DSL will use the full guidance document, [Sharing nudes and semi-nudes – advice for educational settings](#) to decide next steps and whether other agencies need to be involved (see flow chart below from the UKCIS guidance) and next steps regarding liaising with parents and supporting pupils. The school will also make use of guidance from [The Marie Collins Foundation](#) with regards to supporting victims of Technology Assisted Child Sexual Abuse.



This LGfL document (available at nudes.lgfl.net) may also be helpful for DSLs in making their decision about whether to refer a concern about sharing of sexual imagery of children:

SAFEGUARDING QUESTION TIME

Q: WHEN SHOULD WE REFER NUDE SHARING?

A: IMMEDIATELY *IF* THE IMAGE/VIDEO:

- involves an **adult**
- is potentially **coerced**, blackmailed or groomed or concerns about **capacity to consent**
- might depict sexual acts unusual for their **developmental stage or violent**
- involves sexual acts / **under 13s**
- or the young person is at **immediate risk of harm**..., **suicidal or self-harming**

Text simplified, taken from page 20 of 'Sharing Nudes and Semi-Nudes', UKCIS – search.gov.uk

We recommend DSLs read the entire UKCIS document; there is much more to know than this, and many helpful resources including training, scenarios and further guidance. Note also the one-pager for all staff!



LGfL
SafeguardED

Priority Areas

Upskirting

Everyone must understand that upskirting (taking a photo or video 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, pupils can come and talk to members of staff if they have made a mistake or had a problem in this area. Upskirting has become more prevalent due to the increased use of smart glasses and other discreet recording technology that can capture imagery without individuals knowing.

Bullying

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

Child-on-child sexual violence and sexual harassment

All staff will be aware that children can abuse other children (often referred to as child-on-child abuse), and that it can happen both inside and outside of school and online. All staff will follow the Trust's Child Protection and Safeguarding Policy and procedures and be clear in how important their role is in preventing and responding where they believe a child may be at risk from it.

Part Five 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 that 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.

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

Social media incidents involving pupils are often safeguarding concerns and should be treated as such where there are concerns of harm being caused, and staff should follow the safeguarding policy. Other policies that govern these types of incidents are the school's Acceptable Use Policies/social media policy.

Further to this, where an incident relates to an inappropriate, upsetting, violent or abusive social media post by a member of the school community (e.g. parent or visitor), Consilium Academies will request that the post be deleted and will expect this to be actioned promptly. The police may need to be contacted if an offence is committed.

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 must 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 easily accessed and highly prevalent on mainstream platforms.

Data protection and cyber security

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/carers 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, Trustees, volunteers, contractors, trainee teachers 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 is 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 compliant 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

The DSL has lead responsibility for filtering and monitoring and works closely with the Trust Head of IT to implement the [DfE Filtering and Monitoring Standards](#).

We provide 'appropriate filtering and monitoring' (as outlined in KCSIE) in our school.

Our filtering system is called Sophos XG and monitoring is provided by NetSupport Classroom Cloud. For devices that go off-site, Classroom Cloud must always be installed. These systems are accredited by the UK Safer Internet Centre .

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. We ensure all staff are aware of their responsibility in feeding back about areas of concern, potential for pupils to bypass systems and any potential over blocking. Staff can submit concerns at any point through the IT helpdesk and will be asked for feedback at the time of the regular checks, which take place between the on-site IT team and the DSL.

Technical and safeguarding colleagues work together closely to carry out an annual review and regular checks of filtering and monitoring, and to ensure that the school responds to issues, considers how to prevent further concerns and integrates with the curriculum.

We carry out half-termly checks to ensure filtering is operational, functioning as expected, etc., and an annual review as part of an online safety audit of strategy, approach etc. More details of both documents and results are available on request from the DSL.

Where staff use Gen AI, they must follow the guidelines and principles of our AI Policy. For students and young people, we block the generative AI category via our filtering and only allow specific pre-approved sites (see the 'Use of Generative AI' section of this policy for more information, as schools must ensure that any Gen AI used with pupils meets the [DfE Product Safety Standards for Gen AI](#)). We know that what children input and what the tool outputs cannot be guaranteed as safe and inappropriate/harmful content can be generated, so we carefully monitor output and limit their use (also in line with DfE guidelines).

