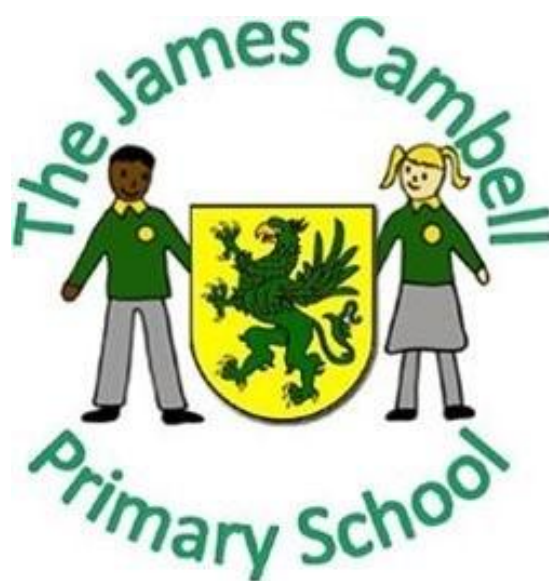


Online safety policy

James Cambell Primary School



Approved by:	Clara Breakwell	Date: October 2026
Last reviewed on:	October 2026	
Next review due by:	October 2027	

Contents

Contents	2
What's different about this policy for September 2026?	3
Introduction	5
Key people / dates	5
What is this policy?	5
Who is in charge of online safety?	6
What are the main online safety risks in 2026/2027?	6
How will this policy be communicated?	7
Overview	7
Aims	7
Further Help and Support	8
Scope	9
Roles and responsibilities	9
Education and curriculum	9
Handling online-safety concerns and incidents	10
Actions where there are concerns about a child	12
Sharing nudes and semi-nudes (including AI-generated images and deepfakes)	17
Upskirting	19
Bullying	19
Sexual violence and harassment	19
Misuse of school technology (devices, systems, networks or platforms)	19
Social media incidents	20
Data protection and data security	21
Cyber security	22
Appropriate filtering and monitoring	22
Generative artificial intelligence (AI)	24
Electronic communications	24
Email	24
School website	25
Cloud platforms	26

Digital images and video	26
Social media	27
The James Cambell Primary School's SM presence	27
Staff, pupils' and parents' SM presence	28
Device usage	29
Personal devices including mobile phones, wearable technology and bring your own device (BYOD)	29
Network / internet access on school devices	30
Searching and confiscation	30
Appendix 1 – Roles	32
All staff	33
Headteacher/Principal – Joe Wilson	34
Designated Safeguarding Lead / Online Safety Lead – Denise Parker-Skinner	35
Governing Body, led by Online Safety / Safeguarding Link Governor Key responsibilities (quotes are taken from Keeping Children Safe in Education)	37
PSHE / RSHE Lead/s – Hazel Thompson	38
Computing Lead – Rebecca Higginson	39
Subject / aspect leaders	39
Network Manager/technician – Joshua Collier (partnership learning IT)	39
Data Protection Officer (DPO) Michael Junnix (Partnership Learning trust)	40
Volunteers and contractors (including tutor)	41
Pupils	41
Parents/carers	42
External groups including parent associations	42

What's different about this policy for September 2026?

This policy has been fully reviewed for the 2026/27 academic year to reflect [Keeping Children Safe in Education 2026](#) (KCSIE 2026), which came into force on 1 September 2026 and replaces KCSIE 2025, together with other recent Department for Education (DfE) guidance. The main changes are:

- **Artificial intelligence (AI):** the 4 Cs of online risk have been updated, as in KCSIE 2026, to include harmful interactions with generative AI (such as AI chatbots and 'companion' apps) and AI-generated explicit images. A new section on generative AI reflects the DfE's [Generative AI in education](#) guidance and [Generative AI: product safety standards](#).
- **Filtering and monitoring:** the governing body must ensure that the effectiveness of filtering and monitoring is reviewed at least once every academic year by the SLT member responsible for filtering and monitoring, supported by the DSL and IT support, and that a record is kept of the

checks made. This reflects the updated DfE [Filtering and monitoring standards](#), which now include AI-generated content.

- **Nudes and semi-nudes:** updated terminology now covers self-generated, digitally altered and wholly AI-generated images, including 'deepfakes' and 'deep nudes', whether created or shared consensually or not.
- **Mobile phones:** the DfE [Mobile phones in schools](#) guidance became statutory in 2026. Schools should be mobile phone-free environments by default throughout the school day, and staff should not use their own phones for personal reasons in front of pupils.
- **Cyber security** is recognised as a safeguarding matter for the first time, with reference to the DfE [Cyber security standards for schools and colleges](#).
- **Training and reading:** all staff must now read Part one of KCSIE in full (the shorter version previously in Annex A has been removed), and all staff training includes the expectations, roles and responsibilities for filtering and monitoring.
- **Curriculum:** the revised statutory [RSHE guidance](#) is compulsory from September 2026 and includes new content on online safety, online financial harms and critically evaluating what pupils see online.
- **Terminology and references:** updated language (for example 'child-on-child abuse' and 'Family Help'), trainee teachers are now included alongside other staff, and out-of-date references (for example COVID-19 lockdowns and the National Tutoring Programme) have been removed.

Introduction

Key people / dates

	Designated Safeguarding Lead (DSL) team	Alan Jacob
	Deputy Designated Safeguarding Leads	Clara Breakwell, Amanda Waterlow, Charlotte Redmond and Lisa Marshal
	Online-safety lead (if different)	Alan Jacob
	Link governor for safeguarding (includes online safety)	Stephen Noon
	PSHE/RSHE/RSE lead	Shaun Murray
	Network manager / other technical support	Stuart Aiken
	Senior leadership team (SLT) lead for filtering and monitoring	Alan Jacob
	Data Protection Officer (DPO)	Michael Junnix (Partnership Learning Trust)
	Date this policy was reviewed and by whom	October 2026 – Alan Jacob
	Date of next review and by whom	October 2027 (or sooner if statutory guidance changes) – Alan Jacob

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' 2026 (KCSIE), 'Working Together to Safeguard Children' 2023, 'Teaching Online Safety in Schools' (updated 2023), the statutory RSHE guidance (2025, compulsory from September 2026), the statutory 'Mobile phones in schools' guidance (2026), the DfE Filtering and monitoring and Cyber security standards for schools and colleges, the Online Safety Act 2023 and other statutory documents. It is cross-curricular (with relevance beyond Relationships, Health and Sex Education, Citizenship and Computing) and designed to sit alongside the school's statutory Safeguarding Policy. Any issues and concerns with online safety **must** always follow the school's safeguarding and child protection procedures.

Who is in charge of online safety?

KCSIE makes clear that “the designated safeguarding lead should take **lead** responsibility for safeguarding and child protection (including online safety and understanding the filtering and monitoring systems and processes in place).” The DSL can delegate activities but not the responsibility for this area and whilst subject leads, e.g. for RSHE will plan the curriculum for their area, it is important that this ties into a whole-school approach. At The James Cambell Primary School, a named member of the senior leadership team is responsible for filtering and monitoring, working closely with the DSL and our IT support (see Key people / dates above).

What are the main online safety risks in 2026/2027?

KCSIE 2026 categorises online-safety risks as the 4 Cs: **Content, Contact, Conduct and Commerce**, and has updated these to reflect artificial intelligence. **Content** includes exposure to illegal, inappropriate or harmful material, for example pornography, racism, misogyny, self-harm, suicide, radicalisation and extremism, misinformation, disinformation and conspiracy theories. **Contact** includes harmful online interaction with other users or with generative AI applications that simulate human interaction, such as AI chatbots and ‘companion’ apps. **Conduct** includes online behaviour that increases the likelihood of, or causes, harm, for example making, sending and receiving explicit images (including images generated using AI) and online bullying. **Commerce** includes online gambling, inappropriate advertising, phishing and financial scams. These areas provide a helpful approach to understanding the risks and the potential school response, whether technological or educational. They do not stand in isolation, and it is important to understand the interplay between all four.

Ofcom’s [Children and Parents: Media Use and Attitudes](#) research (May 2026) shows how quickly this picture is changing for primary-aged children. Smartphone ownership rises from 56% of 10-year-olds to 83% of 11-year-olds; more than half (56%) of 8–17-year-olds now use AI tools, and one in ten (11%) say they have used AI ‘as someone to talk to’ or ‘as a friend’. Over seven in ten children play games online, and nearly three-quarters of 11–17-year-olds said they had seen harmful content online, most often while scrolling their feed.

