Online Safety & Acceptable Use Policy

Long Sutton Church of England Primary School

<table>
<tr><th>Date of Last Review</th><th>Date of Next Review</th></tr>
<tr><td>February 2023
(reviewed by governors May 2023)</td><td>February 2024</td></tr>
<tr><th colspan="2">Responsibility for Review and Monitoring / Auditing</th></tr>
<tr><td colspan="2">Headteacher in partnership with staff & Foundation Governors</td></tr>
<tr><th colspan="2">Purpose</th></tr>
<tr><td colspan="2">This Online Safety Policy outlines the commitment of Long Sutton Primary School to safeguard members of our school community online in accordance with statutory guidance and best practice.
The Online Safety Policy applies to all members of the school community (including staff, learners, volunteers, parents and Carers and visitors) who have access to and are users of school digital systems, both in and out of school. It also applies to the use of personal digital technology on the school site (where allowed).</td></tr>
</table>

Long Sutton Church of England Primary School
Online Safety and Acceptable Use Policy

The welfare of the students at our school is of paramount importance. We recognise that pupils today are growing up in an increasingly complex world. IT and new technologies offer many opportunities but that there are also challenges and risks. The different types of harmful content that children can come across online include sexual content, including pornography; violent, distressing or aggressive content; value-based content and biased content. How we aim to reduce these risks and prepare children to be responsible internet citizens is outlined in this policy.

The Online Safety Policy and its implementation will be reviewed annually, or more regularly in light of any significant new developments, threats or incidents.

Responsibilities

Headteacher and Senior Leadership

The Headteacher with support from the Deputy Headteacher/ Online Safety Lead is responsible for all matters of safeguarding, including online safety at Long Sutton CE Primary. Both hold the role of Designated Safeguarding Lead.

Governors

Governors are responsible for the approval of the Online Safety Policy and for reviewing the effectiveness of the policy.

Teaching and Support Staff

Teaching and support staff are responsible for ensuring that they have an awareness of current online safety matters and of the school policy and practices, including the responsibility they have for immediately reporting and recording any suspected misuse or problem as per the school safeguarding procedures. This is set out in Appendix 1, 'Acceptable Use of ICT at Long Sutton Primary School'.

Pupils

Pupils are responsible for using the school digital systems in accordance with the learner acceptable use agreement and Online Safety Policy.

Parents and Carers

Parents and Carers play a crucial role in ensuring that their children understand the need to use the online services and devices in an appropriate way. The school will take every opportunity to help carers and parents to understand these issues through publishing the Online Safety Policy, links to support and helpline on the school website and on the newsletter. Parents and carers are responsible for checking the website regularly, reading information on newsletters and responding appropriately in their use of social media posts regarding the school.

Parent's will be asked to read through the school's 'Online Safety Acceptable Use Agreement' (appendix 1) with their child and sign accordingly.

Teaching and Learning

Why internet use is important

We believe that the internet and other digital technologies are powerful resources, which when utilised effectively, can transform and enhance both teaching and learning. The internet is an essential element within 21st century life for education, business and social interaction. The school provides pupils with the opportunities to use the excellent resources on the internet, alongside developing the skills necessary to access, analyse and evaluate them in a safe, considered and respectful way. The reliance on the internet during periods of remote teaching and learning has shown why it is an ongoing priority.

Internet use and safety is a part of the statutory curriculum and is an integral part of the whole school ethos of being kind, respectful and being the best you can be. It is woven across the whole school curriculum and is an integral part of our safeguarding policy.

Online Safety Education Programme

Pupils

Online safety should be a focus in all areas of the curriculum and staff should reinforce online safety messages across the curriculum and embed this within a wider whole school approach. The online safety curriculum should be broad, relevant and provide progression, with opportunities for creative activities provided in the following ways:

- A planned online safety curriculum for all age groups, matched against the nationally agreed framework of 'Education for a Connected World', using a variety of resources and contexts to support this.

