Online Safety Policy

Date of policy: December 2025

Member of staff responsible:

Review date: December 2026 or in-line with changes in KCSIE 2026

Contents:

Statement of intent

1. Legal framework
2. Roles and responsibilities
3. The curriculum
4. Staff training
5. Educating parents
6. Classroom use
7. Internet access
8. Filtering and monitoring online activity
9. Network security
10. Emails
11. Social networking
12. The school website
13. Use of school-owned devices
14. Use of personal devices
15. Use of mobile phones by pupils
16. Managing reports of online safety incidents
17. Responding to specific online safety concerns
18. Use of Generative AI
19. Monitoring and review
20. Appendix

- **Statement of intent**

  Lady Bay Primary School understands that using online services is an important aspect of raising educational standards, promoting pupil achievement and enhancing teaching and learning.

  The use of online services is embedded throughout the school; therefore, there are a number of controls in place to ensure the safety of pupils and staff.

  The breadth of issues classified within online safety is considerable, but they can be categorised into four areas of risk:

- **Content**: Being exposed to illegal, inappropriate or harmful material, e.g. pornography, fake news, and racist or radical and extremist views.
- **Contact**: Being subjected to harmful online interaction with other users, e.g. commercial advertising and adults posing as children or young adults.
- **Conduct**: Personal online behaviour that increases the likelihood of, or causes, harm, e.g. sending and receiving explicit messages, and cyberbullying.
- **Commerce**: Risks such as online gambling, inappropriate advertising, phishing and or financial scams

  The measures implemented to protect pupils and staff revolve around these areas of risk. Our school has created this policy with the aim of ensuring appropriate and safe use of the internet and other digital technology devices by all pupils and staff.

1. Legal framework

This policy has due regard to all relevant legislation and guidance including, but not limited to, the following:

- Voyeurism (Offences) Act 2019
- The General Data Protection Regulation (GDPR)
- Data Protection Act 2018
- DfE (2023) 'Keeping children safe in education'
- DfE (2019) 'Teaching online safety in school'
- DfE (2022) 'Searching, screening and confiscation'
- National Cyber Security Centre (2017) 'Cyber Security: Small Business Guide'
- UK Council for Child Internet Safety 'Education for a Connected World'
- UK Council for Child Internet Safety (2020) 'Sharing nudes and semi-nudes: advice for education settings working with children and young people'
- DfE (2015) Protecting children from radicalisation: the prevent duty.

This policy operates in conjunction with the following school policies:

- Allegations of Abuse Against Staff Policy (comes under - NDP)
- Acceptable Use Policies
- Child Protection Safeguarding Policy
- Anti-Bullying Policy
- RHE Policy
- Staff Code of Conduct
- Behaviour Policy
- Disciplinary Policy and Procedures (Nottinghamshire Disciplinary Procedure)
- Data Protection Policy
- Privacy Notice
- Photography Policy
- Prevent Policy Statement
- Mobile Phone Policy

2. Roles and responsibilities

The **governing board** is responsible for:

- Ensuring that this policy is effective and complies with relevant laws and statutory guidance.
- Ensuring the DSL's remit covers online safety.
- Reviewing this policy on an **annual** basis.
- Ensuring their own knowledge of online safety is up-to-date. This may include attending online safety training delivered to staff/parents.
- Ensuring 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.
- Ensuring that there are appropriate filtering and monitoring systems in place.

The **headteacher** is responsible for:

- Being the DSL and supporting any deputies including the Online Safety Coordinator, by ensuring they have enough time and resources to carry out their responsibilities in relation to online safety.
- Safeguarding and child protection including online safety and understanding the filtering and monitoring systems and processes in place.
- Acting as the named point of contact within the school on all online safeguarding issues.
- Monitoring online safety incidents to identify trends and any gaps in the school's provision, and using this data to update the school's procedures.
- Ensuring appropriate referrals are made to external agencies, as required
- Ensuring staff receive regular, up-to-date and appropriate online safety training and information as part of their induction and safeguarding training.
- Ensuring online safety practices are audited and evaluated.
- Working with the **governing body** to update this policy on an **annual** basis.