KCSIE 2026 continues to highlight extra-familial harms, where children are at risk of abuse or exploitation in situations outside their families, including sexual and criminal exploitation, serious youth violence and radicalisation, all of which can begin or be facilitated online. It strengthens guidance on misogyny and its links to harmful sexual behaviour, and names ‘deepfakes’ explicitly for the first time.

Analysis from the Centre of Expertise on Child Sexual Abuse also highlights the prevalence of child sexual abuse, with an estimated 500,000 children experiencing child sexual abuse every year. The Internet Watch Foundation’s [2025 Annual Data and Insights Report](#) confirmed 311,610 reports of child sexual abuse material, including 3,443 AI-generated child sexual abuse videos (a 260-fold increase on the previous year); 77% of the children in the imagery were girls. Reports of sextortion, where children are blackmailed using sexual images, rose by 127%, with the great majority of victims being boys. Grooming and image-based abuse can begin in the primary years, which makes the transition years crucial in the

fight against sexual exploitation, in primary and secondary. See cse.lgfl.net for resources to support DSLs, RSHE/PSHE leads and parents, including the [Undressed](#) campaign.

Part five of KCSIE 2026 sets out how schools should respond to **child-on-child sexual violence and sexual harassment**, much of which has an online element, for example the non-consensual sharing of images (including deepfakes) and abuse in group chats or online games. KCSIE 2026 recognises that some forms of child-on-child abuse disproportionately affect girls, while being clear that all abuse is unacceptable. We ensure appropriate processes are in place to allow pupils to report concerns freely, knowing these will be taken seriously and dealt with swiftly and appropriately, through the school's internal reporting channels. Pupils are also made aware of Childline (0800 1111) and the Childline and IWF [Report Remove](#) tool, and adults can contact the NSPCC Helpline (0808 800 5000).

Generative AI is a fast-growing area of both opportunity and risk. Children may meet AI-generated content that is inaccurate, inappropriate or harmful, form relationships with AI 'companion' chatbots, or be targeted with AI-generated sexual imagery created with 'nudification' apps. In its response to the [Growing up in the online world](#) consultation (2026), the government committed to banning social media services for under-16s and to stopping AI chatbots offering sexualised content to under-18s; the school will update its practice and advice to parents as these measures come into force. The quick survey at safeposters.lgfl.net may help to surface some of these issues. Teachers may also find LGfL's SafeSkills Online Safety Quiz and diagnostic teaching tool at safeskillsinfo.lgfl.net particularly useful to capture and assess pupil resilience and competence for digital life.

How will this policy be communicated?

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

- Posted on the school website
- Integral to safeguarding updates and training for all staff, including trainee teachers (especially in September refreshers), with training covering the expectations, roles and responsibilities for filtering and monitoring
- Clearly reflected in the Acceptable Use Policies (AUPs) for staff, volunteers, contractors, governors, pupils and parents/carers (which must be in accessible language appropriate to these groups), which will be issued to whole school community, on entry to the school, annually and whenever changed, plus displayed in school
- Available in paper format where requested
- Reviews of this online-safety policy will include input from staff, pupils and other stakeholders, helping to ensure further engagement

Overview

Aims

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

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

Further Help and Support

Internal school channels should always be followed first for reporting and support, as documented in school policy documents, especially in response to incidents, which should be reported in line with the Safeguarding Policy. The DSL will handle referrals to local authority children's social care (including the multi-agency safeguarding hub, MASH) and normally the headteacher will handle referrals to the LA designated officer (LADO). The local authority, Partnership Learning Trust or third-party support organisations the school works with may also have advisors to offer general support.

Beyond this, reporting.lgfl.net has a list of curated links to external support and helplines for both pupils and staff, including the [Professionals' Online Safety Helpline](#) from the UK Safer Internet Centre, the NSPCC Helpline (0808 800 5000), NCA CEOP for reporting online sexual abuse and grooming, the Childline and IWF Report Remove tool, as well as hotlines for hate crime, terrorism and fraud which might be useful to share with parents, and anonymous support for children and young people.

Scope

This policy applies to all members of The James Cambell Primary School community (including teaching and support staff, trainee teachers, supply teachers and tutors, governors, 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.

Roles and responsibilities

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

Depending on their role, all members of the school community should **read the relevant section in Appendix 1 of this document** that describes individual roles and responsibilities. Please note there is one for All Staff which must be read even by those who have a named role in another section. There are also pupil, governor, etc role descriptions in the annex.

Education and curriculum

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

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

The revised statutory [RSHE guidance](#) (published July 2025 and compulsory from September 2026) strengthens online safety content in primary Relationships and Health Education. This includes helping pupils to critically engage with what they see online, to understand their rights in relation to privacy, consent and personal data, to understand age restrictions on platforms such as social media and gambling, and to recognise online financial harms such as in-game spending, scams and fraud.

RSHE guidance also recommends schools assess teaching to “identify where pupils need extra support or intervention [through] tests, written assignments or self evaluations, to capture progress.” [See LGfL’s

SafeSkills Online Safety Quiz and diagnostic teaching tool which is linked to statements from UKCIS Education for a Connected World framework, enabling teachers to monitor progress throughout the year and drill down to school, class and pupil level to identify areas for development at safeskillsinfo.lgfl.net]

The following subjects have the clearest online safety links (see the relevant role descriptors above for more information):

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

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

Whenever overseeing the use of technology (devices, the internet, new technology such as generative AI and augmented reality, etc) in school or setting as homework tasks, all staff should encourage sensible use, monitor what pupils are doing and consider potential dangers and the age appropriateness of websites and tools (ask the DSL what appropriate filtering and monitoring systems are in place). KCSIE 2026 reminds schools that parents and carers are likely to find it helpful to understand what systems schools use to filter and monitor online use, and that it is especially important for parents and carers to be aware of what their children are being asked to do online, including the sites they will be asked to access, and to be clear who from the school (if anyone) their child is going to be interacting with online.

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

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

Annual reviews of curriculum plans / schemes of work (including for SEND pupils) are used as an opportunity to follow this framework more closely in its key areas of Self-image and Identity, Online relationships, Online reputation, Online bullying, Managing online information, Health, Wellbeing and lifestyle, Privacy and security, and Copyright and ownership.

Handling online-safety concerns and incidents

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

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

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

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

- Safeguarding and Child Protection Policy
- Child-on-child abuse (including sexual violence and sexual harassment) procedures, within the Safeguarding and Child Protection Policy
- Anti-Bullying Policy
- Behaviour Policy (including school sanctions, child-on-child abuse and searching, screening and confiscation)
- Acceptable Use Policies
- Mobile Phone Policy (in line with the statutory 'Mobile phones in schools' guidance)
- Data Protection Policy, agreements and other documentation (e.g. privacy statement and consent forms for data sharing, image use etc)

- Whistle-blowing Policy for Schools including managing allegations
- Remote learning policy
- Equality Policy
- Health & Safety Policy
- RSHE Policy
- Staff Code of Conduct
- Communication Policy
- Cyber security and IT security procedures (Partnership Learning IT)