Safe Search is enforced on any accessible search engines on all school-managed devices Please note however that even with Safe Search enforced, AI is embedded in many search engine responses, and this presents risk to users in terms of misinformation, bias, hallucinations and inappropriate content.

We recommend the use of Google.

Our YouTube mode is Moderate – Restricted YouTube access. This helps us to limit inappropriate content that is served to pupils.

The DSL checks filtering reports and notifications and takes any necessary action as a result.

According to the DfE standards, the school should have a plan for how to “monitor pupils when using school-managed devices connected to the internet. At Consilium Academies, we use Classroom Cloud for monitoring. The Trust does not permit the use of BYOD for staff or students.

Monitoring software is deployed through management systems to all staff and students’ devices across the Trust. DSLs should be aware that reports and monitoring from certain devices are more limited, in particular Apple technologies such as iPads and Macs can present challenges.

All activity is logged by Classroom Cloud and the network level filtering applications. Alerts relating to students are logged for review by the DSL and appropriate Heads of Year or teaching staff members. For staff activity, logs are reviewed at school level by the DSL and Principal and can be subject to ad-hoc review by members of the central team. Central team activity is reviewed by the Director of HR, with the Director of HR activity reviewed by the Chief Executive.

Alerts are checked as soon as colleagues are notified by their e-mail or online system.

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

Authorised systems

- **Pupils** at this school communicate with each other and with staff using Microsoft Teams. Some curriculum software packages also include the ability to upload and share information.
- **Staff, LAB Members and Trustees** at this school use the email system provided by Microsoft 365 for all school emails. They must never use a personal/private email account (or other messaging platforms) to communicate with children or parents, or to colleagues when relating to school/child data, using a non-school-administered system.

Any systems must be centrally managed and administered by the school or authorised IT partner (i.e. they can be monitored/audited/viewed centrally; are not private or linked to private accounts). This is for the mutual protection and privacy of all staff, pupils and parents, supporting safeguarding best-practice, protecting children against abuse, staff against potential allegations and in line with UK data protection legislation.

Use of any new platform or app with communication facilities or any child login or storing school/child data must be approved in advance by the Trust and centrally managed.

Any unauthorised attempt to use a different system may be a safeguarding concern or disciplinary matter and should be notified to the DSL (if by a child) or to the Principal (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/Principal/DPO (the circumstances of the incident will determine whose remit this is) should be informed immediately.

Behaviour/usage principles of messaging/commenting systems

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/Principal/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.

Use of generative AI

At Consilium Academies, we acknowledge that generative AI platforms (e.g. ChatGPT, Canva, Co-pilot or Gemini for the creation of new text/imagery/code/music etc) are becoming commonly used by both children and adults. We are aware of and follow the [DfE's guidance](#) on this and we follow the subsequent principles:

The use of any Gen AI in our setting (by staff or pupils) will be carefully managed by the school to ensure that users and their data are safe.

Staff are only permitted to use their school email account when using pre-approved Gen AI, and they must not enter data relating to children, staff or the school which is personal or sensitive.

The school has a clear and well communicated approach to the use of any Gen AI (by staff or pupils), and this is aligned with the school's values and pedagogical approaches.

To help users to safely use technology, we will talk about the use of these tools with pupils, staff and parents – their practical use as well as their safety and ethical pros and cons.

We are aware that there will be use of these apps and exposure to Gen AI creations on devices at home for many pupils – these experiences may be both positive/creative and also negative (e.g. data breaches, misinformation, bullying, deepfakes, creation of deepfake intimate imagery and chatbots that encourage unhealthy and inappropriate relationships). Therefore, it is important as a school that we support pupils in developing digital literacy skills to help mitigate these risks.