The Online Safety Coordinator is responsible for:

- Taking the lead responsibility for online safety in the school.
- Undertaking training so they understand the risks associated with online safety and can recognise additional risks that vulnerable pupils and children with SEND face online.

- Liaising with relevant members of staff on online safety matters, e.g. the SENCO, Computing Lead and ICT technician.
- Ensuring online safety is recognised as part of the school's safeguarding responsibilities and that a coordinated approach is implemented.
- Staying up-to-date with current research, legislation and online trends.
- Coordinating the school's participation in local and national online safety events, e.g. Safer Internet Day.
- Supporting staff to ensure that online safety is embedded throughout the curriculum so that all pupils can develop an appropriate understanding of online safety.
- Organising engagement with parents to keep them up-to-date with current online safety issues and how the school is keeping pupils safe.
- Ensuring all members of the school community understand the reporting procedure and that all concerns are uploaded to CPOMS.
- Reporting to the **headteacher** about online safety on a **termly** basis.
- Working with the **headteacher and governing board** to update this policy on an **annual** basis.
- Sending a copy of the **Acceptable Use Policy** at **the beginning of each academic year** to parents.

The ICT technician and our connectivity providers are responsible for:

- Implementing appropriate security measures as directed by the **headteacher**.
- Ensuring that the school's filtering and monitoring systems are updated as appropriate.

All staff members are responsible for:

- Adhering to this policy, the **Acceptable Use Policy** and other relevant policies.
- Completing safeguarding and protection training, including online safety at induction.
- Taking responsibility for the security of ICT systems and electronic data they use or have access to.
- Modelling good online behaviours.
- Maintaining a professional level of conduct in their personal use of technology.
- Completing annual online safety child protection training and keep up to date with any updates received, as appropriate.
- Having an awareness of online safety issues including the expectations, applicable roles and responsibilities in relation to filtering and monitoring.

- Reporting concerns in line with the school's reporting procedure.
- Where relevant to their role, ensuring online safety is embedded in their teaching of the curriculum.

Pupils are responsible for:

- Adhering to this policy, the **Acceptable Use Policy** and other relevant policies.
- Seeking help from school staff if they are concerned about something they or a peer has experienced online.
- Reporting online safety incidents and concerns in line with the procedures within this policy.

3. The curriculum

Online safety is embedded throughout the curriculum; however, it is particularly addressed in the following subjects:

- RHE
- Computing

The curriculum and the school's approach to online safety is developed in line with the UK Council for Child Internet Safety's 'Education for a Connected World' framework (Project Evolve) and the DfE's 'Teaching online safety in school' guidance.

Pupils are taught the underpinning knowledge and behaviours that can help them to navigate the online world safely and confidently regardless of the device, platform or app they are using.

Online safety teaching is always appropriate to pupils' ages and developmental stages.

The underpinning knowledge and behaviours pupils learn through the curriculum include the following themes (Project Evolve):

- Self-Image and Identity
- Online Relationships
- Online Reputation
- Online Bullying
- Managing Online Information
- Health, Well-being and Lifestyle
- Privacy and Security
- Copyright and Ownership

The online risks pupils may face online are always considered when developing the curriculum.

The DSL is involved with the development of the school's online safety curriculum.

The school recognises that, while any pupil can be vulnerable online, there are some pupils who may be more susceptible to online harm or have less support from family and friends in staying safe online, e.g. pupils with SEND and LAC. Relevant members of staff, e.g. the SENCO and designated teacher for LAC, work together to ensure the curriculum is tailored so these pupils receive the information and support they need.

Class teachers review external resources prior to using them for the online safety curriculum, to ensure they are appropriate for the cohort of pupils. When reviewing these resources, the following questions are asked:

- Where does this organisation get their information from?
- What is their evidence base?
- Have they been externally quality assured?
- What is their background?
- Are they age appropriate for pupils?
- Are they appropriate for pupils' developmental stage?

