

The purpose of the policy is to:

- Have robust procedures in place to ensure the online safety of students, staff, volunteers and board members
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology, including mobile and smart technology (which we refer to as ‘mobile phones’)
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

The 4 Key Categories of Risk

Our approach to online safety is based on addressing the following categories of risk:

- **Content** – being exposed to illegal, inappropriate, or harmful content, for example: pornography, racism, misogyny, self-harm, suicide, antisemitism, radicalisation, extremism, misinformation, disinformation (including fake news) and conspiracy theories.
- **Contact** – being subjected to harmful online interaction with other users, such as child-on-child pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes
- **Conduct** – personal online behaviour that increases the likelihood of, or causes, harm, such as making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography), sharing other explicit images and online bullying
- **Contract or Commerce** – risks such as online gambling, inappropriate advertising, phishing and/or financial scam

More information can be found on the link [here](#).

	Content Child as recipient	Contact Child as participant	Conduct Child as actor	Contract Child as consumer
Aggressive	Violent, gory, graphic, racist, hateful and extremist content	Harassment, stalking, hateful behaviour, unwanted surveillance	Bullying, hateful or hostile peer activity e.g. trolling, exclusion, shaming	Identity theft, fraud, phishing, scams, gambling, blackmail, security risks
Sexual	Pornography (legal and illegal), sexualization of culture, body image norms	Sexual harassment, sexual grooming, generation and sharing of child sexual abuse material	Sexual harassment, non-consensual sexual messages, sexual pressures	Sextortion, trafficking for purposes of sexual exploitation, streaming child sexual abuse
Values	Age-inappropriate user-generated or marketing content, mis/disinformation	Ideological persuasion, radicalization and extremist recruitment	Potentially harmful user communities e.g. self-harm, anti-vaccine, peer pressures	Information filtering, profiling bias, polarisation, persuasive design
Cross-cutting	Privacy and data protection abuses, physical and mental health risks, forms of discrimination			

Updating the 4Cs of online risk.

Legislation and guidance

This policy is based on the Department for Education's (DfE) statutory safeguarding guidance, [Keeping Children Safe in Education](#), and its advice for schools on:

- [Teaching online safety in schools](#)
- [Preventing and tackling bullying](#) and [cyber-bullying: advice for headteachers and school staff](#)
- [Relationships and sex education](#)
- [Searching, screening and confiscation](#)
- [Filtering and Monitoring](#)

It also refers to the DfE's guidance on [protecting children from radicalisation](#). The school also consults contemporary advice from the [UK Safer Internet Centre](#) and the [Internet Watch Foundation](#).

It reflects existing legislation, including but not limited to the [Education Act 1996](#) (as amended), the [Education and Inspections Act 2006](#) and the [Equality Act 2010](#). In addition, it reflects the [Education Act 2011](#), which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on students' electronic devices where they believe there is a 'good reason' to do so.

The policy also takes into account the National Curriculum computing programmes of study.

Roles and Responsibilities

The Designated Safeguard Lead

Details of the Riverside School's DSL's are set out in our [child protection and safeguarding policy](#) as well as relevant job descriptions.

The DSL takes lead responsibility for online safety in school, in particular:

- Liaise and coordinate any response with relevant school leadership
- Supporting the Co-Directors in ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Working with staff, as necessary, to address any online safety issues or incidents
- Managing all online safety issues and incidents in line with the school child protection policy
- Ensuring that any online safety incidents are logged and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyberbullying are logged and dealt with appropriately in line with the school's [Anti-bullying policy](#) (CPOMs or Behaviour Management Log as appropriate)
- Updating and delivering staff training on online safety
- Liaising with other agencies and/or external services if necessary

The School Board

The governing board has overall responsibility for monitoring this policy and holding the Co-Directors to account for its implementation.

All Staff

All staff and volunteers are responsible for:

- Maintaining an understanding of this policy
- Implementing this policy consistently
- Agreeing and adhering to the terms on acceptable use of the school's ICT systems and the internet, and ensuring that students follow the school's terms on acceptable use
- Working with the DSL to ensure that any online safety incidents are logged in CPOMs as an "online - social media" incident and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school Code of Conduct and Promotion of Good Behaviour policy
- Responding appropriately to all reports and concerns about sexual violence and/or harassment, both online and offline and maintaining an attitude of 'it could happen here'.