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

Online storage or learning 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)

School website

The school website is a key public-facing information portal for the school community (both existing and prospective stakeholders) with a key reputational value. The Principal and Trustees have delegated the day-to-day responsibility of updating the content of the website and ensuring compliance with DfE stipulations to the Head of Governance and Compliance.

The website is managed by / hosted by E4Education and the Marketing Team.

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 must only be used with permission. Many open-access libraries of public-domain images/sounds, etc. can be used. Finding something on Google or YouTube does not mean that copyright has been respected. If in doubt, check with the Marketing Team.

Digital images and video

In light of image manipulation by Gen AI platforms to create sexual imagery of children and adults, the UK Online Harms Early Warning Working Group published guidance in May 2026 stating that schools should reconsider publishing pupil and staff images on websites/social media ([guidance here](#)).

Our approach to publishing imagery of pupils on our website/social media/marketing materials is to publish lower resolution images of children which will be kept under review. Photos are only added following consent from parents and carers.

When a pupil 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.

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 Consilium Academies, no member of staff will ever use their personal phone to capture photos or videos of pupils.

Photos are stored within our cloud platform in line with the retention schedule of the school's Data Protection Policy. Any concerns about the nature of these images will be reported to the DSL.

Parents must **not** covertly film or record any interactions with pupils or adults in schools or near the school gates, nor share images of other people's children on social media, as there may be cultural or legal reasons why this would be inappropriate or even dangerous (see nofilming.lgfl.net for more information). Further information on managing pupil image and video content is available [here](#).

We encourage parents and children to think about their online reputation and digital footprint, and role model not oversharing on social media (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 used and 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.

Social media

Our SM presence

Consilium Academies 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.

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. We conduct regular checks of privacy and security settings on social media accounts to ensure appropriate access.

The Marketing Team is responsible for managing our X-Twitter/Facebook/and other social media accounts and checking our Wikipedia and Google reviews and other mentions online. In some academies, delegated access for day-to-day upload will be given to members of the leadership or administrative teams. This is at the discretion of the Marketing Manager.

Staff, pupils' and parents' social media presence

Social media is a fact of modern life, and as a school, we accept that many parents, staff and pupils will use it. However, as stated in the acceptable use policies, 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, pupils and parents, also undermining staff morale and the reputation of the school (which is important for the pupils we serve).

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

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

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

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

As outlined in the Acceptable Use Policies, 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 are discouraged from 'following' staff, Trustees, LAB members, trainee teacher, 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 Principal/Principal and should be declared upon entry of the pupil or staff member to the school).*

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

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 that 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)

- Our approach to pupils using mobile phones is in line with the DfE Guidance. Students during the school day, phones and smart watches must remain turned off at all times. 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.
- Personal recording devices, such as smart glasses, are not permitted in school without written permission. It is forbidden to take secret photos, videos or recordings of teachers or pupils, including remotely, with any device.

All staff who work directly with children

- 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 seek permission from the Principal to retain access to their device for the specific incident.
- Volunteers, contractors, LAB members, Trustees, trainee teachers, 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 should be sought from a member of school staff and all photos must be taken in the presence of a member staff.
- See also the 'Digital images and video' section of this document and the school data protection cyber security policies. Child/staff data should never be downloaded onto a private phone.
- Other personal recording devices such as smart glasses are not permitted in school without written permission. It is forbidden to take secret photos, videos or recordings of teachers or pupils, including remotely, with any device.

In some instances, it may be appropriate for students and staff to retain access to technology in order to effectively manage a health condition such as diabetes. Our approach will be based on relevant risk assessments and in dialogue with parents and other key professionals.

Parents

- 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.
- Should ask permission before taking any photos, e.g. of displays in corridors or classrooms, and avoid capturing other children. Please see the Digital images and video section of this document for more information about filming and photography at school events.
- Parents are asked not to call pupils on their mobile phones during the school day; urgent messages can be passed via the school office.
- We do not allow Apple AirTags or similar devices in school. Please note that it is against the terms and conditions of these products to use them to track a child.
- It is forbidden to take secret photos, videos or recordings of teachers or pupils, including remotely, with any device. Other personal recording devices such as smart glasses are not permitted in school without written permission.