- A progression of skills document which ensures age-related expectations for our mixed age class structure
- The incorporation of relevant national initiatives and opportunities such as Safer Internet Day and Anti-bullying week.
- Digital competency is planned and threaded through other curriculum areas, such as PSE, SRE and English.
- The programme is accessible to learners of different abilities, including those with additional needs.
- Pupils should be helped to understand the need for a Pupil Acceptable Use agreement and encouraged to adopt safe and responsible use of the internet both inside and outside of school. This links to our school values of love, courage and hope.

Staff

- A planned programme of online safety training will be made available to all staff which may be additional to or part of the annual safeguarding training. This will be regularly updated and enforced
- All new staff will receive Safeguarding training, which includes online safety, as part of their induction programme.

Governors

- Participation in the school training and annual safeguarding training
- A higher level of **training will be made available for the governor responsible for Online Safety**

Parents and Carers

The school will seek to provide information for families through:

- Regular communication, awareness-raising and engagement on safety issues, curriculum activities and reporting routes
- Letters, newsletters and website
- High profile events and campaigns e.g. Safer Internet Day
- Reference and links to relevant sites and support services on school website

See appendix 1 for specific details on the acceptable use of ICT at Long Sutton CE Primary.

Technology

Information system security

The school will be responsible for ensuring that the school network is as safe and secure as is possible and that the policies and procedures approved within this policy are implemented.

The school ICT systems capacity and security will be regularly reviewed; at least annually.

Our IT provider / network manager – **Rocket Computer Services** – provides web filtering and virus protection for the school.

ICT systems capacity and security, including regular reviews and audits of the safety and security of school technical systems will be carried out by Rocket and any recommendations or breaches will be reported to senior leaders, via the admin officer.

Personal security of staff and pupils with their documents will come through the use of personal log ins and passwords for staff as well as individual accounts for pupils with a set password.

Published content and the school website

The contact details available on the school website are the school address, email address and telephone number. Staff, governors' or pupils' personal information will not be published.

The headteacher will take overall editorial responsibility for the website and ensure that content published is accurate and appropriate. The class teachers will be responsible for the content published onto their class pages.

Publishing pupils' images and work.

Pupils' full names will not be used anywhere on the school website, particularly with association to photographs.

Photographs that include pupils will be selected carefully. Permission forms are completed by all parents when children begin the school before photographs of pupils are published on the school website. Permission lists are kept in the school office and staffroom. Class teachers are to ensure that they are checking this when adding photographs to the school website and class pages. Photographs of pupils must not be taken or stored on personal devices.

Social networking and personal publishing

All schools and local authorities have a duty of care to provide a safe learning environment for pupils and staff. Schools and local authorities 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 group liable to the injured party.

The school ensures that personal information is not published.

Staff should ensure that;

- No reference should be made in social media regarding pupils, parents and carers and other material against the school.
- They do not engage in online discussion on personal matters relating to members of the school community.
- Personal opinion should not be attributed to the school or local authority.
- Security settings are regularly checked to minimise risk of loss of personal information

Rocket blocks/filters access to social networking sites.

Pupils will be advised never to give out personal details of any kind which may identify them or their location.

Pupils and parents will be advised that there are a variety of social network spaces outside school. While some are designed for children of primary age, other have age restrictions and therefore are deemed inappropriate.

Personal Use:

- Personal communications are those made via a personal social media accounts. In all cases, where a personal account is used which associates itself with the school or impacts on the school, it must be made clear that the member of staff is not communicating on behalf of the school with an appropriate disclaimer. Such personal communications are within the scope of this policy

- Personal communications which do not refer to or impact upon the school are outside the scope of this policy.

- Where excessive personal use of social media in school is suspected, and considered to be interfering with relevant duties, disciplinary action may be taken. Where deemed appropriate any concerns/actions may be entered on CPOMS in order to monitor.

Managing filtering

The school will work with both the network manager and Internet service provider to ensure systems to protect pupils are reviewed and improved. The filtering provided meets the standards defined in the IK Safer Internet Centre.

There are established and effective routes for users to report inappropriate content, with the school admin officer being the point of liaison with the school provider.

The service provider, computing lead and admin officer will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable across all devices capable of accessing the Internet.