External visitors may be invited into school to help with the delivery of certain aspects of the online safety curriculum. The **headteacher and DSL** decide when it is appropriate to invite external groups into school and ensure the visitors selected are appropriate.

The class teacher and DSL keep updated with regard to pupils in the class who have suffered or may be suffering from online abuse or harm in this way. The DSL advises the staff member on how to best support any pupil who may be especially impacted by a lesson or activity.

Lessons and activities are planned carefully so they do not draw attention to a pupil who is being or has been abused or harmed online, to avoid publicising the abuse.

During an online safety lesson or activity, the class teacher ensures a safe environment is maintained in which pupils feel comfortable to say what they feel and are not worried about getting into trouble or being judged.

If a staff member is concerned about anything pupils raise during online safety lessons and activities, they will make a report in line with sections 15 and 16 of this policy.

If a pupil makes a disclosure to a member of staff regarding online abuse following a lesson or activity, the staff member will follow the reporting procedure outlined in sections 15 and 16 of this policy.

4. Staff training

All staff will receive online safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- formal online safety and data protection training will be made available to all staff. This will be regularly updated and reinforced. An audit of the online safety training needs of all staff will be carried out regularly.
- the training will be an integral part of the school's annual safeguarding and data protection training for all staff
- all new staff will receive online safety training as part of their induction programme, ensuring that they fully understand the school online safety policy and acceptable use agreements.
- the Online Safety Lead will provide advice/guidance/training to individuals as required.

The DSL and any deputies undergo training to provide them with the knowledge and skills they need to carry out their role, this includes online safety training. This training is updated annually.

In addition to this formal training, the DSL and any deputies receive regular online safety updates to allow them to keep up with any developments relevant to their role. In relation to online safety, these updates allow the DSL and their deputies to:

- Understand the unique risks associated with online safety and be confident that they have the relevant knowledge and capability required to keep pupils safe while they are online at school.
- Recognise the additional risks that pupils with SEND face online and offer them support to stay safe online.

All staff receive a copy of this policy upon their induction and are informed of any changes to the policy.

Staff are required to adhere to the **Staff Code of Conduct** at all times, which includes provisions for the acceptable use of technologies and the use of social media.

All staff are informed about how to report online safety concerns, in line with sections 16 and 17 of this policy.

The Online Safety Coordinator acts as the first point of contact for staff requiring advice about online safety.

Staff are trained annually on the changes outlined in KCSIE 2025. This is carried out through the NCC quiz. Staff were trained on the risk of misinformation, disinformation and deep fakes and why these are dangerous to children. We have also made staff aware of the potential risk of conspiracy theories.

5. Educating parents

The school works in partnership with parents to ensure pupils stay safe online at school and at home.

Parents are provided with information about the school's approach to online safety and their role in protecting their children. Parental awareness is raised in the following ways:

- Twilight training sessions
- The school's website
- Newsletters
- Distribution of the online safety magazine Digital Parenting

Parents are sent a copy of the **Acceptable Use Policy** at **the beginning of each academic year** and are encouraged to go through this with their child to ensure their child understands the document and the implications of not following it.

6. Classroom use

A wide range of technology is used during lessons, including the following:

- Computers
- Laptops
- iPads
- Cameras
- OneDrive
- The school's server

Prior to using any websites, tools, apps or other online platforms in the classroom, or recommending that pupils use these platforms at home, the class teacher always reviews and evaluates the resource.

Class teachers ensure that any internet-derived materials are used in line with copyright law.

Pupils are supervised when using online materials during lesson time – this supervision is suitable to their age and ability.

Seesaw Digital Learning Journals

Pupils have their own Seesaw digital learning journals. Seesaw provides a powerful way of collating and celebrating the achievements of our pupils and sharing them with our parents. Pupils are able to post images, videos and audio recordings related to their classwork on their journals. All posts, including comments, have to be approved by the class teacher. Seesaw is also used for home learning. Parents only have access to their own child's journal content. Parents sign a school Seesaw permission form.