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

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

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

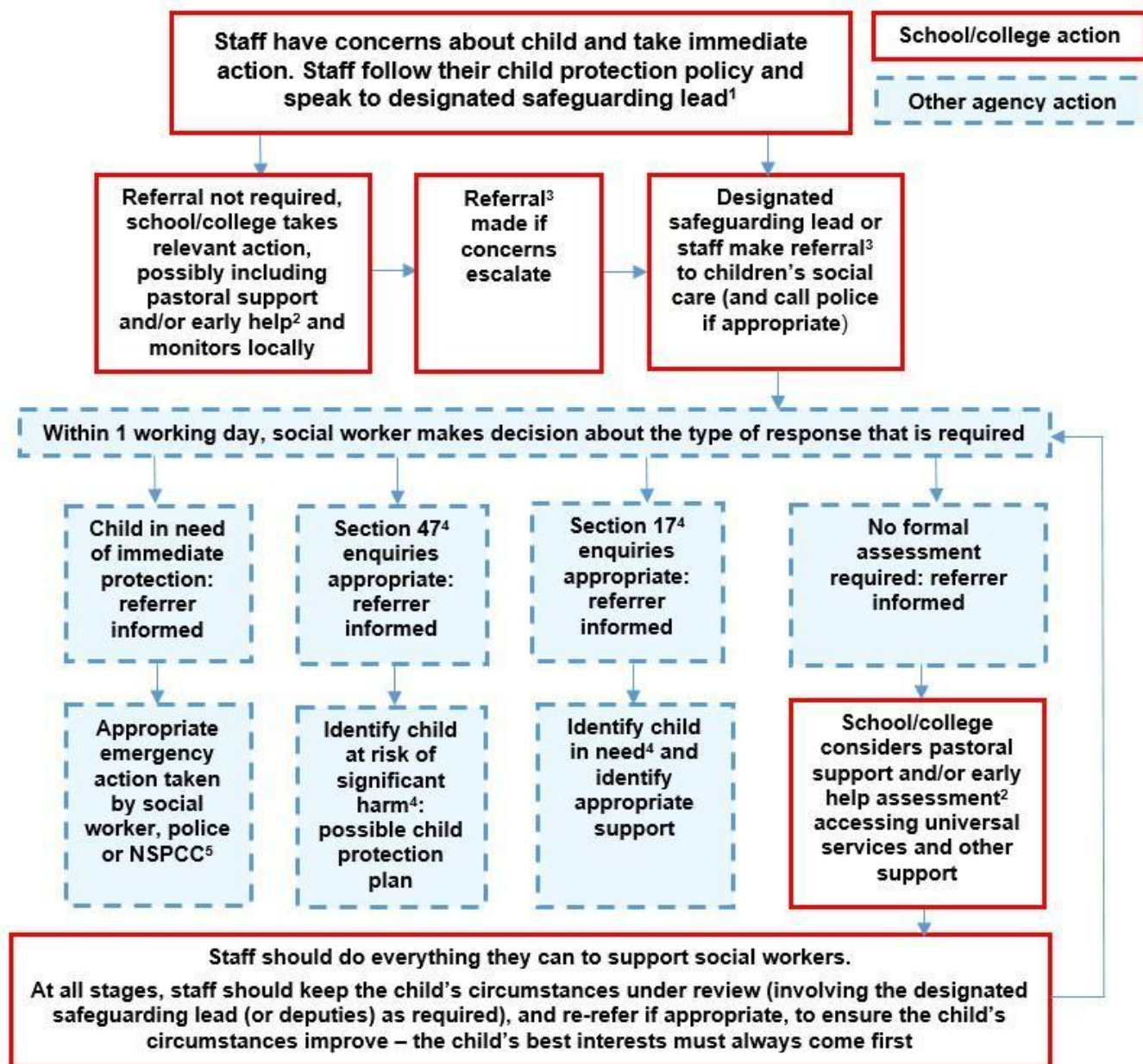
The school will actively seek support from other agencies as needed (i.e. the local authority, Partnership Learning Trust, LGfL, UK Safer Internet Centre's Professionals' Online Safety Helpline (POSH), NCA CEOP, Prevent Officer, Police, IWF and the Harmful Sexual Behaviour Support Service). The DfE guidance [Behaviour in schools: advice for headteachers and school staff](#) (February 2024) provides advice and related legal duties including support for pupils and powers of staff when responding to incidents, including child-on-child sexual violence and sexual harassment, behaviour incidents online and mobile phones.

We will inform parents/carers of online-safety incidents involving their children (unless to do so would put a child at risk of harm), and the Police where staff or pupils engage in or are subject to behaviour which we consider is particularly disturbing or breaks the law (particular procedures are in place for sharing nudes and semi-nudes and upskirting; see sections below).

The school will make sure that reporting procedures continue to work if pupils are learning remotely or the school site is closed for any reason, and will make alternative provisions in advance where these might be needed.

Actions where there are concerns about a child

The following flow chart (it cannot be edited) shows the actions to take where there are concerns about a child, as set out in Keeping Children Safe in Education, the key education safeguarding document (see Flowchart 1, page 27, of [KCSIE 2026](#) for the current version). As outlined previously, online safety concerns are no different to any other safeguarding concern.



At The James Cambell Primary School, recognising abuse and taking action Staff, volunteers and governors must follow the procedures set out below in the event of a safeguarding issue.

Overview of procedures.

One of our main responsibilities under our duty of care, 'Working Together to Safeguard Children' (2023) and 'Keeping Children Safe in Education' (2026) is child protection.

Actions to be taken if a child is thought to be 'at risk'

- The rule 'believe first' is to be rigidly applied, particularly in cases of suspected child abuse.
- Anything you see or hear must be reported immediately.
- Any disclosure by a child must be reported immediately.
- You must never interrogate the child, as this may prejudice any action that might be subsequently taken but questioning a child by a teacher/ support staff would be expected.

- Any concerns must be reported to the Designated Safeguarding Lead, Denise Parker-Skinner. If the Lead is not available then to the Deputy Designated Safeguarding Leads – Joe Wilson or Rebecca Seaton.
- On the rare occasion that none of the above are available then contact Assistant head teacher for advice.
- If none of the above can be contacted then contact Children's Services direct. Their number is located on the Inclusion Managers wall or on the Safeguarding board in the staffroom.
- **Never leave a child protection concern to the following day.**
- When a concern is passed to the designated lead or deputy lead then:
 - a) They will ensure information is gathered.
 - b) Liaise with appropriate staff
 - c) Make a decision as to whether to refer to Children's Services, to offer Family Help (previously known as early help) or to monitor the situation.
 - d) Inform appropriate staff of the decision made.
- If a decision is made to refer the concern to Children's Services then the Lead will follow the procedure:
 - a) Referrals to Social Care will always be made by either the **designated lead or the deputy designated leads.**
 - b) Referrals should be made initially by telephoning the duty Referrals Social Worker, this should then be followed up in writing on a "Multi-Agency Referral Form" (MARF) which should be emailed to Children's Services within 24 hours. Children's Services expect it within 48 hours at the latest.
 - c) If perceived risk is more urgent the duty social worker will advise to email immediately
 - d) Where practicable, **if there is no immediate risk to the child** concerns should be discussed with the parent / carer and agreement sought for a referral to be made, **unless seeking agreement is likely to place the child at risk of significant harm through delay or the parents' actions or reactions.**
 - e) Where a professional decides not to seek parental permission before making a referral, the decision must be recorded in the child's file with reasons, dated and signed and confirmed in the referral to Social Care.
- In circumstances where a child has an unexplained or suspicious injury that requires urgent medical attention, the Safeguarding referral process should not delay the administration of First Aid or emergency medical assistance. If a pupil is thought to be at immediate risk because of parental violence, intoxication, substance abuse, mental illness or threats to remove the child during the school day, urgent Police intervention will be requested.

Responsibilities and action in a suspected case of abuse or neglect

Suspicion of Abuse (In the event of noticing a mark or bruise, or perhaps a child who has been behaving differently, when abuse is suspected but there has been no disclosure.)

1. It would be appropriate to ask open questions about the nature of the concern, e.g. bruises, marks, change in behaviour etc. "How did that happen? I've noticed that...Can you tell me about..."
2. Believe the child and reassure them that they were right to talk to you. Explain that you will be passing on the concern.
3. Record the facts and conversation in writing on a "Child Protection Concern" form (available from the shared staff area under proformas, staffroom or at the back of the safeguarding policy) at the earliest opportunity afterwards using the exact words spoken not implied. Please ensure you sign and date the form.
4. Report the suspicion to the Designated Person responsible for Child Protection, the Deputy designated person or the Head teacher. The Designated Person, Deputy designated person or Head teacher will take the appropriate action.

Disclosure (When a child discloses abuse or neglect.)

1. Allow the child to talk – ask only open questions to clarify concerns e.g. "Can you tell me more about...." Do not press for detail, put forward your own ideas or use words that the child has not used themselves.
2. Stay calm and reassuring. E.g." Well done, you're doing well... You've done nothing wrong".
3. Do not make promises that cannot be kept e.g. confidentiality – tell the child that you will have to tell someone else who will be able to help.
4. Believe the child but do not apportion any blame to the perpetrator. (It may be someone they love)
5. Reassure the child that they were not to blame and they were right to talk to you. Explain that you will be passing on the concern.
6. Ask the child if they have told anyone else.
7. Keep an open mind.
8. Record the conversation and facts verbatim immediately afterwards on Safeguard
9. Report to the Designated Person or Deputy Designated Person or as soon as possible.
10. If a case is urgent then verbally report first.
11. If access to Safeguard is not possible at the time then record on paper using the 'Incident Record/ Cause for Concern form'

Child Sexual Exploitation

We are vigilant about risks of child sexual exploitation and refer to the recent guidance;

[Child sexual exploitation: definition and guide for practitioners](#) (DfE) and Keeping Children Safe in Education 2026.