This list is not intended to be exhaustive.

Parents

Parents are expected to:

- Notify a member of staff or the Principal, teachers of form group teachers of any concerns or queries regarding this policy
- Ensure their child has read, understood, and agreed to the terms of the Acceptable Use Policy for Students.

Parents can seek further guidance on keeping children safe online from the following organisations and websites:

- [Be Safe online](#) (Jonathan Taylor)
- What are the issues? – [UK Safer Internet Centre](#)
- Hot topics – [Childnet International](#)
- Parent resource sheet – [Childnet International](#)
- Healthy relationships – [Disrespect Nobody](#)
- [AI - IWF](#)

Primary Schools:

In **Key Stage 1**, students will be taught to:

- Use technology safely and respectfully, keeping personal information private
- Identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies

Students in **Key Stage 2** will be taught to:

- Use technology safely, respectfully and responsibly
- Recognise acceptable and unacceptable behaviour
- Identify a range of ways to report concerns about content and contact

By the **end of primary school**, students will know:

- That people sometimes behave differently online, including by pretending to be someone they are not
- That the same principles apply to online relationships as to face-to-face relationships, including the importance of respect for others online including when we are anonymous
- The rules and principles for keeping safe online, how to recognise risks, harmful content and contact, and how to report them
- How to critically consider their online friendships and sources of information including awareness of the risks associated with people they have never met
- How information and data is shared and used online

- What sorts of boundaries are appropriate in friendships with peers and others (including in a digital context)
- How to respond safely and appropriately to adults they may encounter (in all contexts, including online) whom they do not know

Junior High School

In **Key Stage 3 & 4**, students will be taught to:

- Understand a range of ways to use technology safely, respectfully, responsibly and securely, including protecting their online identity and privacy
- Recognise inappropriate content, contact and conduct, and know how to report concerns
- To understand how changes in technology affect safety, including new ways to protect their online privacy and identity
- How to report a range of concerns

By the **end of Senior High School** students will know:

- Their rights, responsibilities and opportunities online, including that the same expectations of behaviour apply in all contexts, including online
- About online risks, including that any material someone provides to another has the potential to be shared online and the difficulty of removing potentially compromising material placed online
- Not to provide material to others that they would not want shared further and not to share personal material which is sent to them
- What to do and where to get support to report material or manage issues online
- The impact of viewing harmful content
- That specifically sexually explicit material (e.g. pornography) presents a distorted picture of sexual behaviours, can damage the way people see themselves in relation to others and negatively affect how they behave towards sexual partners
- That sharing and viewing indecent images of children (including those created by children) is a criminal offence which carries severe penalties including jail
- How information and data is generated, collected, shared and used online
- How to identify harmful behaviours online (including bullying, abuse or harassment) and how to report, or find support, if they have been affected by those behaviours
- How people can actively communicate and recognise consent from others, including sexual consent, and how and when consent can be withdrawn (in all contexts, including online)

All schools

The safe use of social media and the internet will also be covered in other subjects where relevant.

- Where necessary, teaching about safeguarding, including online safety, will be adapted for vulnerable children, victims of abuse and some students with SEND.

Educating parents about online safety

The school will raise parents' awareness of internet safety through letters or other communications home, and through parent workshops delivered by Jonathan Taylor every two to three years by an online safety expert.

If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with the Head of Student Welfare, class teachers or school leadership.

Filtering and Monitoring

The Department for Education's statutory guidance 'Keeping Children Safe in Education' obliges schools and colleges to "ensure appropriate filters and appropriate monitoring systems are in place. Students should not be able to access harmful or inappropriate material from the school or college's IT system" however, schools will need to 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."

At Riverside School we manage this risk with a sophisticated and robust firewall software, Cyberhound. When children use the school's network to access the internet, they are protected from inappropriate content by our filtering and monitoring systems. However, many students are able to access the internet using their own data plan. To minimise inappropriate use, "roamsafe" software is installed on the school's laptops. Roamsafe enforces the filtering rules no matter where the laptop is connected.

