



St. Peter & St. Paul CE Primary School, Burgh-le-Marsh
"Striving for excellence together in a caring Christian community."

RESPECT COMPASSION COURAGE



ONLINE SAFETY POLICY

Responsible: Governing Body

Agreed: January 2023

To be reviewed: Annually (or in the event of serious incident or legislation changes)

Reviewed: November 2023, November 2024, November 2025 (improved clarity, coherence, and readability. Added AI-specific guidance)

Note: Throughout this policy Designated Safeguarding Lead (DSL) also refers to Deputy Designated Safeguarding Leads, even if not explicitly noted.

1. Aims

St. Peter and St. Paul CE Primary School aims to ensure the online safety of all pupils, staff, volunteers, and governors through robust procedures that protect everyone from harm. We are committed to empowering our school community to use technology safely, including mobile, smart devices, and emerging artificial intelligence (AI) tools. Clear processes have been established to identify, intervene, and escalate online safety concerns or incidents when necessary.

Our approach to online safety addresses four key categories of risk. **Content** refers to exposure to illegal, inappropriate, or harmful material, such as pornography, fake news, racism, misogyny, self-harm, suicide, antisemitism, radicalisation, extremism, or AI-generated content that is misleading, harmful, or inappropriate. **Contact** involves harmful online interactions, including peer-to-peer pressure, commercial exploitation, and adults posing as young people to groom or exploit children. **Conduct** relates to personal online behaviour that may increase risk of harm, such as sharing explicit images or videos, non-consensual distribution of content, cyber-bullying, harassment, or misuse of AI tools. **Commerce** refers to financial risks including phishing, scams, inappropriate advertising, or online gambling.

2. Legislation and Guidance

This policy aligns with statutory safeguarding guidance, including the Department for Education's Keeping Children Safe in Education (KCSIE) and related guidance on teaching online safety, preventing and tackling bullying, and searching, screening, and confiscation. It also incorporates guidance on relationships and sex education, protecting children from radicalisation, and the safe use of digital and AI technologies. Relevant legislation includes the Education Acts of 1996, 2006, and 2011, the Equality Act 2010, and data protection laws. The policy also reflects National Curriculum computing programmes of study, including digital literacy and ethical use of technology.

3. Roles and Responsibilities

The Governing Body has overall responsibility for monitoring this policy and holding the headteacher accountable for its implementation. Governors are expected to read and understand the policy, agree to the terms of acceptable use of school IT systems, and ensure that online safety, including the safe use of AI, is embedded in safeguarding and other related policies. Governors should ensure that teaching about online safety is adapted for vulnerable pupils and those with SEND.

The headteacher ensures that staff understand and consistently implement this policy. The designated safeguarding lead (DSL) and deputies manage online safety incidents, provide reports, update and deliver training, liaise with external agencies, and oversee incidents involving AI misuse.

IT management, provided by Education Lincs Ltd, ensures that security systems are in place and maintained, including monitoring, filtering, and access controls. These systems protect pupils from harmful content, unsafe contact, inappropriate AI use, and malicious software.

All staff and volunteers are responsible for understanding and implementing this policy consistently, following acceptable use agreements, and supporting pupils to do the same. They must respond to concerns about online safety, cyber-bullying, or AI misuse appropriately.

Parents are expected to ensure their children understand and follow the school's acceptable use agreements and report any concerns about online safety or AI use. Visitors and community members using school IT are expected to follow this policy and agree to acceptable use where relevant.

4. Educating Pupils

Online safety is embedded in the curriculum, including computing, PSHE, relationships, and health education. Pupils are taught to use technology, including AI tools, safely, respectfully, and responsibly. In Key Stage 1, children learn to keep personal information private and report concerns. In Key Stage 2, they learn to recognise acceptable and unacceptable behaviour, critically assess online content, and understand ethical AI use. By the end of primary school, pupils understand online risks, AI risks, the importance of digital citizenship, and how to make safe, informed decisions online. Teaching is adapted as necessary for vulnerable pupils or those with SEND.

5. Educating Parents

The school raises parents' awareness of online safety, including AI, through letters, website updates, ParentHub, and during parents' evenings. Parents are informed of filtering and monitoring systems, what pupils are asked to do online, and with whom they may interact. Queries should be raised with the headteacher or DSL.

6. Cyber-Bullying

Cyber-bullying occurs online, including through social media, messaging apps, gaming platforms, and AI-generated content. The school teaches pupils what cyber-bullying is, why it occurs, and how to report it. Lessons include discussions on digital ethics and responsible AI use. Parents receive guidance on

recognising signs of cyber-bullying. Incidents are managed under the behaviour policy, logged by the DSL, and escalated to external agencies or police when illegal material is involved.