We are aware of the key indicators of children being sexually exploited which can include:

- going missing for periods of time or regularly coming home late;
- regularly missing school or education or not taking part in education;
- appearing with unexplained gifts or new possessions;
- associating with other young people involved in exploitation;
- having older boyfriends or girlfriends;
- suffering from sexually transmitted infections;
- mood swings or changes in emotional wellbeing;
- drug and alcohol misuse; and
- displaying inappropriate sexualised behaviour;
- being secretive about their online activity, having more than one phone or social media account, or receiving gifts, money or gaming credit from people they have met online;

Practitioners should also be aware that many children and young people who are victims of sexual exploitation do not recognise themselves as such. In any such case, concerns will be discussed with one of the CP Leads.

Female Genital Mutilation

We are also vigilant about the risk and potential likelihood of female genital mutilation (FGM). We refer to the [Multi-agency statutory guidance on female genital mutilation](#):

SPECIFIC FACTORS THAT MAY HEIGHTEN A GIRL'S OR WOMAN'S RISK OF BEING AFFECTED BY FGM

There are a number of factors in addition to a girl's or woman's community or country of origin that could increase the risk that she will be subjected to FGM:

- The position of the family and the level of integration within UK society – it is believed that communities less integrated into British society are more likely to carry out FGM.
- Any girl born to a woman who has been subjected to FGM must be considered to be at risk of FGM, as must other female children in the extended family.
- Any girl who has a sister who has already undergone FGM must be considered to be at risk of FGM, as must other female children in the extended family.
- Any girl withdrawn from Personal, Social and Health Education or Sex and Relationship Education may be at risk as a result of her parents wishing to keep her uninformed about her body and rights.

INDICATIONS THAT FGM MAY BE ABOUT TO TAKE PLACE SOON

The age at which girls undergo FGM varies enormously according to the community. **The procedure may be carried out when the girl is new-born, during childhood or adolescence, at marriage or during the first pregnancy.**

FGM happens to British girls in the UK as well as overseas.

INDICATIONS THAT FGM MAY HAVE ALREADY TAKEN PLACE:

It is important that professionals look out for signs that FGM has taken place so that:

- The girl or woman affected can be supported to deal with the consequences of FGM.
- Enquiries can be made about other female family members who may need to be safeguarded from harm.
- Criminal investigations into the perpetrators, including those who carry out the procedure, can be considered to prosecute those breaking the law and to protect others from harm.

There are a number of indications that a girl or woman has been subjected to FGM:

- A girl may have difficulty walking, sitting or standing and may even look uncomfortable.
- A girl may spend longer than normal in the bathroom or toilet due to difficulties urinating. A girl may spend long periods of time away from a classroom during the day with bladder or menstrual problems.
- A girl may have frequent urinary, menstrual or stomach problems.
- There may be prolonged or repeated absences from school or college.
- A prolonged absence from school or college with noticeable behaviour changes (e.g. withdrawal or depression) on the girl's return could be an indication that a girl has recently undergone FGM.
- A girl may be particularly reluctant to undergo normal medical examinations.
- A girl may confide in a professional.
- A girl may ask for help, but may not be explicit about the problem due to embarrassment or fear.
- A girl may talk about pain or discomfort between her legs.

Any concerns about pupils at risk of experiencing, or already having experienced FGM, should be reported to one of the CP Leads. Teachers also have a statutory duty to report to the police where they discover (either through disclosure by the victim or visual evidence) that FGM appears to have been carried out on a girl under 18; this must be done personally, as well as informing the DSL.

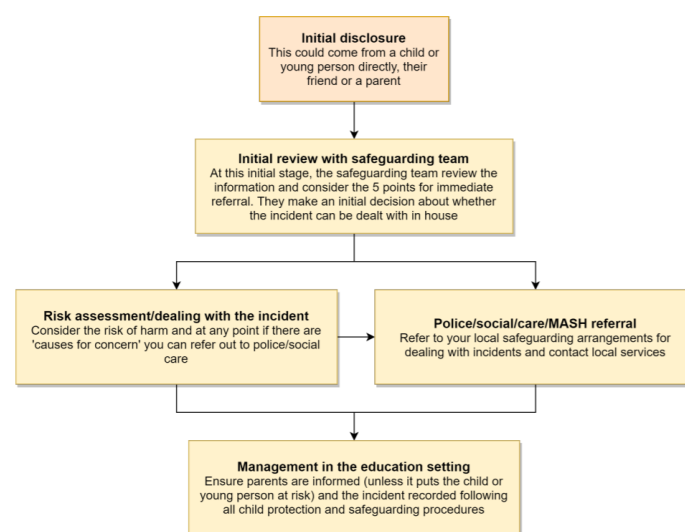
Sharing nudes and semi-nudes (including AI-generated images and deepfakes)

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 working with children and young people](#) (updated March 2024) to avoid unnecessary criminalisation of children. KCSIE 2026 makes clear that this

includes images that are self-generated, created by others, digitally altered or wholly generated using artificial intelligence (sometimes described as 'deepfakes' or 'deep nudes'), whether they are created or shared consensually or non-consensually, and that every such incident requires a safeguarding response. NB – where one of the parties is over 18, this is no longer 'sharing nudes' but child sexual abuse.

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

The school DSL will in turn use the full guidance document, [Sharing nudes and semi-nudes: advice for education settings](#), to decide next steps and whether other agencies need to be involved.



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

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

It is important that everyone understands that making, possessing or sharing a nude or semi-nude image of anyone under 18 is illegal, including where the image has been digitally altered or generated using AI, and that creating sexually explicit deepfakes and supplying 'nudification' tools are also criminal offences (Data (Use and Access) Act 2025; Crime and Policing Act 2026). However, pupils can come and talk to members of staff if they have made a mistake or had a problem in this area, and they will be supported. Children and young people can use the Childline and IWF [Report Remove](#) tool to help get nude images of themselves removed from the internet.

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

Upskirting

It is important that everyone understands that upskirting (taking a photo or video under a person's clothing, not necessarily a skirt, without their permission) is a criminal offence under the Voyeurism (Offences) Act 2019 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.

Bullying

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

Online bullying can include abuse in group chats and online games, and the creation or sharing of fake or AI-generated images, videos or audio of another pupil or member of staff; all such incidents will be taken seriously. Staff should also refer to the DfE advice [Preventing and tackling bullying](#).

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

Sexual violence and harassment

DfE guidance on sexual violence and sexual harassment between children is set out in Part five of [Keeping Children Safe in Education 2026](#). It would be useful for all staff to be aware of this guidance: Part five covers the immediate response to a report, providing reassurance and confidentiality which is highly relevant for all staff. KCSIE 2026 strengthens guidance on misogyny and its links to harmful sexual behaviour, and recognises that the non-consensual sharing of intimate images, including deepfakes, is a form of child-on-child abuse.

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

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

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

These are defined in the relevant Acceptable Use Policy as well as in this document, for example in the sections relating to the professional and personal use of school platforms/networks/clouds, devices and

other technology, as well as to the Mobile Phone Policy, BYOD (bring your own device) and the use of generative AI.

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

It will be necessary to reinforce these as usual at the beginning of any school year but also to remind pupils that **the same applies for any home or remote learning**, and for any school-approved AI tools.

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

Social media incidents

See the social media section later in this document for rules and expectations of behaviour for children and adults in The James Cambell Primary School community. These are also governed by school Acceptable Use Policies.

Breaches will be dealt with in line with the school behaviour policy (for pupils) or code of conduct/handbook (for staff).

Further to this, where an incident relates to an inappropriate, upsetting, violent or abusive social media post by a member of the school community, The James Cambell Primary School will request that the post be deleted and will expect this to be actioned promptly.