Use of school devices

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

Wi-Fi is accessible to staff for school-related internet use / limited personal use within the framework of the acceptable use policy. All such use is monitored and filtering restrictions apply as if the device were school owned. This means social media and platforms such as WhatsApp will be blocked.

School devices for staff or pupils are restricted to the apps/software installed by the school, whether for use at home or school, and may be used for learning. Staff and pupils are not permitted to use Virtual Private Networks (VPNs) on the school network or make any other attempts to bypass the school's filtering. Our filtering is set up to block all use of Virtual Private Networks (VPNs) on school owned devices and across the network.

Users should know that all and any usage of school owned devices, systems and platforms will be tracked.

Trips / events away from school

For school trips/events away from school, teachers will be issued a school duty phone, and this number will be used for any authorised or emergency communications with pupils and parents. Any deviation from this policy (e.g. by mistake or because the school phone will not work) will be reported immediately to the Principal. Teachers using their personal phone in an emergency will ensure the number is hidden to avoid a parent or pupil accessing a teacher's private phone number.

Where appropriate and cost effective, the Trust will seek to agree with staff members that they will utilise the school phone system mobile application on their personal mobile phones. This allows a single landline number that can be called by pupils, parents or staff and a 'round-robin' call group to all members of staff on the trip is created. This ensures that there is not a single point of failure and that all staff on duty can answer any calls. It is also technically reliable and will use wireless calling or existing travel data plans, rather than relying on out of date pay-as-you-go technology or restricted corporate accounts that may not always work when outside of the UK.

If on trips, pupils are encouraged to connect to another organisation's Wi-Fi/network, staff must be aware that other connections may not be as well controlled (e.g. via filtering and monitoring) as the network and systems in school. Therefore, staff are responsible for risk assessing and managing such situations and should seek advice from the DSL where necessary.

Parents will be reminded about their child's permitted device use whilst on trips away from school, including that tracking devices such as Airtags are not permitted for the safety of all pupils.

Searching and confiscation

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

Full details of the school's search procedures are available in the school's Behaviour Policy.

Appendix A – Roles

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

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

Roles:

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

All staff

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 2026. 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

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 2026 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

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 on 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 and trainee teachers:
 - all staff must read KCSIE Part 1 and all those working with children also Annex A – translations are available in 13 community languages at kcsietranslate.lgfl.net
 - 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.lgfl.net with provisions] and those hired by parents.

Local Academy Board, led by Safeguarding Link Governor

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

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 and Annex A.
- “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].
- Trustees and LAB members should ensure Consilium Academies has appropriate filtering and monitoring systems in place and regularly review their effectiveness at least once every academic year.
- Read all of KCSIE to ensure all Trustees and LAB members understand their safeguarding responsibilities.

PSHE / RSHE Lead/s

Key responsibilities:

- As listed in the ‘all staff’ section, plus:
- Embed statutory [RSHE Guidance](#), including consent, mental wellbeing, healthy relationships and staying safe online, as well as raising awareness of the risks and challenges from the latest trends in 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.”

- Focus on the underpinning knowledge and behaviours outlined in [Teaching Online Safety in Schools](#), in an age-appropriate way to help pupils navigate the online world safely and confidently regardless of their device, platform or app.
- Assess teaching to “identify where pupils need extra support or intervention [through] tests, written assignments or self-evaluations, to capture progress” to complement the computing curriculum.
- Work closely with the DSL and all other staff to ensure understanding of the issues, approaches, and messaging within PSHE / RSHE.
- Develop and implement a RSHE policy and publish this 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 and all other staff to ensure understanding of the issues, approaches, and messaging within Computing.
- Collaborate with technical staff and others responsible for ICT use in school to ensure a common and consistent approach, in line with acceptable-use agreements.

Subject / aspect leaders

Key responsibilities:

- As listed in the ‘all staff’ section, plus:
- Look for opportunities to embed online safety in your subject or aspect, especially as part of the RSHE curriculum, and model positive attitudes and approaches to staff and pupils alike.
- Consider how the UKCIS framework ‘Education for a Connected World’ and ‘Teaching Online Safety in Schools’ can be applied in your context.
- Work closely with the DSL 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.