Seesaw is compliant with GDPR in how it stores data.

7. Internet access

Pupils, staff and other members of the school community are only granted access to the school's internet network once they have read and signed the **Acceptable Use Policy** (see appendix).

Records are kept of Staff agreements.

8. Filtering and monitoring online activity

The **governing board** ensures the school's ICT network has appropriate filters and monitoring systems in place.

The **headteacher and Online Safety Coordinator** determine with advice from ATOM IT what filtering and monitoring systems are required. On October 2nd 2024 Lady Bay moved to Securly, a cloud-based web filter designed exclusively for schools. This filters all access to the internet on all devices in school.

The filtering and monitoring systems the school implements are appropriate to pupils' ages, the number of pupils using the network, how often pupils access the network, and the proportionality of costs compared to the risks.

The connectivity provider, ATOM IT, undertakes regular checks on the filtering and monitoring systems to ensure they are effective and appropriate.

Requests regarding making changes to the filtering system are directed to the Online safety Co-ordinator.

Reports of inappropriate websites or materials are made to **the headteacher** immediately, who investigates the matter and takes appropriate action.

Deliberate breaches of the filtering system are reported to **the headteacher**, who will escalate the matter appropriately.

If a pupil has deliberately breached the filtering system, they will be disciplined in line with the Behaviour Policy.

If a member of staff has deliberately breached the filtering system, they will be disciplined in line with the **Disciplinary Policy and Procedure**.

If material that is believed to be illegal is accessed, inadvertently or deliberately, this material will be reported to the appropriate agency immediately, e.g. the Internet Watch Foundation (IWF), CEOP and/or the police.

The school's network and school-owned devices are appropriately monitored.

All users of the network and school-owned devices are informed about how and why they are monitored.

Concerns identified through monitoring are reported to the **the headteacher** who manages the situation in line with sections 15 and 16 of this policy.

9. Network security

Technical security features, such as anti-virus software, are kept up-to-date and managed by the **ICT technician**.

Firewalls are switched on at all times.

Staff members report all malware and virus attacks to the **ICT technician**.

All members of staff have their own unique usernames and private passwords to access the school's systems.

Pupils in **Key Stage 1 and 2** are provided with their own unique username and private passwords for particular websites/ apps.

Staff members and pupils are responsible for keeping their passwords private.

Users are required to lock access to devices and systems when they are not in use.

10. Emails

Access to and the use of emails is managed in line with the **Data Protection Policy**, **Acceptable Use Policy** and **Privacy notice**.

Staff are given approved school email accounts and are advised to use these accounts at school and when doing school-related work outside of school hours.

Any email that contains sensitive or personal information is only sent using secure and encrypted email.

11. Social networking

Personal use

Access to social networking sites is filtered as appropriate.

Staff and pupils are not permitted to use social media for personal use during lesson time.

Staff members are advised that their conduct on social media can have an impact on their role and reputation within the school.

Staff receive **regular updates** on how to use social media safely and responsibly.

Staff are not permitted to communicate with pupils or parents over social networking sites and are reminded to alter their privacy settings to ensure pupils and parents are not able to contact them on social media.

Pupils are taught how to use social media safely and responsibly through the online safety curriculum.

Concerns regarding the online conduct of any member of the school community on social media are reported to the **DSL** and managed in accordance with the relevant policy, e.g. **Anti-Bullying Policy, Staff Code of Conduct and Behaviour Policy**.

The **Staff Code of Conduct** contains information on the acceptable use of social media – staff members are required to follow these expectations at all times.

12. The school website

The **headteacher** is responsible for the overall content of the school website – they will ensure the content is appropriate, accurate, up-to-date and meets government requirements.

The website complies with guidelines for publications including accessibility, data protection, respect for intellectual property rights, privacy policies and copyright law.

Personal information relating to staff and pupils is not published on the website.

Images and videos are only posted on the website if the provisions in the **Photography Policy** are met.