Searching of electronic devices follows statutory guidance. Staff will not view indecent images of children but will report them immediately to the DSL. Misuse of AI by pupils that results in harm, deception, or inappropriate content is treated with the same seriousness as other online safety incidents.

7. Acceptable Use

All members of the school community, including pupils, staff, governors, volunteers, and relevant visitors, must follow the school's acceptable use agreements. School IT, including AI platforms, must only be used for educational or professional purposes. Activity may be monitored to ensure compliance.

8. Mobile Devices

Year 6 pupils who walk home independently may bring mobile devices, but these must remain switched off while on school premises. Misuse of devices or AI tools may result in confiscation or disciplinary action.

9. Staff Use of Devices

Staff must secure work devices with strong passwords, encryption, and automatic locks. Devices must not be shared and are to be used only for professional purposes. Staff must follow acceptable use agreements when using AI tools in the classroom or for planning, ensuring data privacy, accuracy, and ethical use. Security concerns must be reported to the headteacher or IT support immediately.

10. Responding to Misuse

Pupil misuse of IT, AI tools, or the internet is addressed through the behaviour, anti-bullying, and acceptable use policies, with responses proportionate to the incident. Staff misuse is addressed through HR and disciplinary procedures. Serious incidents, including illegal activity, are reported to the police.

11. Training

All new staff receive online safety and AI training during induction. All staff undertake refresher training annually, covering online abuse, cyber-bullying, online radicalisation, and responsible AI use. DSLs and deputies update their knowledge regularly, and governors receive training as part of safeguarding induction. Volunteers receive training as appropriate.

12. Monitoring

All online safety incidents, including AI-related concerns, are logged and monitored by senior leaders and DSLs. The policy is reviewed at least annually to reflect evolving technologies, risks, and safeguarding requirements.

13. Links with Other Policies

This online safety policy should be read in conjunction with:

- Child Protection and Safeguarding Policy
 - Behaviour Policy
 - Staff Disciplinary Procedures
 - Data Protection Policy and Privacy Notices
 - Complaints Procedure
 - IT and Internet Acceptable Use Policy
 - Use of AI Policy
-

14. Use of AI in School (see also full Use of AI Policy)

The school recognises that AI tools can enhance learning and teaching but also present new risks. AI use in school is guided by the following principles:

1. Staff and pupils should use AI responsibly to support learning and teaching, not to bypass assessment or safeguarding expectations.
2. Outputs from AI tools must be reviewed critically to ensure accuracy, reliability, and ethical use.
3. Personal information must not be input into AI tools without consent, in line with data protection requirements.
4. AI use is supervised and monitored to prevent harm or misuse.
5. Misuse of AI, including creating harmful or inappropriate content, will be addressed under the behaviour or staff disciplinary policies.



APPENDIX 1: ACCEPTABLE USE POLICY – STAFF, GOVERNORS & VISITORS

Note: All internet, email, and AI-related activity conducted on school equipment or systems is subject to monitoring. This policy should be read in conjunction with the Online Safety Policy. Staff, governors, and visitors are expected to familiarise themselves with the policy. Being made aware of the policy is taken to indicate understanding and compliance.

1. Internet Access: Staff, governors, and visitors must not access or attempt to access any sites containing content that is illegal, abusive, discriminatory, pornographic, or intended to promote racial or religious hatred. This includes content that encourages illegal acts, harm, or extremist ideologies. Any inadvertent access must be treated as an online safety incident and reported immediately to the Online Safety/Safeguarding Lead, with a CPOMS incident form completed. The use of AI tools to generate content, summaries, or research must be safe, legal, and professional. Staff must ensure AI-generated material does not contain inappropriate, biased, or unsafe content, and outputs must be critically reviewed before use with pupils or colleagues.

2. Use of Email: School email addresses must only be used for professional purposes. Personal business, AI-generated communications without oversight, or mass distribution to external contacts without approval is prohibited. Staff are reminded that school emails and data are subject to Freedom of Information requests and may be reviewed under Subject Access Requests.

3. Passwords: Staff, governors, and visitors must keep passwords private and secure. Under no circumstances should passwords be shared with colleagues, pupils, or other individuals, except in exceptional circumstances as authorised by IT Support. Passwords must also not be used in AI systems unless encrypted and secure.

4. Data Protection and Encryption: When working remotely or off-site, all school devices, USBs, or other media must be encrypted. Sensitive data—including pupil information, staff records, and AI-generated outputs containing personal data—must never be stored on unencrypted devices. Any data transfer must be secure and comply with GDPR and the school's Data Protection Policy.