Consilium 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.
- Support safeguarding teams to understand and manage filtering and monitoring systems and carry out regular reviews and annual checks.

- Support DSLs and SLT to carry out an annual online safety audit as 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 DfE and remote learning.
- Keep up to date with the school's online safety policy and technical information 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 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 any changes to these systems (especially access to personal and sensitive records / data and to systems such as YouTube mode, web filtering settings, sharing permissions for files on cloud platforms etc. Ensure filtering and monitoring systems work on new devices and services before releasing them to pupils and staff.
- Maintain up-to-date documentation of the school's online security and technical procedures.
- To report online safety related issues that come to their attention in line with school policy.
- Manage the school's systems, networks and devices according to a strict password policy, with systems in place for detection of misuse and malicious attack, with adequate protection, encryption and backup for data, including disaster recovery plans, and auditable access controls.
- Ensure the data protection policy and cyber security policy are up to date, easy to follow and practicable.
- Monitor the use of school technology, online platforms and social media presence and ensure that any misuse/attempted misuse is identified and reported in line with school policy.

Data Protection Officer (DPO)

Key responsibilities:

Alongside those of other staff, provide data protection expertise and training and support the DP and cyber security policy and compliance with those and legislation and ensure that the policies conform with each other and with this policy.

Not to 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, "Data protection laws do not prevent the sharing of information for the purposes of keeping children safe and promoting their welfare."

Note that retention schedules for safeguarding records may be required to be set as 'Very long-term need (until pupil is aged 25 or older)'. However, some local authorities require record retention until the age of 25 for all pupil records. You should check the requirements in your area.

Ensure that all access to safeguarding data is limited as appropriate and also monitored and audited.

Volunteers and contractors (including tutor)

Key responsibilities:

- Read, understand, sign and adhere to an Acceptable Use Policy (AUP)
- Report any concerns, no matter how small, to the Designated Safeguarding Lead.
- Maintain an awareness of current online safety issues and guidance.
- Model safe, responsible and professional behaviours in their own use of technology at school and as part of remote teaching or any online communications.

- Note that as per the AUP agreement, a contractor will never attempt to arrange any meeting, **including a tutoring session**, without the full prior knowledge and approval from the school, and will never do so directly with a pupil. The same applies to any private/direct communication with a pupil.

Pupils

Key responsibilities:

Read, understand, sign and adhere to the pupil Acceptable Use Policy.

Parents/carers

Key responsibilities:

- Read, sign and adhere to the school's parental Acceptable Use Policy (AUP), read the pupil AUP and encourage their children to follow it.

External groups (e.g. those hiring the premises) including parent associations

Key responsibilities:

- Any external individual/organisation will sign an acceptable use policy prior to using technology or the internet within the 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 others' images or details without permission and refraining from posting negative, threatening or violent comments about others, including the school staff, volunteers, governors, contractors, pupils or other parents/carers.

Appendix B: The National Landscape of Online Safety

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 see in the context of the 4 Cs (see KCSIE for more details).

National Online Safeguarding Trends

1. MONITORING

The following are concerns highlighted through partnership with Senso and monitoring data from LGfL schools. Many children are using Gen AI platforms on the school network and/or school devices, and the following have occurred:

- The creation of child sexual abuse material by and of children.
- The spread of AI generated hoaxes, misinformation and disinformation. Sometimes these can be so realistic that it is difficult to determine what is true or not. One notable example of this was the sharing of fake information across social media about serious threats of violence in and between schools, which led to children/parents being fearful and some not attending school.
- Children turning to Gen AI platforms for advice – some of which is harmful and extremely worrying, e.g. dieting, relationships, bullying, and advice about self-harm.
- Increased use of AI companions and chatbots which mimic human connection and have been seen to lead to AI induced psychosis, overuse, and heightened feelings of loneliness and shame. Tragically, there have also been numerous cases worldwide of children dying by suicide as a result of interactions with such bots.