An annual filtering and monitoring review takes place annually and is outlined in the Filtering and Monitoring Policy.

Cyber-bullying

Definition

Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of one person or group by another person or group, where the relationship involves an imbalance of power. (See also the [Anti-bullying policy](#).)

Generative artificial intelligence (AI)

Riverside School recognises the educational value of artificial intelligence (AI) tools, including generative AI, but also acknowledges the potential risks associated with their misuse. The following uses of AI are unacceptable for all users:

- Compromising academic integrity, including plagiarism or cheating;
- Using AI where a teacher has explicitly stated it is not expected or permitted;
- Creating deepfakes or impersonating others;
- Harassment or bullying;
- Engaging in criminal activity, coercion, grooming, or exploitation.

These expectations are detailed further in the school's Artificial Intelligence (AI) Policy.

Riverside School will educate pupils on the safe and responsible use of AI tools, in line with DfE guidance. Online safety teaching will cover issues such as misinformation and disinformation, deepfakes, chatbots, privacy concerns, and the ethical use of AI.

The school's filtering, monitoring, and cyber-security systems are reviewed regularly to minimise risks from AI-enabled technologies. Any use of AI to harass or bully pupils will be dealt with under the school's Anti-Bullying Policy, Code of Conduct, and Promotion of Good Behaviour Policy.

Preventing and addressing cyber-bullying

To help prevent cyber-bullying, we will ensure that students understand what it is and what to do if they become aware of it happening to them or others. Students are encouraged to report any incidents of bullying, including cyber-bullying to a teacher or member of the Leadership Team. Junior and Senior High students may also report any incidents of bullying on the [Student Concerns and Suggestions Form](#), including where they are a witness rather than the victim.

The school will actively discuss cyber-bullying with students, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Form tutors, computing teachers and visiting speakers will discuss cyber-bullying with their tutor groups.

Teaching staff are encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. For example in computing, PSHE lessons, and other subjects where appropriate. High School online safety lessons are delivered through the school's Health, Relationships and Sex Education curriculum.

The school also shares information on cyber-bullying for parents so that they are aware of the signs, how to report it and how they can support children who may be affected.

In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the school behaviour policy. Where illegal, inappropriate or harmful material has been spread among students, the school will use all reasonable endeavours to ensure the incident is contained. (Appendix 1)

The DSL, Principals and Co-Directors will consider whether the incident should be reported to the police if it involves illegal material, and will work with external services if it is deemed necessary to do so.

Examining electronic devices

School staff have the specific power under the Education and Inspections Act 2006 (which has been increased by the Education Act 2011) to search for and, if necessary, delete inappropriate images or files on students' electronic devices, including mobile phones, iPads and other tablet devices, where they believe there is a 'good reason' to do so.

When deciding whether there is a good reason to examine or erase data or files on an electronic device, staff must reasonably suspect that the data or file in question has been, or could be, used to:

- Cause harm, and/or
- Disrupt teaching, and/or
- Break any of the school rules

If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSL and members of the senior leadership team to decide whether they should:

- Delete that material, or
- Retain it as evidence (of a criminal offence or a breach of school discipline), and/or
- Report it to the police*

* Staff may also confiscate devices for evidence to hand to the police, if a pupil discloses that they are being abused and that this abuse includes an online element.

Any searching of students will be carried out in line with:

- The DfE's latest guidance on [screening, searching and confiscation](#)
- UKCIS guidance on [sharing nudes and semi-nudes: advice for education settings working with children and young people](#)

Any complaints about searching for or deleting inappropriate images or files on students' electronic devices will be dealt with through the school complaints procedure.

Acceptable use of the internet in school

All students and staff, volunteers and governors are expected to familiarise themselves with the [Riverside School Acceptable Use Policy - Students](#) and the [Riverside School Acceptable Use Policy - Staff](#).

We will monitor the websites visited by students, staff, volunteers, governors and visitors (where relevant) to ensure they comply with the above.