5. Images and Videos: Staff, governors, and visitors must not upload images or videos of themselves, pupils, or colleagues to any online platform without explicit consent. This applies to both professional and personal contexts. Staff must ensure that automatic cloud backups (e.g., iCloud, Google Photos) do not upload school images or AI-generated content containing sensitive information without consent.

6. Personal Use of School IT: School IT equipment may only be used for personal purposes if specific permission is granted by the Headteacher, who will set clear boundaries. Personal or AI-assisted use must not interfere with school work or compromise online safety.

7. Use of Personal IT: Permission to use personal IT equipment for school purposes must be sought from the Headteacher. The Online Safety Lead and IT Support will assess risks before approval. Staff must ensure personal devices do not automatically store or back up sensitive school data, including AI-generated content.

8. Viruses and Malware: Any suspected virus or malware outbreak must be reported immediately to the IT Technical Support Helpdesk. Include the name of the virus (if known) and any actions taken. Staff must exercise caution when downloading AI tools, software, or datasets from external sources to avoid malware risks.

9. Online Safety: Online safety is everyone's responsibility. Staff, governors, and visitors are expected to model positive online behaviour, promote safe use of technology, and encourage pupils to make responsible digital and AI-enabled choices.

10. Social Networking: Staff, governors, and visitors must adhere to the Social Media Policy and Local Authority guidelines. Personal use of social media must never undermine the school, its staff, parents, or pupils. AI-generated posts or content shared on social media must also be reviewed for accuracy, privacy, and appropriateness.

11. AI Tools and Use: Staff may use AI tools to support teaching, administration, or professional research only under the following conditions:

1. AI outputs must be critically evaluated for accuracy, bias, and appropriateness before being used in a school context.
2. AI must never be used to generate, manipulate, or store sensitive pupil data without explicit consent and compliance with GDPR.
3. AI use must comply with the school's acceptable use policy, safeguarding policies, and data protection regulations.
4. Staff must not encourage pupils to use AI tools unsupervised or to generate content that could be unsafe, misleading, or inappropriate.

12. How the School Will Respond to Misuse: Misuse of the school's IT systems, AI tools, or internet access may lead to disciplinary action and/or reporting to external authorities if appropriate. The action taken will depend on the nature, seriousness, and circumstances of the incident.

13. Acknowledgement: By being made aware of this Acceptable Use Policy, including guidance on AI use, staff, governors, and visitors are expected to comply with its requirements. Misuse may result in disciplinary action or reporting to external authorities.



APPENDIX 2: ACCEPTABLE USE POLICY – PUPILS

RULES FOR GOOD ONLINE BEHAVIOUR

Note: All Internet, email, and AI activity in school or using school equipment may be monitored.

I promise – to only use the school IT equipment and AI tools for schoolwork that the teacher has asked me to do.

I promise – not to look for, make, or show other people things that may be upsetting or harmful.

I promise – to show respect for the work that other people have done.

I will not – use other people's work, pictures, or AI-generated content without permission.

I will not – damage the IT equipment. If I accidentally damage something, I will tell my teacher.

I will not – share my password with anybody. If I forget my password, I will let my teacher know.

I will not – use other people's usernames or passwords.

I will not – share personal information online with anyone.

I will not – download anything from the Internet or AI tools unless my teacher has asked me to.

I will – let my teacher know if anybody asks me for personal information.

I will – let my teacher know if anybody says or does anything to me that is hurtful, unsafe, or upsets me.

I will – be respectful to everybody online and when using AI. I will treat everybody the way I want to be treated.

I understand – that some people on the Internet are not who they say they are, some AI content may not be correct, and some people can be unkind. I will tell my teacher if I am ever concerned in school, or my parents if I am at home.

I understand – that if I break these rules, there will be consequences for my actions, and my parents will be told. Being made aware of these rules means I agree to follow them.

Signed (Parent): _____ Date: _____

Signed (Pupil): _____ Date: _____



INTERNET FILTERING AND MONITORING INFORMATION FOR PARENTS

Use of the Internet is a vital part of your child's education. At our school, we make extensive use of the Internet and approved AI tools to enhance learning, provide opportunities for research, and support collaboration and communication.