There have also been numerous concerns related to staff use of Gen AI, including privacy and intellectual property breaches, and an increase in poor quality learning resources created using Gen AI.

Schools must address this, not just in the classroom, but by educating staff, governors, trustees, parents and pupils on safe use of digital technology, both for school and personal use. For guidance and resources, visit genai.lgfl.net.

Senso monitoring data has also revealed other concerns in schools:

- Children accessing inappropriate online games, dating sites and web chat where there is the risk of seeing adult and violent content and having interactions with strangers.
- The normalisation of violent and racist language between children, much of which doesn't suggest a particular ideology, but which could lead to extremism.

All these issues require a whole school approach to online safeguarding, as there is no quick or simple solution. It requires a combination of strong leadership, clear roles and responsibilities, robust policies and procedures, effective technical systems, highly competent staff who are regularly updated on this fast-paced world, effective and regular collaboration with parents, successful digital literacy and online safety teaching and more.

2. OFCOM'S LATEST RESEARCH

Ofcom's '[Children and Parents media use and attitudes report](#)' published in 2026 has shown the following:

Internet use is nearly universal, with 99% of 8-17-year-olds going online, and the vast majority of children are using digital technology by the time they start primary school. A critical transition occurs at age 11, where personal mobile phone ownership jumps from 56% to 83%. Schools must also address the rapid adoption of Generative AI, now used by 56% of 8-17-year-olds, primarily for schoolwork (51%). Despite high confidence, a 'digital literacy gap' exists: 31% of students could not identify a fake social media profile, and 46% believe AI search summaries are "always accurate".

Social pressures remain high, with 70% of students feeling pressure to be popular on social apps. Negative experiences are common; 23% of 8–17-year-olds personally experienced "nasty or hurtful" behaviour in the last

year, occurring most frequently on social media (47%) and in online games (38%). Vulnerable students, such as those with mental health conditions, are significantly more likely to feel their screen time is "too high" (56%).

Schools are the primary source of online safety information for 49% of parents. While 85% of students recall online safety lessons, only 23% remember being taught how to spot AI-generated content, and 21% recall lessons on identifying advertising. This suggests a need for updated curricular that reflect the evolving risks of AI and commercial influence.

3. IWF, CSAM CONCERNS

Data from the IWF in their 2025 [annual report](#) highlights the scale of child sexual abuse imagery online. In 2025, the IWF assessed 451,210 reports, confirming that 311,610 contained child sexual abuse material (CSAM).

Schools should be specifically alert to emerging and persistent harms identified by the IWF, which include:

- Sexually coerced extortion (sextortion): Targeted threats against students – teenage boys in particular.
- AI-generated abuse: The use of generative tools to create non-consensual sexual imagery.
- Violence against women and girls (VAWG): A growing trend in digital spaces around violent and misogynistic narratives and language.

4. "COM NETWORKS"

A further concern highlighted by the [National Crime Agency](#), is that of the existence of 'Com Networks'. These are networks of predominantly teenage boys, dedicated to inflicting harm and committing a range of criminality both on and offline, including cyber, fraud, extremism, serious violence, and child sexual abuse. The victims of these crimes are typically other children, some as young as 11, who have been coerced into seriously harming or sexually abusing themselves, siblings or pets. These networks are not hidden away in the dark web, but instead on platforms such as Discord, Telegram, Roblox, and Minecraft. Schools can help to protect children from these networks by enforcing effective filtering, training staff to recognise signs of exploitation, supporting parents to understand and mitigate the risks and building a curriculum that teaches students to identify grooming behaviours.

5. CYBER ATTACKS

[Data](#) from the Department for Science, Innovation and Technology (DSIT) states that 73% of secondary schools and 49% of primary schools identified a cyber breach or attack in the past 12 months (a significant jump from the previous year). Phishing remains the biggest entry point. AI is being used by scammers to generate sophisticated, error-free phishing emails targeting school administration and staff accounts. Schools are encouraged to ensure that they bridge the gap between technical understanding/cyber security policies, and operational understanding and practice.