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

Data protection and data security

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

There are references to the relationship between data protection and safeguarding in key Department for Education documents [Keeping Children Safe in Education](#), [Data protection in schools](#) and [Information sharing advice for safeguarding practitioners](#) (2024), which the DPO and DSL will seek to apply. KCSIE makes the following point, which is useful for all staff:

“The Data Protection Act 2018 and UK GDPR do 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 includes ‘safeguarding of children and individuals at risk’ as a condition that allows practitioners to share special category personal data, even without consent**, and the Data (Use and Access) Act 2025 recognises safeguarding vulnerable individuals as a legitimate interest for processing personal data. When Designated Safeguarding Leads in schools are considering whether, or not, to share safeguarding information (especially with other agencies) 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 pupils, staff, governors, volunteers, contractors and parents are bound by the school’s data protection policy and agreements, which can be found here- [Data Protection Policy](#).

Rigorous controls on the network, Trust IT sign-on for technical services, firewalls and filtering all support data protection.

The headteacher, data protection officer and Partnership Learning Trust work together to ensure a UK 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. This includes;

- CCTV
- Use of personal vs school devices
- Password policy / multi-factor authentication
- Reminders to lock devices when leaving unattended
- Device encryption
- Access to and access audit logs for school systems
- Security processes and policies
- Wireless access
- File sharing
- Cloud platform use, access and sharing protocols

- Use of generative AI tools (no personal or sensitive data may be entered into AI tools that have not been approved by the school and the DPO)

Cyber security

KCSIE 2026 recognises cyber security as part of safeguarding: the governing body should take measures to safeguard children by protecting personal information and ensuring the school has appropriate cyber security systems in place. Cyber attacks, such as ransomware and phishing, can disrupt education, expose sensitive safeguarding information and put children at risk.

The school, working with Partnership Learning IT, follows the DfE [Cyber security standards for schools and colleges](#). In particular:

- a cyber risk assessment is carried out annually and reviewed each term
- staff (and governors with access to school systems) receive regular cyber awareness training, including how to spot and report phishing
- devices and networks are protected by anti-malware and firewalls, and software is licensed and kept up to date
- user accounts and access privileges are controlled, with multi-factor authentication for any account that can access personal or sensitive data
- data is backed up in line with a backup plan that is reviewed every year
- any suspected cyber incident or data breach is reported immediately to the Headteacher, Partnership Learning IT and the DPO, and serious incidents are reported to Action Fraud, the DfE and (where personal data is affected) the Information Commissioner's Office

Appropriate filtering and monitoring

Keeping Children Safe in Education 2026 requires the governing body to ensure that the school has appropriate filtering and monitoring systems in place, and that a review of their effectiveness is carried out **at least once every academic year**. Children should not be able to access harmful or inappropriate material from the school's IT system, but at the same time the school must be careful that "over blocking" does not lead to unreasonable restrictions as to what children can be taught with regards to online teaching and safeguarding.

The school meets the DfE [Filtering and monitoring standards for schools and colleges](#), which require schools to:

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

Roles. The SLT lead for filtering and monitoring (see Key people / dates) is responsible for ensuring these standards are met. The DSL takes lead responsibility for understanding the filtering and monitoring

systems and processes in place and for acting on safeguarding concerns that they reveal. Partnership Learning IT and our network manager provide the technical service, implement agreed changes and carry out checks, but the strategic decisions about what is allowed and blocked, and why, are made by school leaders. The link governor for safeguarding oversees this on behalf of the governing body and discusses the standards with IT staff and service providers.

Annual review. At least once every academic year (and whenever there is a significant change, such as new devices, new technology including AI tools, or a safeguarding concern), the SLT lead, supported by the DSL and IT support, reviews the effectiveness of filtering and monitoring. The review considers the risks to our pupils, what has been blocked or flagged and why, how generative AI tools are used in school, and any technical limitations of current systems. Checks are made that filtering is working on all internet-connected devices in all relevant locations and **a record is kept of when checks took place, which users and locations were tested, any issues identified and the action taken.** The outcome is reported to the governing body.

At this school, the internet connection is provided by LGFL and the MAT provider (Partnership Learning IT). This means we have a dedicated and secure, schoolsafe connection that is protected with firewalls and multiple layers of security, including web filtering that is designed to meet the UK Safer Internet Centre's [appropriate filtering and monitoring](#) definitions. Because generative AI tools can produce real-time, personalised content, the school considers, before introducing any AI tool, whether its filtering and monitoring can identify harmful AI-generated content and interactions.

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

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

At The James Cambell Primary School, our monitoring strategy currently combines options 1,2 and 3: pupils use the internet under adult supervision at all times, and internet and web access logs are reviewed, with alerts shared with the DSL. Whether active/pro-active technology monitoring (option 3) is needed is considered at each annual review, taking into account our risk assessment and any new technology in use. All staff are trained to understand the filtering and monitoring expectations and their role in them, and must report to the DSL straight away if they witness or suspect that a pupil has accessed or tried to access harmful content, if they become aware of a failure in the filtering system or abuse of the system, or if they feel that filtering is unreasonably restricting teaching and learning.

Where staff are concerned that children are developing extremist views or showing signs of becoming radicalised, including through online content, they should discuss this with the Designated Safeguarding Lead in line with the Prevent duty. We use the curriculum to ensure that children understand how people with extreme views share these with others, especially using the internet.

We are committed to ensuring that our pupils are offered a broad and balanced curriculum that aims to prepare them for life in modern Britain. Teaching the school's core values alongside the fundamental

British Values, supports quality teaching and learning, whilst making a positive contribution to the development of a fair, just and civil society.

Generative artificial intelligence (AI)

Generative AI tools, such as chatbots and image generators, can support teaching, learning and workload, but they also create new safeguarding, data protection and intellectual property risks. The school follows the DfE guidance [Generative artificial intelligence \(AI\) in education](#) and [Generative AI: product safety standards](#), and KCSIE 2026 expects filtering and monitoring arrangements to take account of AI tools. The following principles apply:

- Only AI tools that have been approved by the Headteacher and the DPO (with a data protection impact assessment where needed) may be used for school purposes. Before approval, leaders check that the tool meets the DfE product safety standards, including filtering, monitoring and reporting, and that it is appropriate for the age of the users
- Pupils only use AI tools that are designed and approved for education, as part of planned learning under adult supervision, and in line with each tool's age restrictions. Pupils do not use consumer AI chatbots or 'companion' apps in school
- Staff must not enter personal data about pupils, staff or families, or any safeguarding information, into AI tools that have not been approved for that purpose
- Staff remain professionally responsible for anything they produce with the help of AI and must check it for accuracy, bias and appropriateness before use
- Images, video or audio of pupils, staff or other members of the school community must never be uploaded to, altered or generated using AI tools, except where approved by the Headteacher for a specific, safe purpose
- Pupils are taught, in an age-appropriate way, that AI can be wrong or biased, that AI chatbots are not people or friends, and that images, video and audio can be faked; they know to tell a trusted adult if anything they see or are asked to do online, including by an AI tool, worries them
- Any concern about the misuse of AI, including the creation of fake or sexual images of a child, is a safeguarding concern and must be reported to the DSL immediately

Electronic communications

Please read this section alongside references to pupil-staff communications in the overall school Safeguarding Policy, and in conjunction with the Data Protection Policy. This section only covers electronic communications, but the same principles of transparency, appropriate conduct and audit trail apply.

Email

- Staff at this school use the Outlook mail system for all school emails

The System is linked to the USO authentication system and are fully auditable, trackable and managed by IT on behalf of the school. This is for the mutual protection and privacy of all staff, pupils and parents, as well as to support data protection.

General principles for email use are as follows:

- Email, ParentMail and Class Dojo are the only means of electronic communication to be used between staff and parents. Use of a different platform must be approved in advance by the data-protection officer / headteacher. 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 Headteacher (if by a staff member).
- Email may only be sent using the email systems above. There should be no circumstances where a private email is used; if this happens by mistake, the DSL/Headteacher/DPO (the particular circumstances of the incident will determine whose remit this is) should be informed immediately.
- Staff or pupil personal data should never be sent/shared/stored in unencrypted email.
 - If data needs to be shared with external agencies, this will be via egress or CPOMs.
 - Internally, staff should use the school network, including when working from home when remote access is available.
- 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
- Pupils and staff are NOT allowed to use the email system for personal use and should be aware that all use is monitored, their emails may be read and the same rules of appropriate behaviour apply at all times. Emails using inappropriate language, images, malware or to adult sites may be blocked and not arrive at their intended destination.