13. Use of school-owned devices

Staff members are issued with the following devices to assist with their work:

- Laptop
- Class iPad for SLT and class teachers

Pupils are provided with school-owned devices as necessary to assist in the delivery of the curriculum, e.g. PCs, laptops and iPads to use during lessons.

All school-owned laptops are password protected.

All mobile school-owned devices are fitted with tracking software to ensure they can be retrieved if lost or stolen.

The ICT technician reviews laptops and PCs as necessary to carry out software updates and ensure there is no inappropriate material on the devices.

No software, apps or other programmes can be downloaded onto a device without authorisation from the **ICT technician and the Computing coordinators.**

Staff members or pupils found to be misusing school-owned devices are disciplined in line with the **Disciplinary Policy and Procedure** and **Behaviour Policy**.

14. Use of personal devices

Any personal electronic device that is brought into school is the responsibility of the user.

Staff members are not permitted to use their personal devices during lesson time, other than in an emergency.

Staff members are not permitted to use their personal devices to take photos or videos of pupils.

Staff members report concerns about their colleagues' use of personal devices on the school premises in line with the **Allegations of Abuse Against Staff Policy**.

If a member of staff is thought to have illegal content saved or stored on a personal device, or to have committed an offence using a personal device, the **headteacher** will inform the police and action will be taken in line with the **Allegations of Abuse Against Staff Policy**.

Any concerns about visitors' use of personal devices on the school premises are reported to the **DSL**.

15. Use of mobile phones by pupils

As a school we understand the fact many children have unlimited and unrestricted access to the internet via mobile phone networks (i.e. 3G, 4G and 5G). This access means some children sexually harass, bully, and control others via their mobile and smart technology, share indecent images consensually and non-consensually (often via large chat groups) and view harmful content. To prevent the misuse of mobile phones in school, we have a **Mobile Phone Policy** in place which clearly outlines the use of mobiles phones by pupils in school and sanctions should a pupil fail to adhere to this policy.

16. Managing reports of online safety incidents

Staff members and pupils are informed about what constitutes inappropriate online behaviour in the following ways:

- Staff training
- The online safety curriculum
- Assemblies

Concerns regarding a staff member's online behaviour are reported to the **headteacher** who decides on the best course of action in line with the relevant policies, e.g. **Staff Code of Conduct, Allegations of Abuse Against Staff Policy and Disciplinary Policy and Procedures**.

Concerns regarding a pupil's online behaviour are reported to the **DSL** who investigates concerns with relevant staff members.

Concerns regarding a pupil's online behaviour are dealt with in accordance with relevant policies depending on their nature, e.g. **Behaviour Policy and Child Protection and Safeguarding Policy**.

Where there is a concern that illegal activity has taken place, the **headteacher** contacts the police.

All online safety incidents and the school's response are recorded on CPOMS.

Section 17 of this policy outlines how the school responds to specific online safety concerns, such as cyberbullying and peer-on-peer abuse.

17. Responding to specific online safety concerns

Cyberbullying

Cyberbullying, against both pupils and staff, is not tolerated.

Any incidents of cyberbullying are dealt with quickly and effectively whenever they occur.

Information about the school's full response to incidents of cyberbullying can be found in the **Anti-bullying Policy**.

The school recognises that peer-on-peer abuse can take place online.

The school responds to all concerns regarding online peer-on-peer abuse, whether or not the incident took place at school.

Concerns regarding online peer-on-peer abuse are reported to the **DSL** who will investigate the matter in line with the **Child Protection Policy**.

Information about the school's full response to incidents of online peer-on-peer abuse can be found in the **Child Protection Policy**.

Upskirting

Under the Voyeurism (Offences) Act 2019, it is an offence to operate equipment and to record an image beneath a person's clothing without consent and with the intention of observing, or enabling another person to observe, the victim's genitals or buttocks (whether exposed or covered with underwear), in circumstances where their genitals, buttocks or underwear would not otherwise be visible, for a specified purpose.