Students using mobile devices in school

Staff should enforce and students should follow the guidance found in the,

- [Primary School Mobile Phone Policy](#)
- [Junior High Mobile Phone Policy](#)
- [Senior High Mobile Phone Policy](#)

Staff using work devices outside school

All staff members will take appropriate steps to ensure their devices remain secure. This includes, but is not limited to:

- Keeping the device password-protected – strong passwords are at least 8 characters, with a combination of upper and lower-case letters, numbers and special characters (e.g. asterisk or currency symbol)
- Ensuring their hard drive is encrypted – this means if the device is lost or stolen, no one can access the files stored on the hard drive by attaching it to a new device
- Making sure the device locks if left inactive for a period of time
- Not sharing the device among family or friends
- Installing anti-virus and anti-spyware software
- Keeping operating systems up to date – always install the latest updates

Staff members must not use the device in any way which would violate the school's terms of the [mobile phones and personal device use](#) guidance. Additional advice for Early Years staff members should be followed [here](#).

Work devices must be used solely for work activities.

If staff have any concerns over the security of their device, they must seek advice from touchware and their Principal.

Email and Communications

A wide range of rapidly developing communications technologies has the potential to enhance learning. Schools need to consider the benefit of using these technologies for education whilst reducing their risks.

- Staff [Email Communication Guidance](#) is shared with all staff and included in the Staff Handbook.
- Staff should only use their Riverside school email account when communicating any school business (including emails to parents). Users should be aware that email communications (addresses of sent and received emails, but not the content) are monitored.
- Any digital communication between staff and students or parents / carers must be professional in tone and content, and must only take place on school approved systems. Personal email addresses or social media must not be used for these communications.
- Users must immediately tell an appropriate member of staff if they receive any communication which is offensive, discriminatory, threatening or bullying in nature, and should not respond to any such communication.
- Staff or student personal contact information should not be published.
- Students should be taught about online safety issues such as the risks attached to the sharing of personal details. They should also be taught strategies to deal with inappropriate communications and be reminded of the need to communicate appropriately when using digital technologies.
- In all communication, students must not reveal their personal details or those of others, or arrange to meet anyone without specific permission.
- Students need to be educated in how to deal with incoming email and associated attachments.
- The school should consider how email from students to external bodies is presented and controlled.

Social Media – Staff (Protecting Professional Identity)

All schools have a duty of care to provide a safe learning environment for students and staff. Schools could be held responsible, indirectly, for acts of their employees in the course of their employment. Staff members who harass, cyberbully, discriminate on the grounds of sex, race or disability or who defame a third party may render the school or local authority liable to the injured party. Reasonable steps to prevent predictable harm must be in place. Staff use of social media is documented in the [Staff Code of Conduct](#) and the [Social Media Policy](#).

- The school has clear reporting guidance, including responsibilities, procedures and sanctions
- All school staff sign the Acceptable Use Agreement indicating they understand and will follow the guidance contained
- School staff ensure they make no reference in social media to students, parents / carers or school staff

- School staff should not engage in online discussion on personal matters relating to members of the school community
- School staff should ensure that personal opinions are not attributed to the school
- School staff should ensure that security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information
- As part of active social media engagement, it is considered good practice to proactively monitor the internet for public postings about the school. The school should effectively respond to social media comments made by others according to a defined policy or process

Social Media and the Student

- The school will control access to social networking sites, and where relevant educate students in their safe use
- Students will be advised never to give out personal details of any kind which may identify them, their friends or their location
- Students and parents will be advised that the use of social network spaces outside school brings a range of dangers for primary aged students
- Students will be advised to use nicknames and avatars when using social networking sites