See also the social media section of this policy.

School website

The school website is a key public-facing information portal for the school community (both existing and prospective stakeholders) with a key reputational value. The Headteacher and Governors have delegated the day-to-day responsibility of updating the content of the website to Miss Breakwell. The site is managed by / hosted by Partnership Learning IT services. The website must meet the DfE requirements for the information that schools must publish online.

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

- Schools have the same duty as any person or organisation to respect and uphold copyright law – schools have been fined thousands of pounds for copyright breaches. Sources must always be credited and material only used with permission. If in doubt, check with the headteacher or business manager. There are many open-access libraries of high-quality public-domain images that can be used (e.g. pixabay.com for marketing materials – beware some adult content on this

site). Pupils and staff at Partnership learning schools also have access to licences for music, sound effects, art collection images and others.

- Images of pupils are only published in line with parental consent (see Digital images and video), and AI-generated or AI-altered images must never be used to depict real pupils or staff

Cloud platforms

It is important to consider data protection before adopting a cloud platform or service – see our DP policy here- [Data Protection Policy](#).

For online safety, basic rules of good password hygiene (“Treat your password like your toothbrush – never share it with anyone!”), multi-factor authentication, expert administration and training can help to keep staff and pupils safe, and to avoid incidents. The data protection officer, Michael Junnix, and the network manager, Peter Maynard, 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 (including AI tools), what may or may not be stored in them and by whom. This is noted in a DPIA (data protection impact assessment) and parental permission is sought where required
- Regular training ensures all staff understand sharing functionality and this is audited to ensure that pupil data is not shared by mistake. Open access or widely shared folders are clearly marked as such
- Pupils 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
- Multi-factor authentication is used for access to staff or pupil data on CPOMs by authorised personnel only
- Pupil images/videos are only made public with parental permission
- Only school-approved platforms are used by students or staff to store pupil work
- All stakeholders understand the difference between consumer and education products (e.g. a private Gmail account or Google Drive and those belonging to a managed educational domain)

Digital images and video

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

- For the newsletter
- For displays around the school
- For online prospectus or websites
- For publication

- For school events
- For use in paper-based school marketing

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

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

All staff are governed by their contract of employment and the school's Acceptable Use Policy, which covers the use of mobile phones/personal equipment for taking pictures of pupils, and where these are stored. At The James Cambell Primary School, members of staff may never use personal phones or other personal devices to capture photos or videos of pupils, and images of pupils must never be uploaded to AI tools.

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

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

Pupils are taught about how images, video and audio can be manipulated or created using AI (including 'deepfakes') in their online safety education programme and also taught to consider how to publish for a wide range of audiences which might include governors, parents or younger children.

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

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

Social media

The James Cambell Primary School's SM presence

The James Cambell Primary School works on the principle that if we don't manage our social media reputation, someone else will.

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

Negative coverage almost always causes some level of disruption. Up to half of all cases dealt with by the Professionals Online Safety Helpline (POSH: helpline@saferinternet.org.uk) involve schools' (and staff members') online reputation.

Accordingly, we manage and monitor our social media footprint carefully to know what is being said about the school and to respond to criticism and praise in a fair, responsible manner, even if there are no official/active school social media accounts.

Staff, pupils' and parents' SM presence

Social media (including here all apps, sites and games that allow sharing and interaction between users) is a fact of modern life, and as a school, we accept that many parents, staff and pupils will use it. However, as stated in the acceptable use policies which all members of the school community sign, we expect everybody to behave in a positive manner, engaging respectfully with the school and each other on social media, in the same way as they would face to face.

This positive behaviour can be summarised as not making any posts which are or could be construed as bullying, aggressive, rude, insulting, illegal or otherwise inappropriate, or which might bring the school or (particularly for staff) teaching profession into disrepute. This applies both to public pages and to private posts, e.g. parent chats, pages or groups.

If parents have a concern about the school, we would urge them to contact us directly and in private to resolve the matter. If an issue cannot be resolved in this way, the school [complaints 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).

Most social media and messaging platforms (including WhatsApp, whose minimum age in the UK is now 13) have a minimum age of 13 or above. We ask parents to respect age ratings on social media platforms, games and AI apps wherever possible and not encourage or condone underage use. Under the Online Safety Act 2023, platforms must now use highly effective age checks to prevent children accessing pornography and other harmful content, and the government has committed to banning social media services for under-16s.

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

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

ParentMail and Class Dojo are the official electronic communication channel between parents and the school, and between staff and pupils.

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

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

* Exceptions may be made, e.g. for pre-existing family links, but these must be approved by the Headteacher, 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 Headteacher (if by a staff member).

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

The serious consequences of inappropriate behaviour on social media are underlined by the fact that the Teaching Regulation Agency regularly issues prohibition orders to teachers for misconduct involving the misuse of social media and 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

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 acceptable use policies and the following sections of this document which all impact upon device usage: copyright, data protection, social media, misuse of technology, and digital images and video.

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

- **Pupils:** in line with the statutory DfE [Mobile phones in schools](#) guidance, The James Cambell Primary School is a mobile phone-free environment. Pupils may not use mobile phones, or smartwatches and other devices with communication, camera or internet functions, at any time

during the school day, including lessons, break and lunchtimes. Where parents agree that a pupil needs a phone for their journey to or from school, it is switched off and handed in to the class teacher or school office on arrival and collected at the end of the day. Exceptions (for example for a medical condition such as diabetes monitoring, a special educational need or disability, or a young carer) must be agreed in advance with the Headteacher and recorded. Phones or devices used in breach of this policy may be confiscated in line with the Behaviour Policy.

- **All staff who work directly with children** should leave their mobile phones on silent and must not use their own mobile phone for personal reasons in front of pupils throughout the school day; phones should only be used in private staff areas where there are no children present. Child/staff data should never be downloaded onto a private phone. If a staff member is expecting an important personal call when teaching or otherwise on duty, they may leave their phone with the school office to answer on their behalf or ask for the message to be left with the school office.
- **Volunteers, contractors, governors** should leave their phones in their pockets and turned off. Under no circumstances should they be used in the presence of children or to take photographs or videos in the presence of children. If this is required (e.g. for contractors to take photos of equipment or buildings), permission of the headteacher should be sought (the headteacher may choose to delegate this) and this should be done in the presence of a member staff.
- **Parents** are asked to leave their phones in their pockets and turned off when they are on site. They should ask permission before taking any photos, e.g. of displays in corridors or classrooms, and avoid capturing other children. When at school events, expectations are made clear at the start of any performance or trip regarding electronic devices and publications.

Network / internet access on school devices

- **Pupils** are not allowed networked file access via personal devices.
- **Staff** may only connect personal devices to the school network or Wi-Fi where this has been authorised by Partnership Learning IT, and must never store or download child or staff data onto a personal device. See also the Digital images and video section and the Data protection and data security section.
- Parents have no access to the school network or wireless internet on personal devices.

Trips / events away from school

For school trips/events away from school the headteacher will authorise any use of personal mobile phone where a school based device is not available for emergency calls, but not photos. Staff using their personal phone in an emergency will ensure that the number is hidden to avoid a parent or pupil accessing a staff member's private phone number.

Searching and confiscation

In line with the DfE guidance [Searching, screening and confiscation: guidance for schools](#) and the statutory Mobile phones in schools guidance, the Headteacher and staff authorised by them have a statutory power to search pupils/property on school premises and to confiscate mobile phones and other devices where proportionate. 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. Staff must not view, copy or forward any image that they suspect is a nude or semi-nude image of a child, and must pass the device to the DSL, who will follow the UKCIS guidance. Where appropriate within a primary setting, parents will be informed prior to such a search.

Appendix 1 – Roles

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

Roles:

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

All staff

Key responsibilities:

- Read and follow this policy in conjunction with the school's main safeguarding policy and Keeping Children Safe in Education 2026 – all staff must read Part one of KCSIE in full
- 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) is: Denise Parker-Skinner and 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/handbook
- Understand the school's filtering and monitoring systems, your role in them and how to report concerns (for example if you see a pupil access harmful content, if filtering fails, or if over-blocking is affecting teaching), as covered in your safeguarding training
- Follow the Mobile Phone Policy, including not using your own mobile phone for personal reasons in front of pupils during the school day
- Only use school-approved generative AI tools for school work, never enter personal or safeguarding data into unapproved tools, and report any concern about AI misuse (including fake or sexual images of a child) to the DSL
- 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 pupils)
- 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 pupils remotely, be mindful of additional safeguarding considerations
- Carefully supervise and guide pupils 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 cyber security best-practice at all times, including password hygiene, multi-factor authentication and how to spot and report phishing
- Prepare and check all online sources and classroom resources before using for accuracy and appropriateness.
- Encourage pupils/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 sexual harassment, misogyny and the sharing of nude or semi-nude images, including deepfakes – [Keeping Children Safe in Education 2026](#).
- 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 know
- Receive regular updates from the DSL 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.