A "specified purpose" is namely:

- Obtaining sexual gratification (either for themselves or for the person they are enabling to view the victim's genitals, buttocks or underwear).
- To humiliate, distress or alarm the victim.

"Operating equipment" includes enabling, or securing, activation by another person without that person's knowledge, e.g. a motion activated camera.

Upskirting is not tolerated by the school.

Incidents of upskirting are reported to the **DSL** who will then decide on the next steps to take, which may include police involvement, in line with the **Child Protection Policy**.

Sharing nudes and semi-nudes

This is defined as the sending or posting of nude or semi-nude images, videos or live streams online by young people under the age of 18. This could be via social media, gaming platforms, chat apps or forums. It could also involve sharing between devices via services like Apple's AirDrop which works offline.

All concerns regarding sharing nudes and semi-nudes are reported to the **DSL**.

Following a report of sharing nudes and semi-nudes, the process outlined in the school's Child Protection Policy is followed.

When investigating a report, staff members do not view the youth produced sexual imagery unless there is a good and clear reason to do so.

If a staff member believes there is a good reason to view youth produced sexual imagery as part of an investigation, they discuss this with the headteacher first.

The decision to view imagery is based on the professional judgement of the DSL and always complies with the **Child Protection Policy**.

Any accidental or intentional viewing of youth produced sexual imagery that is undertaken as part of an investigation is recorded.

If it is necessary to view the imagery, it will not be copied, printed or shared.

Online abuse and exploitation

Through the online safety curriculum, pupils are taught about how to recognise online abuse and where they can go for support if they experience it.

The school responds to concerns regarding online abuse and exploitation, whether or not it took place on the school premises or using school-owned equipment.

All concerns relating to online abuse and exploitation, including child sexual abuse and exploitation and criminal exploitation, are reported to the **DSL** and dealt with in line with the **Child Protection and Safeguarding Policy**.

Online hate

The school does not tolerate online hate content directed towards or posted by members of the school community.