Responding to Incidents

- The school will take all reasonable precautions to ensure online safety
- Complaints of internet misuse will be dealt with by a senior member of staff, with the Principal and DSL as first point of contact
- Any complaint about staff misuse must be referred to the Co-Director, unless the concern is about the Director in which case the complaint is referred to the Chair of Board
- Further, where a staff member misuses the school's ICT systems or the internet, or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the Personnel Matter and [Staff Code of Conduct](#). The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.
- Complaints of a child protection nature must be dealt with in accordance with school child protection procedures
- If a member of staff or pupil receives online communication that is considered particularly disturbing or illegal, the Police will be contacted
- If an incident involving sexting comes to the attention of a member of staff, it must be reported to the Designated Safeguarding Lead immediately (see flow chart appendix 1 for further advice relating to sexting incidents)
- Where a pupil misuses the school's ICT systems or internet, we will follow the procedures set out in our policies on [Admissions, Discipline & Exclusions](#). The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.
- Monitoring of incidents takes place and contributes to developments in policy and practice in online safety within the school
- Parents / carers are informed of online safety incidents involving children and young people for whom they are responsible

Further information on how to respond to specific incidents can be found in the [Child Protection \(Safeguarding\) Policy](#).

Remote Teaching

Professional Boundaries

Teaching online is different to teaching face-to-face. But adults should always maintain professional relationships with children and young people. Staff are reminded to follow the Staff Code of Conduct

throughout remote learning.

Child Protection Concerns & Raising Concerns

If children aren't seeing trusted adults at school every day, it's even more important that staff are able to identify any child protection concerns and take appropriate action.

For example, concerns may arise when:

- a staff member sees or hears something worrying during an online lesson
- a child discloses abuse during a phone call or via email.

Staff should continue to document concerns on the CPOMs platform, following the guidelines as set out in this policy.

Platforms

Always make sure the platform you are using is suitable for the children's age group, stage of development and ability. Set up school accounts for any online platforms you use (don't use teachers' personal accounts). Double check the privacy settings.

Contacting Children at Home

Sometimes staff might need to contact children individually, for example to give feedback on homework. Use parents' or carers' email addresses, or phone numbers to communicate with children, unless this poses a safeguarding risk. School generated student email addresses can also be used. Use school accounts to communicate via email or online platforms, never teachers' personal accounts.

Training

All new staff members will receive safeguarding training, as part of their induction, on safe internet use and online safeguarding issues including cyber-bullying.

All staff members will receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates as required.

By way of this training, all staff will be made aware that:

- Technology is a significant component in many safeguarding and wellbeing issues, and that children are at risk of online abuse
- Children can abuse their peers online through:
 - Abusive, harassing, and misogynistic messages
 - Non-consensual sharing of indecent nude and semi-nude images and/or videos, especially around chat groups
 - Sharing of abusive images and pornography, to those who don't want to receive such content
- Physical abuse, sexual violence and initiation/hazing type violence can all contain an online element

Training will also help staff:

- develop better awareness to assist in spotting the signs and symptoms of online abuse
- develop the ability to ensure students can recognise dangers and risks in online activity and can weigh the risks up
- develop the ability to influence students to make the healthiest long-term choices and keep them safe from harm in the short term

The DSL's for each division will undertake child protection and safeguarding training, which will include online safety, at least every 2 years. They will also update their knowledge and skills on the subject of online safety at regular intervals, and at least annually.

Governors will receive training on safe internet use and online safeguarding issues as part of their safeguarding training.

Volunteers will receive appropriate training and updates, if applicable.

More information about safeguarding training is set out in our child protection and safeguarding policy.

Monitoring arrangements

The DSL logs behaviour and safeguarding issues related to online safety on CPOMs.

Links with other policies

[Artificial Intelligence \(AI\) Policy](#)

[Social Media Policy](#)

[Anti-Bullying Policy](#)

[Child on Child Abuse Policy](#)

[ICT Acceptable Use Policy - Staff](#)

[ICT Acceptable Use Policy - Students](#)

[Laptop User Charter & Insurance Agreement \(Staff\)](#)

[Laptop User Charter and Insurance Agreement \(Student\)](#)

[Mobile Phone and Personal Device Use \(Staff\)](#)

[Mobile-Free Learning Environment Policy - Primary & Junior High School](#)

[Mobile-Free Learning Environment Policy - Senior High](#)

[Admissions, Discipline & Exclusions](#)

[Child Protection \(Safeguarding\) Policy](#)