Managing mobile technologies

Mobile technology devices may be school owned/provided or personally owned and might include: smartphone, tablet, notebook / laptop or other technology that usually has the capability of utilising the school's wireless network. The device then has access to the wider internet and other cloud based services such as email and data storage. All users should understand that the primary purpose of the use mobile / personal devices in a school context is educational.

The use of mobile technologies within school is carefully managed and falls within the acceptable use agreement for details of use within the school setting.

Use of video conferencing tools for online teaching (eg Teams or Zoom) will only be used in group/class work and links for access will always be sent through pupil email accounts, which are secured using Microsoft O365 with relevant password procedures in place.

The use of mobile phones by pupils is not permitted on the school premises. Mobile phones for pupils will only be allowed in exceptional circumstances, and then only by prior agreement. Any phone must be handed into the school office for the period of the school day.

Contact with children should be via the school phone only.

YouTube and Google Images

Videos on the file-sharing website YouTube can be used to effectively support many areas of the curriculum. When these videos are used safely and appropriately, they can be an extremely beneficial resource for Class Teachers and Support Staff.

In the same way google images provides a plethora of curriculum enhancing opportunities to make teachers resources more relevant, accessible and powerful.

However, there are potential risks when working with YouTube, Vimeo and Google Images that staff should be aware of. For example, despite a filter/flagging policy being in use on YouTube, inappropriate images, unsuitable written comments, or bad language can still all be accidentally revealed to the children. In order to prevent this from happening, the following precautions should be taken:

Finding suitable videos and images.

- Searches, or first observations of a potential video and images, should not be carried out with any child in the class room.
- Before showing a video or image to the class, the video should be watched and listened to carefully by the Class Teacher or LSA, who should look out for inappropriate content material along with any inappropriate comments that appear underneath the video.
- It is the class teacher's responsibility to make the final approval of a video or image used.

Playing the video for the children

- Using the remote control, the whiteboard should be frozen, stilled or muted (depending on the option available on your remote) prior to Full Screen mode being selected for the video. (This is so that no comments or any other videos can be seen by the children).When the video is ready, the whiteboard can be unfrozen and the video watched.
- Before the end of the video, pause it so 'recommended' videos that might potentially contain inappropriate language, are not revealed.
- When the video is finished, the whiteboard should once again be frozen, stilled or muted (or even turned off) so that the video can be exited and the YouTube window closed safely.

Educating the children about safe use of these sites.

Children will have these sites explicitly demonstrated as part of their online safety teaching. Pupils will be made aware of best practices if they come across unsuitable content online including; turning off the screen, telling an adult and protocol for reporting inappropriate material to websites with the help of a website. Under no circumstances will children be using image or video sharing websites unsupervised.

Security, Data and Confidentiality

When accessing, amending and saving any data or information relating to the school or pupils, school staff follow the guidelines set out in the General Data Protection Regulations 2018.

Authorising internet access

All pupils and parents are made aware of the 'Online safety Acceptable Use Agreement' (See appendix 2) before using any school ICT resources.

Assessing risks

The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the international scale and linked nature of internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer or device. The school cannot accept liability for the material accessed, or any consequences of internet access.

The monitoring and decision making of the teachers will determine which websites are accessed when using the internet within lessons.

The school will audit ICT provision to establish whether the Online Safety policy is adequate and that its implementation is effective, particularly in light of new developments with technology.

Handling online safety complaints

Complaints of pupil internet misuse will be dealt with by the appropriate member of staff. This may be the class teacher, Senior Leadership Team including the head teacher. Concerns should be reported as soon as possible after the event on CPOMS should be completed and the DSLs alerted. Guidance on this is given through the 'Responding to incidents' flow chart (Appendix 3).

Any complaint about staff misuse must be referred to the head teacher.

Complaints of a bullying nature must be dealt with in accordance with the school anti bullying policy. The school recognises that anonymous bullying is still bullying.