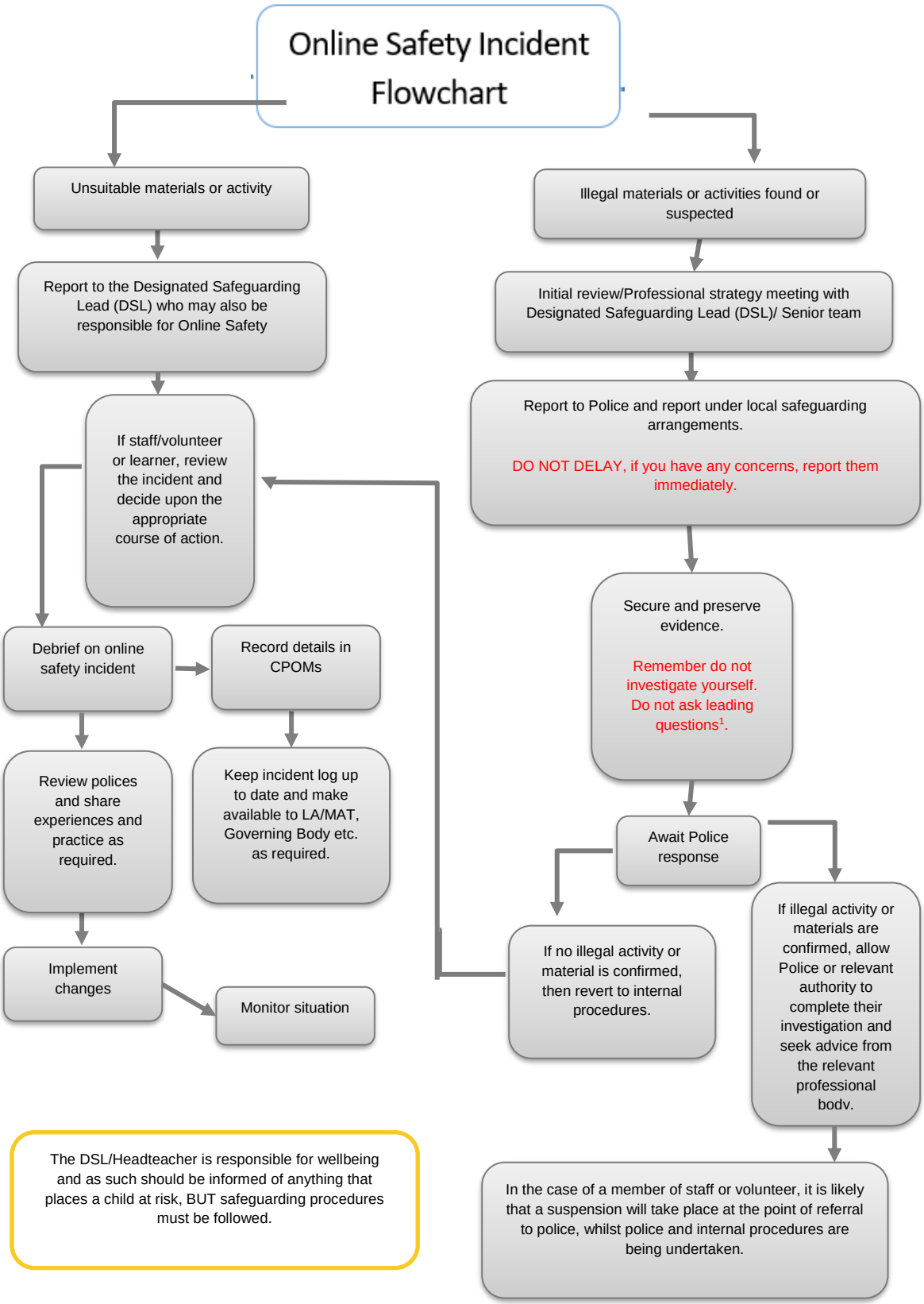
Incidents of online hate are dealt with in line with the relevant school policy depending on the nature of the incident and those involved, e.g. **Staff Code of Conduct, Anti-Bullying Policy.**

Online radicalisation and extremism

The school's filtering system ensures that pupils are safe from terrorist and extremist material when accessing the internet. Children are taught about the risk of radicalisation in upper KS2 classes.

Concerns regarding a staff member or pupil being radicalised online are dealt with in line with the **Child Protection Policy** and **Prevent Policy Statement.**

The school will make the flowchart below available to staff to support the decision-making process for dealing with online safety incidents.



18. Use of Generative AI

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

a. We will talk about the use of these tools, their practical use as well as their ethical pros and cons with pupils as part of our Computing curriculum, staff through our ongoing CPD and parents through the newsletter and awareness raising sessions.
b. We are aware that there will be use of these apps and exposure to AI creations on devices at home for some children – these experiences may be both positive/creative and also negative (inappropriate data use, misinformation, bullying, deepfakes, nudifying apps and inappropriate chatbots). We will discuss children's use of generative AI at home with them as part of their learning in Computing and PSHE.
c. By default, we block access to the Generative AI category for pupils using our Smoothwall filtering system. Access to specific platforms may be granted for teaching and learning purposes if appropriate, and on a case-by-case basis.

19. Monitoring and review

The school recognises that the online world is constantly changing; therefore, **the DSL, Online Safety Coordinator and the headteacher** conduct **regular** light-touch reviews of this policy to evaluate its effectiveness.

The **governing board, headteacher and DSL** review this policy in full on an **annual** basis.