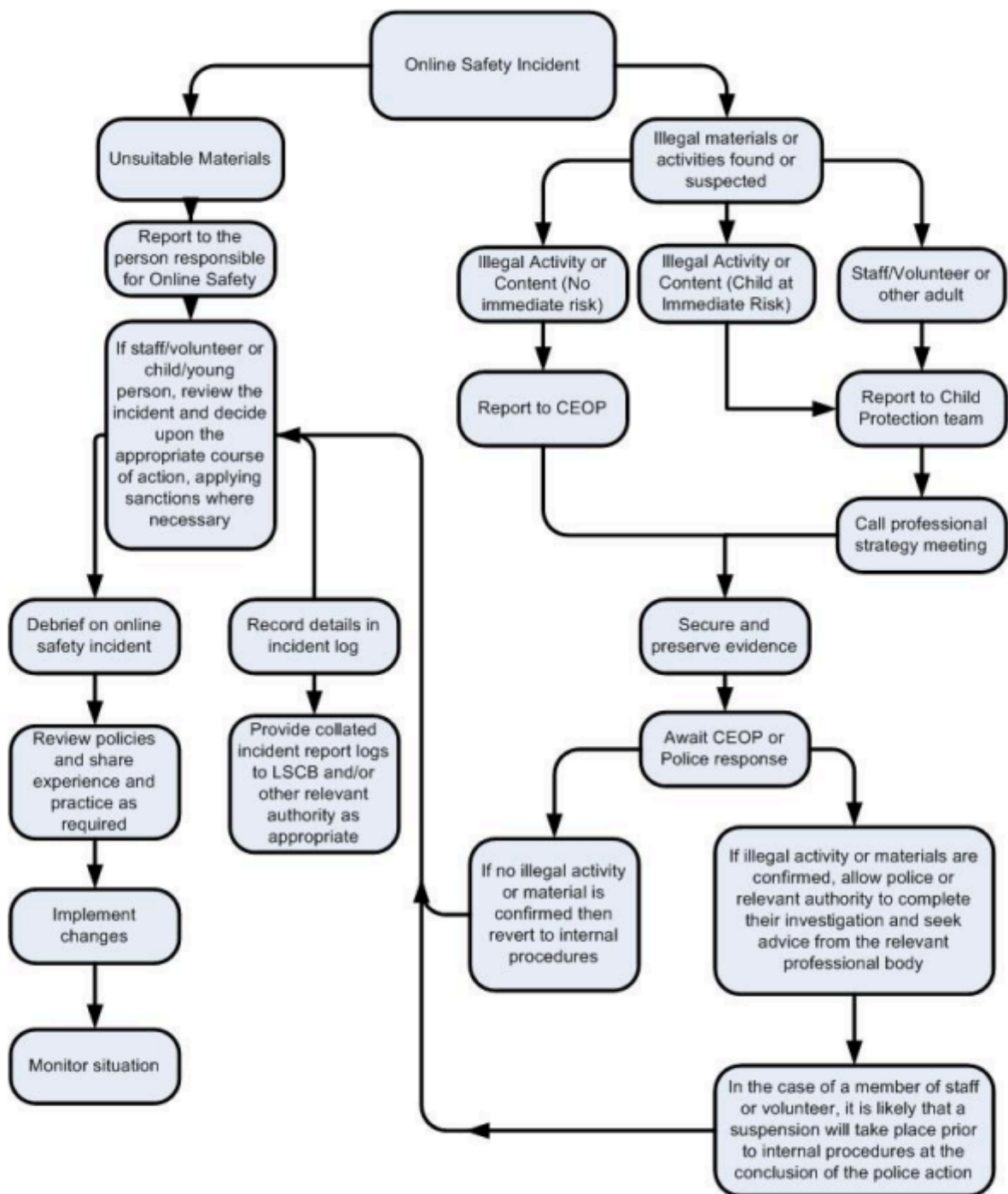
[Filtering and Monitoring Policy](#)

Review Process:

Date of Review: September 2025

Date of Next Review: September 2026

Appendix 1 (example from UK)



CEOP - [Child Exploitation and Online Protection](#)