Complaints of a child protection nature must be dealt with in accordance with school child protection procedures (See the Child Protection Policy)

Dealing with Online Incidents

It is hoped that all members of the school community will be responsible users of digital technologies, who understand and follow school policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse.
In the event of suspicion, all steps in this procedure should be followed:

- Have more than one senior member of staff or governor involved in this process. This is vital to protect individuals if accusations are subsequently reported.
- Conduct the procedure using a designated computer that will not be used by young people and if necessary can be taken off site by the police should the need arise. Use the same computer for the duration of the procedure.
- It is important to ensure that the relevant staff should have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).
- Record the URL of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation.
- Contact NSPCC Helpline for advice – 0800 800 5000

Once this has been completed and fully investigated senior leadership and the Computer Lead will need to judge whether this concern has substance or not. If it does then appropriate action will be required and could include the following:

- Internal response or discipline procedures.
- Involvement by Local Authority.
- Police involvement and/or action.

If content being reviewed includes images of Child abuse and/ or child pornography then the monitoring should be halted and referred to the Police immediately via ceop.police.uk. Any immediate risk would require calling 999. Other instances to report to the police would include:

- incidents of 'grooming' behaviour
- the sending of obscene materials to a child
- adult material which potentially breaches the Obscene Publications Act
- criminally racist material
- promotion of terrorism or extremism
- other criminal conduct, activity or materials

Isolate the computer in question as best you can. Any change to its state may hinder a later police investigation.

It is important that all of the above steps are taken as they will provide an evidence trail for
The school and possibly the police and demonstrate that visits to these sites were carried out for safeguarding purposes.

School recognises that some children have an increased vulnerability to risk online, especially those with language and communication needs, or social communication difficulties. The school has a list of vulnerable children and all staff will be responsible for being aware of their additional needs.

The use of Generative Artificial Education (AI) in school

This is a rapidly changing area; as a school we are aware of the need to monitor developments and respond promptly and responsibly in line with DFE guidelines. (see Appendix 4)

Appendix I

Acceptable Use of ICT at Long Sutton CE Primary

School Responsibilities

The school has a responsibility to provide all children with safe and secure access to a wide range of IT resources and forms of media, including those available online. Children have a clear minimum entitlement to use IT as part of the National Curriculum and this will be taught alongside a comprehensive internet safety curriculum.

The school has a responsibility to ensure that children have access to a wide range of media to accommodate the digital age we live in and will be given opportunities across the curriculum to use different technologies, including iPads.

Misuse

We take misuse of any form of media (*text, digital image of any type, video and or audio file*) by any member of the school community seriously and will deal with any incidents that occur as if they had occurred on school property during the school day. We take the view that all users do so under the direct code of conduct set out below.

- It is an offence under the school code of conduct for any member of the school community to publish any derogatory remark in any form of media.
- It is an offence under the school code of conduct for any member of the school community to extract any form of media for use in cyber bullying.
- It is an offence under the school code of conduct for any member of the school community to produce, publish or store any sexist, racist, sexually exploitive, radicalisation and propaganda material in any form of media.
- It is an offence under the school code of conduct for any member of the school community to knowingly store or seek to spread a virus.

Dealing with misuse

- We will deal with any incidents of cyber bullying as if the bullying had taken place within the physical bounds of the school.
- We will investigate and work with all parties in any incidents of cyber bullying that take place between members of the school community, where clear evidence is provided. The school takes the position that as these persons would have never met without the school as contact point then the school has a duty to help. Following best practice, where cyber bullying threatens violence or is of a sexual nature, the police will be asked for their advice/involvement.
- Offences will be dealt with according to the level of the offence in line with school discipline for pupils and guidelines for staff disciplinary procedures. If the offence is a breach of criminal law, the police will be called in and all evidence will be presented to be the best of the schools ability.
- Minor infringements of these rules by pupils will be dealt with by the head teacher.

Homework

Teachers may provide homework that requires the children to have access to a computer and/or the internet. Pupils who don't have access to a computer or internet at home should be sensitively offered the choice of a worksheet or the opportunity to complete their homework using a school computer at break and lunchtime, and at homework club. If a pupil expressed a desire to use the school network then this arrangement can be assumed to be continual.

Password Security

Each individual is responsible for their own login. Children have individual logins but a generic password, this is for ease of access. Children should still be taught about keeping personal information safe and not share their login details with anyone.

Children should be taught to log off and shut down to ensure that access to other pupils accounts can't be accessed.

Communication

E-Mail

- At school pupils may only use approved messaging accounts. (class g-mail accounts, Purple Mash)
- Pupils must immediately tell a teacher if they receive an offensive message.