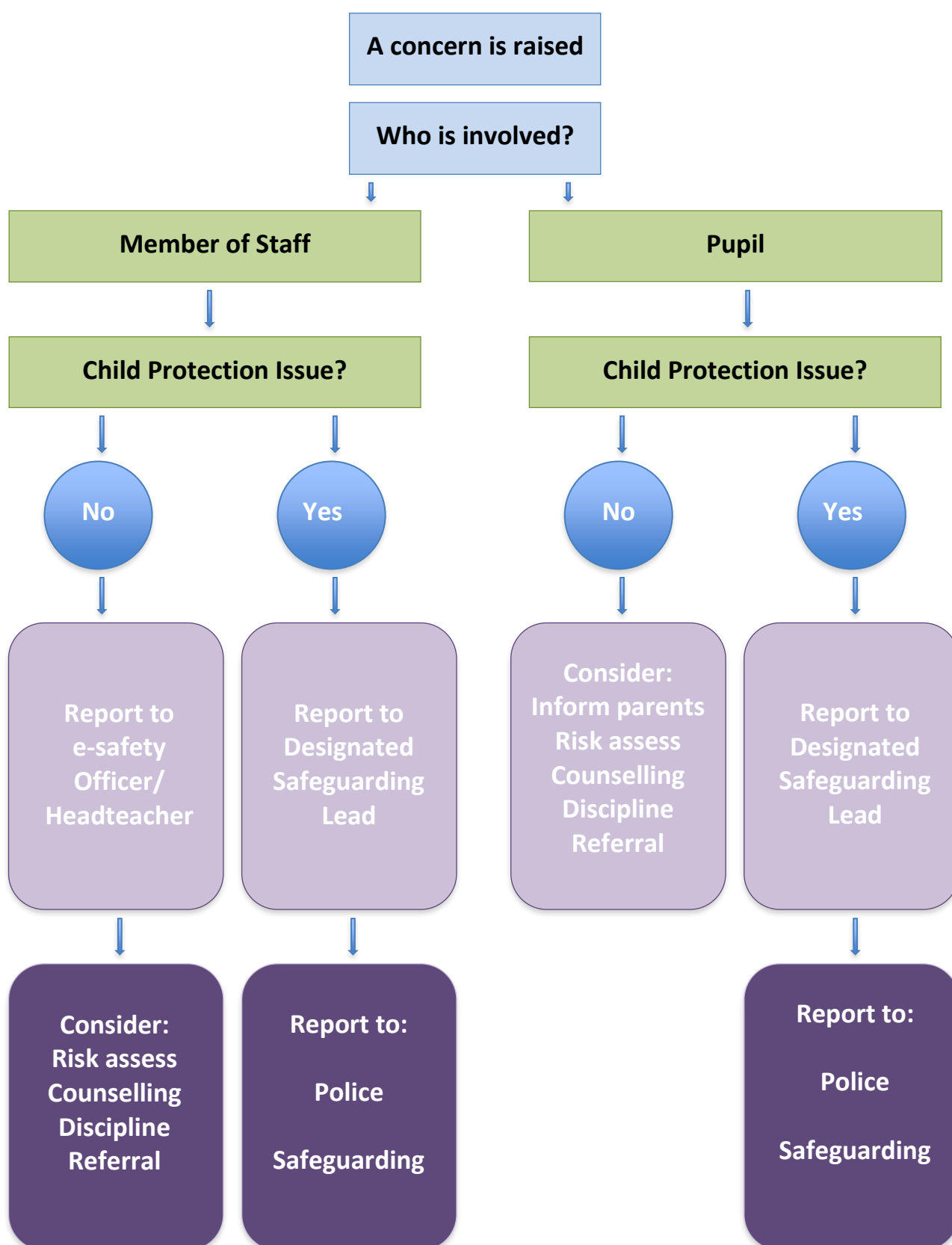
You will be aware that the Internet hosts a wide range of illegal and inappropriate content. To protect your child, we use advanced filtering software to prevent access to harmful sites. Our school currently uses the Cisco Meraki & SENSO filtering solutions, which categorises websites and keystrokes according to their content. Access is then allowed or blocked depending on the user and the device being used.

The software also allows us to monitor Internet and AI activity. Logs are kept showing which user has accessed which sites or tools and when. Ensuring your child's safety online is our highest priority. Occasionally, we may review these logs to ensure there have been no attempts to access inappropriate content or misuse AI tools. If we believe there has been questionable activity involving your child, we will contact you promptly to discuss the circumstances.

Throughout the school year, we teach children about the importance of safe Internet and AI use. We explain that there needs to be a balance between privacy and safety, and that their activity may be monitored. Children are always encouraged to ask questions and to raise any concerns.