	Signed Headteacher
Date of review: November 2024	
Date of next review: November 2025	

20. APPENDIX



Acceptable Use Policy (AUP) Agreement form for KS1 PUPILS

My name is _____

This is how I keep SAFE online:	✓
1. I only use the devices I'm ALLOWED to	
2. I CHECK before I use new sites, games or apps	
3. I ASK for help if I'm stuck	
4. I KNOW people online aren't always who they say	
5. I don't keep SECRETS just because someone asks me to	
6. I am RESPONSIBLE so never share private information	
7. I TELL a trusted adult if I'm upset, worried, scared or confused	
8. I FOLLOW my trusted adults' instructions when I use Seesaw	



Acceptable Use Policy Agreement form for KS2 PUPILS

This agreement will help keep me safe and help me to be fair to others

2. ***I learn online*** – I use the school's internet and devices to learn and have fun. I only use apps, sites and games if a trusted adult says I can. I only use YouTube when I have permission from a trusted adult to do so.
3. ***I am creative online*** – I don't just spend time on apps, sites and games looking at things from other people; I get creative to learn and make things!
4. ***I am a friend online*** – I won't share anything that I know another person wouldn't want shared, or which might upset them. And if I know a friend is worried or needs help, I will remind them to talk to an adult, or even do it for them.
5. ***I am a secure online learner*** – I do not share my passwords.
6. ***I am careful what I click on*** – I don't click on links I don't expect to see.
7. ***I ask for help if I am scared or worried*** – I will talk to a trusted adult if anything upsets me or worries me on an app, site or game.
8. ***I know it's not my fault if I see something bad***– I know I mustn't share it with others. Instead, I will tell a trusted adult straightaway.
9. ***I share positive comments with others*** – I know not to share unpleasant comments about other people eg. in comments on Seesaw about other people's work. I know that everything I post on Seesaw has to be approved by a teacher.
10. ***I ask permission to use images of other*** people – I ask first if I can use an image of another pupil or teacher for example in a presentation or post on Seesaw.
11. ***I understand copyright –*** I know that it is wrong to copy someone else's work and say that it is my own.
12. ***I communicate and collaborate online*** – with people I know and have met in real life or that a trusted adult knows about.
13. ***I tell my parents/carers what I do online*** – they might not know the app, site or game, they need to know what I'm doing.
14. ***I am private online*** – I only give out private information if a trusted adult says it's okay. This might be my home address, phone number or other personal information that could be used to identify me or my family and friends.
15. ***I am a rule-follower online*** – I know that apps, sites and games have rules on how to behave, and some have age restrictions. I follow the rules, only use the ones I am allowed to use, and report bad behaviour.
16. ***I respect people's work*** – I only edit my own digital work.

17. ***I am a researcher online*** – I use safe search tools approved by my trusted adults. I know I can't believe everything I see online, know which sites to trust, and know how to double check information I find.

I have read and understood this agreement.

Outside school, my trusted adults are_____

Signed: _____ **Date: _____**



Acceptable Use Policy Agreement form for Staff

This agreement covers the use of digital technologies in school

I will follow 'good practice' advice in the creation and use of my password. If my password is compromised, I will ensure I change it. I will not use anyone else's password.

I will not allow unauthorised individuals to access email.

I will use the approved, secure email system for any school business.

I will not browse, download or send material that could be considered offensive.

I will report any accidental access to, or receipt of inappropriate materials, or filtering breach.

I will not connect a computer, laptop or other device (including USB flash drive), to the network / Internet that does not have up-to-date anti-virus software.

I will not use personal digital cameras or camera phones for taking and transferring images of pupils or staff without permission.

I will ensure that any private social networking sites / blogs etc. that I create or actively contribute to are not confused with my professional role.

I will ensure any confidential data that I wish to transport from one location to another is protected by encryption.

I will embed the school's online safety curriculum into my teaching.

I understand that all Internet usage / and network usage can be logged and this information could be made available to my manager on request.

I understand that it is my duty to support a whole-school online safety approach and will report any behaviour (of other staff or pupils), which I believe may be inappropriate or concerning in any way, to the DSL or Online safety Coordinator at the school.

I will ensure that supply teachers using my laptop cannot access my emails or children's personal information.

To be completed by the user

I have read, understood and agreed to this policy. I understand that it is my responsibility to ensure I remain up to date and read and understand the school's most recent online safety policy.

Signature: _____

Name: _____

Date: _____