- Pupils must not reveal personal details about themselves or others in online communication, or arrange to meet anyone without specific permission.

*This policy should be read in conjunction with:

- Preventing and tackling bullying policy
- Remote learning policy
- Safeguarding policy
- Staff code of conduct policy

Appendix 2

Online Safety Acceptable Use Agreement

These online safety rules help to protect students and the school by describing acceptable and unacceptable computer use.

Think then Click!

- ✓ I understand that I must have permission from an adult before using the internet.
- ✓ I agree to only use websites that an adult has chosen.
- ✓ I will tell an adult if I see anything that I am uncomfortable with.
- ✓ I know that I must immediately close any web page that I am not sure about or if I see something I do not like
- ✓ I will only send e-mails to people an adult has approved.
- ✓ I will only send e-mails and messages that are polite and friendly.
- ✓ I know that I must never give out personal information or passwords.
- ✓ I agree never to arrange to meet anyone that I do not know.
- ✓ I understand that I should not open emails sent by people that I do not know.
- ✓ I know that we do not use internet chat rooms in school
- ✓ I know that I should use the internet to access appropriate material
- ✓ I understand that my teacher and/or parents will be involved if I do not follow these rules.

The school may exercise its right to monitor the use of the schools computer systems, including access to websites, the interception of e-mail and the deletion of inappropriate materials where it believes unauthorised use of the schools computer system may be taking place, or the system may be being used for criminal purposes or for storing unauthorised or unlawful text, imagery or sound.

Online Safety Rules

All pupils use computer facilities including Internet access as an essential part of learning, as required by the National Curriculum. Both pupils and their parents/carers are asked to sign to show that the Online Safety Rules have been understood and agreed.

Pupil: ***Class:***

Pupil's Agreement:

- ✓ I have read and I understand the school Online Safety Rules.
- ✓ I will use the computer, network, mobile phones, Internet access and other new technologies in a responsible way at all times.
- ✓ I know that network and Internet access may be monitored.

Signed: ***Date:***

Parent's Consent:

I have read and understood the school e-safety rules. I understand that the school will take all reasonable precautions to ensure that pupils are safe and protected whilst using computer facilities, including the internet.

Signed: ***Date:***

Please print name:

Online Safety Rules

Key Stage 1

Think then Click!

These rules help us to stay safe on the Internet:

- We only use the internet when an adult is with us.
- We can click on the buttons or links when we know what they do.
- We can search the Internet with an adult.
- We always ask if we get lost on the Internet.
- We can send and open emails together.
- We can write polite and friendly emails to people that we know.