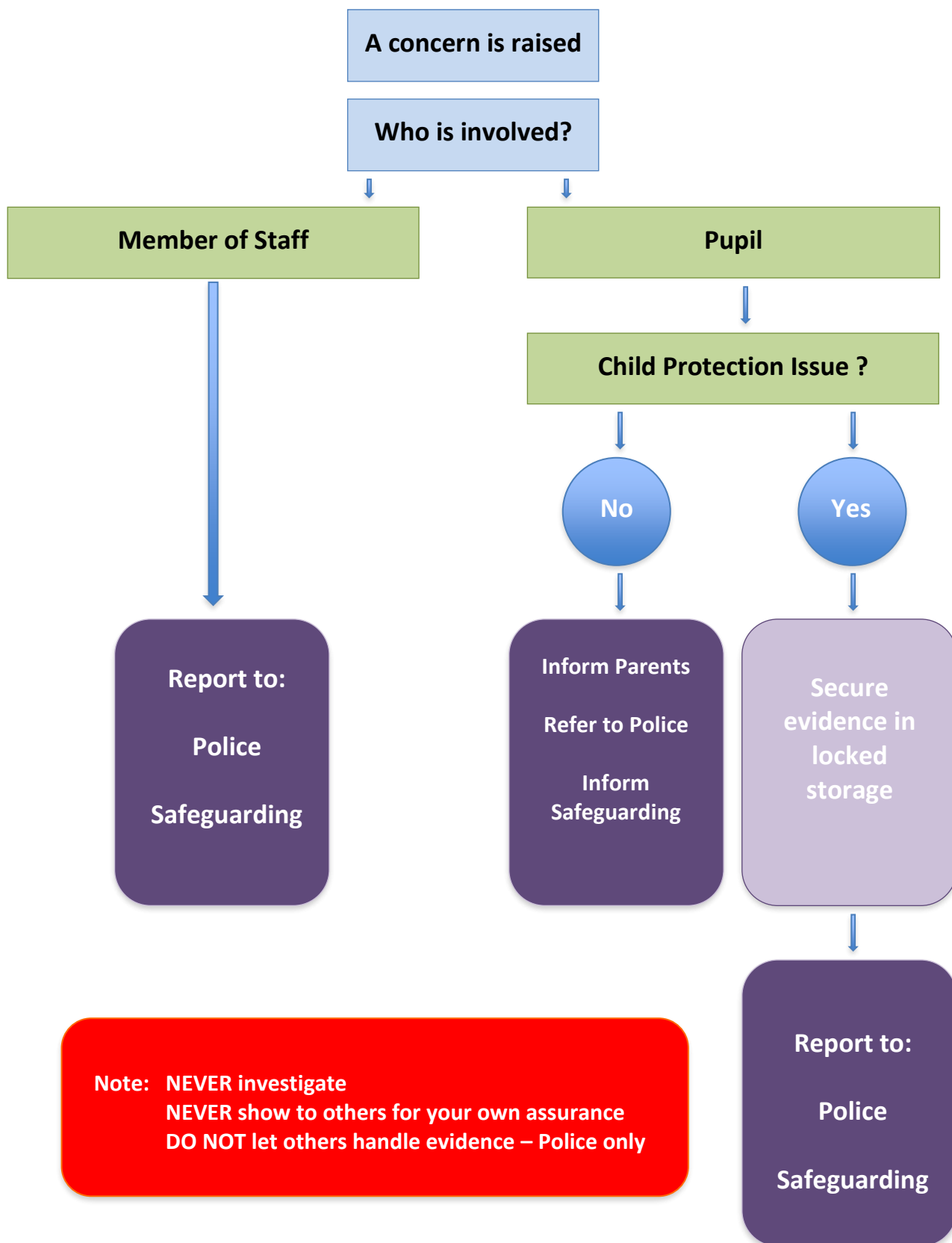
If you have any questions or would like further information about how we keep your child safe online and when using AI, please contact the school.

APPENDIX 3: INAPPROPRIATE ACTIVITY FLOWCHART



If you are in any doubt, consult the Headteacher, Designated Safeguarding Lead or Safeguarding

APPENDIX 4: ILLEGAL ACTIVITY FLOWCHART



APPENDIX 5: ONLINE SAFETY TRAINING NEEDS – SELF-AUDIT FOR STAFF

ONLINE SAFETY TRAINING NEEDS AUDIT

Name of staff member/volunteer:

Date:

Role:

Question

Yes/No (add comments if necessary)

Do you know the name of the person who has lead responsibility for online safety in school?

Are you aware of the ways pupils can abuse their peers online?

Do you know what you must do if a pupil approaches you with a concern or issue?

Are you familiar with the school's acceptable use agreement for staff, volunteers, governors and visitors?

Are you familiar with the school's acceptable use agreement for pupils and parents?

Do you regularly change your password for accessing the school's ICT systems?

Are you familiar with the school's approach to tackling cyber-bullying?

Are there any areas of online safety in which you would like training/further training?