Headteacher Clara Breakwell

Key responsibilities:

- Foster a culture of safeguarding where online safety is fully integrated into whole-school safeguarding
- Oversee and support the activities of the designated safeguarding lead team and ensure they work with technical colleagues to complete an online safety audit in line with KCSIE (including technology in use in the school)
- Undertake training in offline and online safeguarding, in accordance with statutory guidance and local safeguarding partnership support and guidance
- Ensure ALL staff undergo safeguarding training (including online safety) at induction and with regular updates and that they agree and adhere to policies and procedures
- Ensure ALL governors and trustees undergo safeguarding and child protection training and updates (including online safety) to provide strategic challenge and oversight into policy and practice and that governors are regularly updated on the nature and effectiveness of the school's arrangements.
- Ensure the school implements and makes effective use of appropriate ICT systems and services including school-safe filtering and monitoring, protected email systems and that all technology including remote systems are implemented according to child-safety first principles
- Ensure a member of the senior leadership team is assigned responsibility for filtering and monitoring, and that the effectiveness of filtering and monitoring is reviewed at least once every academic year, with a record kept of the checks made, in line with KCSIE 2026 and the DfE Filtering and monitoring standards – in particular understand what is blocked or allowed for whom, when, and how
- Ensure the school has a Mobile Phone Policy that makes the school a mobile phone-free environment by default, in line with the statutory Mobile phones in schools guidance, and that it is applied consistently
- Ensure the school meets the DfE Cyber security standards for schools and colleges, working with Partnership Learning IT
- Approve any generative AI tools used in school, with the DPO, in line with DfE guidance and the Generative AI: product safety standards

- Liaise with the designated safeguarding lead on all online-safety issues which might arise and receive regular updates on school issues and broader policy and practice information
- Support safeguarding leads and technical staff as they review protections for pupils in the home and remote-learning procedures, rules and safeguards.
- Assign responsibility to a nominated member of staff to carry out online searches with consistent guidelines as part of due diligence for shortlisted candidates in the recruitment process, as set out in KCSIE
- Take overall responsibility for data management and information security ensuring the school's provision follows best practice in information handling; work with the DPO, DSL and governors to ensure a UK 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 pupils, including risk of children being radicalised
- Ensure the school website meets statutory requirements.

Designated Safeguarding Lead / Online Safety Lead –Alan Jacob

Key responsibilities (remember 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”. This responsibility is reflected in the DSL job description
- Work with the HT and technical staff to review protections for **pupils in the home** and **remote-learning** procedures, rules and safeguards.
- 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.
- Liaise with the Headteacher and Chair of Governors to ensure that ALL governors and trustees undergo safeguarding and child protection training (including online safety) at induction to enable them to provide strategic challenge and oversight into policy and practice and that this is regularly updated .

- Take day-to-day responsibility for online safety issues and be aware of the potential for serious child protection concerns
- Support the SLT lead for filtering and monitoring with the annual review of filtering and monitoring, ensure a record of checks is kept, and act on any safeguarding concerns that filtering and monitoring reports reveal
- Ensure that incidents involving nude or semi-nude images, including those that are digitally altered or AI-generated (deepfakes), are managed in line with the UKCIS guidance
- Ensure there are suitable cover arrangements so that a DSL or deputy is always available during school hours (and for out-of-hours activities)
- Be mindful of using appropriate language and terminology around children when managing concerns, including avoiding victim-blaming language.
- Remind staff of safeguarding considerations as part of a review of remote learning procedures and technology, including that the same principles of online safety and behaviour apply
- Work closely with SLT, staff and technical colleagues to complete an online safety audit (including technology in use in the school).
- Work with the headteacher, DPO and governors 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, including generative AI, and “undertake Prevent awareness training.”
- Receive regular updates in online safety issues and legislation, be aware of local and school trends
- Ensure that online safety education is embedded across the curriculum in line with the statutory RSHE guidance (e.g. by use of the 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
- Communicate regularly with SLT and the designated safeguarding and online safety governor/committee to discuss current issues (anonymised), review incident logs and filtering/change control logs and discuss how filtering and monitoring work and have been functioning/helping.
- Ensure all staff are aware of the procedures that need to be followed in the event of an online safety incident, and that these are logged in the same way as any other safeguarding incident.
- Ensure adequate provision for staff to flag issues when not in school and for pupils to disclose issues when off site, especially during any remote learning, e.g. a safe, simple, online form on the school home page about ‘something that’s worrying me’ that gets mailed securely to the DSL inbox
- Oversee and discuss ‘appropriate filtering and monitoring’ with governors (is it physical or technical?) and ensure staff are also aware (Ofsted inspectors may ask staff about this). 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”.
- Ensure KCSIE Part five (child-on-child sexual violence and sexual harassment) is understood and followed throughout the school and that staff adopt a zero-tolerance, whole school approach to all forms of child-on-child abuse, and don’t dismiss it as banter (including bullying).

- Facilitate training and advice for all staff, including supply teachers:
 - all staff (including trainee teachers) must read Part one of KCSIE 2026 in full, and school leaders and staff who work directly with children should also read Annex A (Further information)
 - note that the shorter, condensed version of Part one that was previously in Annex A has been removed in KCSIE 2026; the DfE's 'Part one – overview for all staff' may be used as a quick reference but does not replace reading Part one
 - cascade knowledge of risks and opportunities throughout the organisation

Governing Body, led by Online Safety / Safeguarding Link Governor Key responsibilities (quotes are taken from Keeping Children Safe in Education)

- Approve this policy and strategy and subsequently review its effectiveness.
- 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 assurance into policy and practice, ensuring this is regularly updated.
- Ensure that all staff also receive appropriate safeguarding and child protection (including online) training at induction and that this is updated
- Ensure the school has appropriate filtering and monitoring systems in place and that their effectiveness is reviewed at least once every academic year, with a record kept; review the DfE Filtering and monitoring standards and discuss with IT staff and service providers what more needs to be done to support the school in meeting them
- Ensure the school has appropriate cyber security in place, in line with the DfE Cyber security standards for schools and colleges
- Ensure the school has a Mobile Phone Policy in line with the statutory Mobile phones in schools guidance
- Ask about how the school has reviewed protections for **pupils in the home** (including when with online tutors) and **remote-learning** procedures, rules and safeguards.
- "Ensure an appropriate **senior member** of staff, from the school or college **leadership team**, is appointed to the role of DSL [with] **lead responsibility** for safeguarding and child protection (including online safety) [with] the appropriate status and authority [and] time, funding, training, resources and support..."
- Support the school in encouraging parents and the wider community to become engaged in online safety activities
- Have regular strategic reviews with the online-safety coordinator / DSL and incorporate online safety into standing discussions of safeguarding at governor meetings
- 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 headteacher to ensure a UK 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 one of KCSIE in full, and that SLT and all those working directly with children have read Annex A

- “Ensure that all staff undergo safeguarding and child protection training (including online safety, which amongst other things includes an understanding of the expectations, applicable roles and responsibilities in relation to filtering and monitoring) at induction. The training should be regularly updated in line with advice from the local safeguarding partners, integrated, aligned and considered as part of the overarching safeguarding approach.”
- “Ensure that children are taught about safeguarding, including online safety, as part of providing a broad and balanced curriculum.”