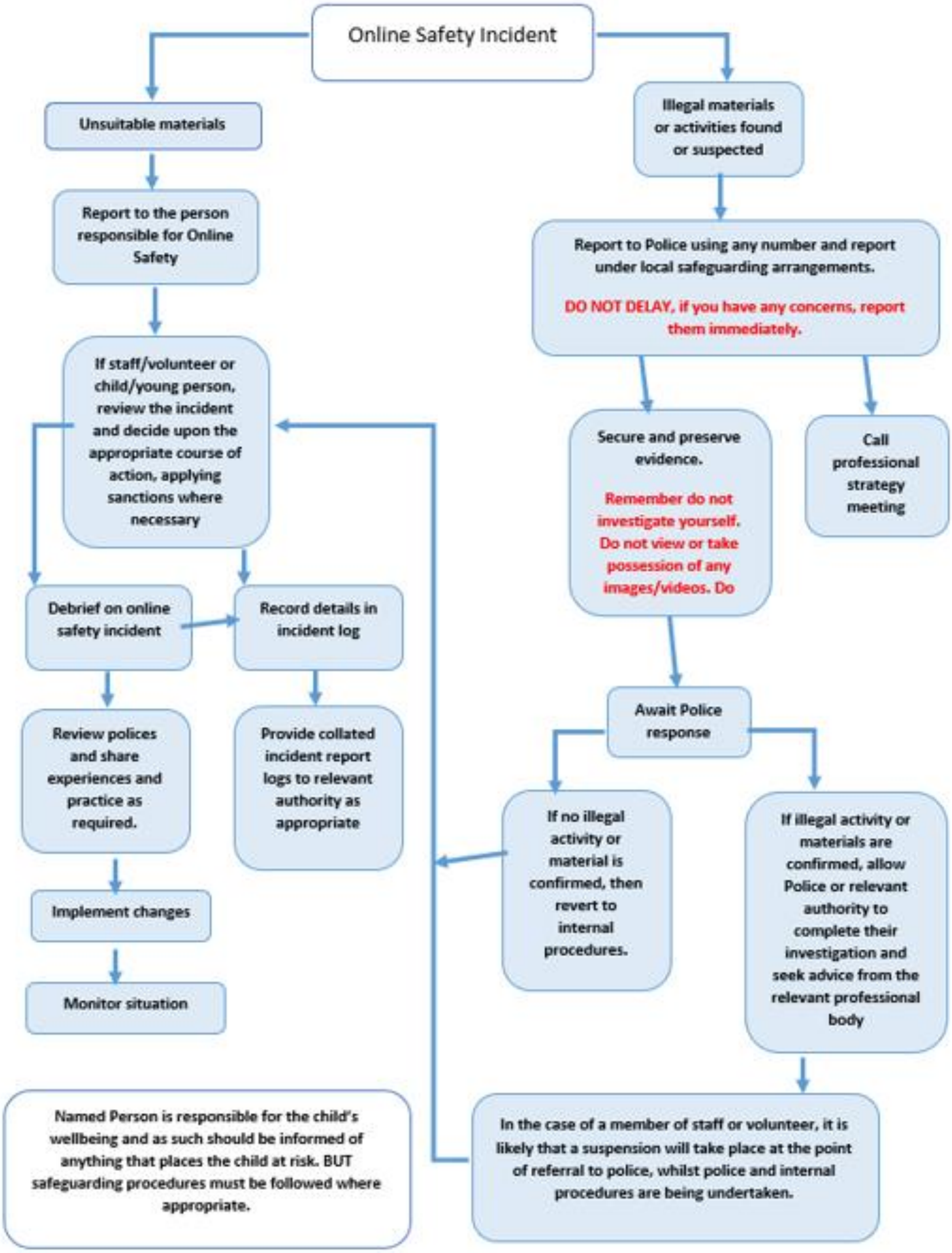
Key Stage 2

Think then Click!

- We ask permission before using the Internet.
- We only use websites that an adult has chosen.
- We tell an adult if we see anything we are uncomfortable with.
- We immediately close any web page we not sure about.
- We only e-mail people an adult has approved.
- We send e-mails that are polite and friendly.
- We never give out personal information or passwords.
- We never arrange to meet anyone we don't know.
- We do not open e-mails sent by anyone we don't know.
- We do not use Internet chat rooms.

Appendix 3

Responding to incidents flow chart



Online Safety Incident

Unsuitable materials

Report to the person responsible for Online Safety

If staff/volunteer or child/young person, review the incident and decide upon the appropriate course of action, applying sanctions where necessary

Debrief on online safety incident

Record details in incident log

Review polices and share experiences and practice as required.

Provide collated incident report logs to relevant authority as appropriate

Implement changes

Monitor situation

Illegal materials or activities found or suspected

Report to Police using any number and report under local safeguarding arrangements.

DO NOT DELAY, if you have any concerns, report them immediately.

Secure and preserve evidence.

Remember do not investigate yourself. Do not view or take possession of any images/videos. Do

Call professional strategy meeting

Await Police response

If no illegal activity or material is confirmed, then revert to internal procedures.

If illegal activity or materials are confirmed, allow Police or relevant authority to complete their investigation and seek advice from the relevant professional body

In the case of a member of staff or volunteer, it is likely that a suspension will take place at the point of referral to police, whilst police and internal procedures are being undertaken.

Named Person is responsible for the child's wellbeing and as such should be informed of anything that places the child at risk. BUT safeguarding procedures must be followed where appropriate.

Appendix 4

https://www.gov.uk/government/publications/generative-artificial-intelligence-in-education/generative-artificial-intelligence-ai-in-education