PSHE / RSHE Lead/s – Shaun Murray

Key responsibilities:

- As listed in the ‘all staff’ section, plus:
- Embed consent, mental wellbeing, healthy relationships and staying safe online into the PSHE / Relationships education and health education curriculum, in line with the revised statutory RSHE guidance (compulsory from September 2026). “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.”
- Include the new content in the revised RSHE guidance, such as critically engaging with what pupils see online (including misinformation and AI-generated content), privacy, consent and personal data, age restrictions on social media and gaming, and online financial harms such as in-game spending, scams and fraud
- Focus on the underpinning knowledge and behaviours outlined in [Teaching Online Safety in Schools](#) in an age appropriate way to help pupils to navigate the online world safely and confidently regardless of their device, platform or app.
- Assess teaching to “identify where pupils need extra support or intervention [through] tests, written assignments or self evaluations, to capture progress” .
- This complements the computing curriculum, which covers the principles of online safety at all key stages, with progression in the content to reflect the different and escalating risks that pupils face. This includes how to use technology safely, responsibly, respectfully and securely, and where to go for help and support when they have concerns about content or contact on the internet or other online technologies.
- Work closely with the DSL/OSL and all other staff to ensure an understanding of the issues, approaches and messaging within PSHE / RSHE.
- Note that an RSHE policy should be included on the school website, and parents should be able to view the curriculum materials used to teach RSHE.
- 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 – Natalie Harle

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
- Develop pupils' understanding of how technology, including generative AI, works, its limitations, and how to use it safely, responsibly and critically
- Work closely with the RSHE lead to avoid overlap but ensure a complementary whole-school approach
- Work closely with the DSL/OSL and all other staff to ensure an understanding of the issues, approaches and messaging within Computing
- Collaborate with technical staff and others responsible for ICT use in school to ensure a common and consistent approach, in line with acceptable-use agreements

Subject / aspect leaders

Key responsibilities:

- As listed in the 'all staff' section, plus:
- Look for opportunities to embed online safety in your subject or aspect, especially as part of the RSHE curriculum, and model positive attitudes and approaches to staff and pupils alike
- Work closely with the DSL/OSL and all other staff to ensure an understanding of the issues, approaches and messaging within their subject
- Ensure subject specific action plans also have an online-safety element

Network Manager/technician – Stuart Aiken

Key responsibilities:

- As listed in the 'all staff' section, plus:
- Collaborate regularly with the DSL, the SLT lead for filtering and monitoring and the leadership team to help them make key strategic decisions around the safeguarding elements of technology. KCSIE expects a good understanding of technology and its role in safeguarding, so help DSLs and SLT to understand systems, settings and implications.
- Support the SLT lead and DSL to carry out the annual review of filtering and monitoring required by KCSIE 2026, in association with Partnership Learning IT. This includes checking that filtering is working on all internet-connected devices in all relevant locations, recording when checks took place, what was tested, any issues and the action taken, and reviewing what is allowed, blocked and why, how 'over blocking' is avoided, and whether systems can manage AI-generated content
- Keep up to date with the school's online safety policy and technical information in order to effectively carry out their online safety role and to inform and update others as relevant

- Work closely with the designated safeguarding lead / online safety lead / data protection officer / LGfL nominated contact / RSHE lead to ensure that school systems and networks reflect school policy and there are no conflicts between educational messages and practice.
- Ensure the above stakeholders understand the consequences of existing services and of any changes to these systems (especially in terms of access to personal and sensitive records / data and to systems such as YouTube mode, web filtering settings, sharing permissions for files on cloud platforms etc
- Maintain up-to-date documentation of the school's online security and technical procedures
- To report online-safety related issues that come to their attention in line with school policy
- Manage the school's systems, networks and devices in line with the DfE Cyber security standards for schools and colleges, according to a strict password policy and multi-factor authentication, 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.
- Work with the Headteacher to ensure the school website meets statutory DfE requirements.

Data Protection Officer (DPO) Michael Junnix (Partnership Learning trust)

Key responsibilities:

NB – this document is not for general data-protection guidance;

- Be aware of references to the relationship between data protection and safeguarding in key Department for Education documents 'Keeping Children Safe in Education', 'Data protection in schools' and 'Information sharing advice for safeguarding practitioners', especially the following:
- "The Data Protection Act 2018 and UK GDPR do 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 includes 'safeguarding of children and individuals at risk' as a condition for processing special category personal data, even without consent.** When Designated Safeguarding Leads in schools are considering whether, or not, to share safeguarding information (especially with other agencies) it is considered best practice for them to record who they are sharing that information with and for what reason. If they have taken a decision not to seek consent from the data subject and/or parent/carer that should also be recorded within the safeguarding file. All relevant information can be shared without consent if to gain consent would place a child at risk. Fears about sharing information **must not be allowed** to stand in the way of promoting the welfare and protecting the safety of children.

Safeguarding records may need to be retained for a very long term (until the pupil is aged 25 or older), and some local authorities require record retention until 25 for **all** pupil records. Work with the DSL, headteacher and governors to ensure frameworks are in place for the protection of data and of safeguarding information sharing as outlined above.

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

Complete data protection impact assessments (DPIAs) for new systems, including cloud platforms and generative AI tools, before they are introduced, and support the school in responding to cyber incidents and data breaches.

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 / online safety lead as named in the AUP
- Maintain an awareness of current online safety issues and guidance
- Follow the school's Mobile Phone Policy and never use a personal device to take photographs or videos of pupils
- Model safe, responsible and professional behaviours in their own use of technology at school and as part of remote teaching or any online communications
- Note that as per AUP agreement a contractor will never attempt to arrange any meeting, **including tutoring session**, without the full prior knowledge and approval of the school, and will never do so directly with a pupil. The same applies to any private/direct communication with a pupil.

Pupils

Key responsibilities:

- Treat **any home or remote learning** in the same way as regular learning in school and behave as if a teacher or parent were watching the screen
- Avoid any private communication or use of personal logins/systems to communicate with or arrange meetings with school staff or tutors
- Follow the school's mobile phone rules: phones and smartwatches are not used during the school day and, if a phone is brought to school, it is handed in on arrival
- Only use AI tools that the school has approved, when an adult says so, and remember that AI chatbots are not real people or friends
- Understand the importance of reporting abuse, misuse or access to inappropriate materials, including any concerns about a member of school staff or supply teacher or online tutor
- Know what action to take if they or someone they know feels worried or vulnerable when using online technology, at school, home or anywhere else, including if someone shares, asks for or makes a nude or fake picture of them
- To understand the importance of adopting safe and responsible behaviours and good online safety practice when using digital technologies outside of school and realise that the school's acceptable use policies cover actions out of school, including on social media

- Remember the rules on the misuse of school technology – devices and logins used at home should be used just like if they were in full view of a teacher.
- Understand the benefits/opportunities and risks/dangers of the online world and know who to talk to at school or outside school if there are problems

Parents/carers

Key responsibilities:

- Talk to the school if they have any concerns about their children's and others' use of technology
- Support the school's Mobile Phone Policy, and contact the school office (not their child's phone) if they need to get an urgent message to their child during the school day
- Promote positive online safety and model safe, responsible, respectful and positive behaviours in their own use of technology, including on social media: not sharing other's images or details without permission and refraining from posting negative, threatening or violent comments about others, including the school staff, volunteers, governors, contractors, pupils or other parents/carers.
- Encourage children to engage fully in home-learning, whether for homework or during any period of remote learning, and flag any concerns
- Support the child during any home learning to avoid video calls in a bedroom if possible and if not, to ensure the child is fully dressed and not in bed, with the camera pointing away from beds/bedding/personal information etc. and the background blurred or changed where possible.
- If organising private online tuition, remain in the room if possible, ensure the child knows tutors should not arrange new sessions directly with the child or attempt to communicate privately. Further advice available in the [Online Tutors – Guidance for Parents and Carers](#) poster at parentsafe.lgfl.net, which is a dedicated parent portal offering updated advice and resources to help parents keep children safe online.
- Outside school it is the responsibility of parents/carers to make sure that what their child does online and at home is appropriate for their age, including which games they play, films they watch, apps and AI tools they use and social networking they use. Most social media and messaging apps (including TikTok, Instagram, Snapchat, WhatsApp and Discord) have a minimum age of 13, and many AI chatbots are not intended for children; parental controls and age-appropriate settings should be used on devices, games consoles and broadband.

External groups including parent associations

Key responsibilities:

- Any external individual/organisation will sign an acceptable use policy prior to using technology or the internet within school
- Support the school in promoting online safety and data protection
- Model safe, responsible, respectful and positive behaviours in their own use of technology, including on social media: not sharing other's images or details without permission and refraining

from posting negative, threatening or violent comments about others, including the school staff, volunteers, governors, contractors, pupils or other parents/carers